Base Load Power Hub (BLPH)

Instructions for Operation and Maintenance for ProSafe-RS

Document Number: 1724000594-IN-MAN-00038

Supplier Document Number: E366772C00-SIS_IOM

Document Class: 3

01	17/02/2025	Issue for Information (IFI)	SKR	MP/AB	SC
00	29/07/2024	Issue for Review (IFR)	SKR	MP/AB	SC
Rev.	Date	Description	Prepared	Reviewed	Approved

YOKOGAWA Co-innovating tomorrow™

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Revision / Change Log

Rev.	Description
0	Issue for Review (IFR)
1	Issue for Information (IFI)

HOLDS LIST

No.	Description
1	
2	
3	
4	

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Table of contents

1 Introduction 7
1.1 Project Overview 7
1.1.1 Project Location 7
1.1.2 Project Concept 8
2 Document Scope 10
2.1 References 10
2.1.1 Project Reference Documents 10
2.1.2 Yokogawa Reference Document 11
2.2 Order of Precedence 12
2.3 Definitions And Abbreviations 13
3 General Instructions 17
3.1 Systems Involved 17
3.2 Prerequisites 17
3.3 Personal Competency 18
4 System Power-up 19
5 Operations 21
5.1 Trip Reset 21
5.2 Maintenance Override 21
5.2.1 MOS Monitoring 22
5.2.2 MOS Activation 22
5.2.3 MOS Removal 22
5.2.4 Emergency MOS Removal 23
5.2.5 Active MOS Monitoring 23
5.3 Start-Up Override 23
5.3.1 Start-up Override Monitoring 23
5.4 Equipment Failure Handling 24
5.5 Valve Trip Facility 24
5.6 Interfaces and System Monitoring 24

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

5.6.1 Critical Action Panel (CAP) 24
5.6.2 System Status on OWS 25
5.6.3 System Status on EWS 25
5.6.4 LED Indication on modules 26

6 Maintenance 27

6.1 Prerequisites 27
6.2 Recommendations for the End User 27
6.3 Preventive Maintenance 28
6.4 First Line Maintenance 29
6.4.1 ProSafe-RS System 29
6.4.2 Power Supply 30
6.4.3 Environmental Conditions 31
6.4.4 Cleaning 31
6.4.5 Air Filters 32
6.4.6 Hazardous Area Equipment 32
6.4.7 Spare Parts 32
6.4.8 Routine checks 32
6.4.9 System Documentation 33
6.4.10 Routine PC Housekeeping 33
6.4.11 Operation History 33
6.5 Shutdown Maintenance 34
6.5.1 ProSafe-RS System 34
6.5.2 System status 34
6.5.3 Cleaning 34
6.5.4 Field Power Supply Redundancy Check 35
6.5.5 Functional check of inputs 35
6.5.6 Functional check of outputs 35
6.5.7 Valves and Solenoids 35
6.5.8 Pressure Transmitters 35

7 Proof Testing 36

7.1 General 36
7.2 Recommendations for the End User 36
7.3 Proof test Coverage - Strategies for Proof testing 38

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

7.4 Recording SIF Activation during Process Demand: 38
7.5 SIS Test (ProSafe-RS) 38
7.5.1 Execution of Proof Test 38
7.5.2 Proof Test for ProSafe-RS 38
8 Trouble Shooting 41
8.1 General 41
8.2 Trouble shooting facilities. 41
8.3 LED indications on ProSafe-RS modules 42
8.4 EWS/OWS Diagnostics Management 42
8.4.1 IOM Report 42
8.4.2 Report from SOE viewer 43
8.4.3 I/O Parameter Settings 43
8.5 Overrides 43
8.6 Test / disconnect terminals 43
9 Attachments 44

List of Figures

Figure 1 - HOLLANDSE KUST NOORD WIND PARK Location Map 7
Figure 2 - Wind Park Details 8
Figure 3 – BLPH Concept 8
Figure 4 – Start-up 20
Figure 5 – System Status on OWS 25

List of tables

Table 1 – Project Reference Documents 11
Table 2 – Yokogawa Reference Documents 12
Table 3 – Definitions 13
Table 4 – Abbreviations 16

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Table 5 – Life spans for Parts of Safety Control and Node Units..... 29
Table 6 – Attachments..... 46

List of Attachments

Refer to Section - 9.0

1 INTRODUCTION

1.1 PROJECT OVERVIEW

Crosswind, a Shell and Eneco joint venture, was awarded the tender to develop the offshore Hollandse Kust Noord (HKN) wind farm, located 18.5km off the coast of Netherlands near the town of Egmond aan Zee. The consortium plans to have HKN operational in 2023 with an installed capacity of 759MW generating at least 3.3TWh per year. This is sufficient renewable power to supply more than 1 million Dutch households with green electricity.

Offshore wind farms produce intermittent electricity and balancing these dips and peaks and integrating this electricity into the national energy system requires new technologies. For this reason, the offshore wind farm will include several new technologies that could be implemented at full-scale in the future. The new technologies being explored include a floating solar park, a short-duration battery storage as well as long-term storage via green hydrogen produced by water electrolysis and subsequently consumed in a fuel cell. The combination of these individual measures, herein referred to as the Base Load Power Hub (BLPH) will ensure a continuous power supply regardless of the wind situation.

1.1.1 Project Location

The Hollandse Kust Noord (HKN) wind farm is located 18.5km off the coast of the Netherlands near the town of Egmond aan Zee.

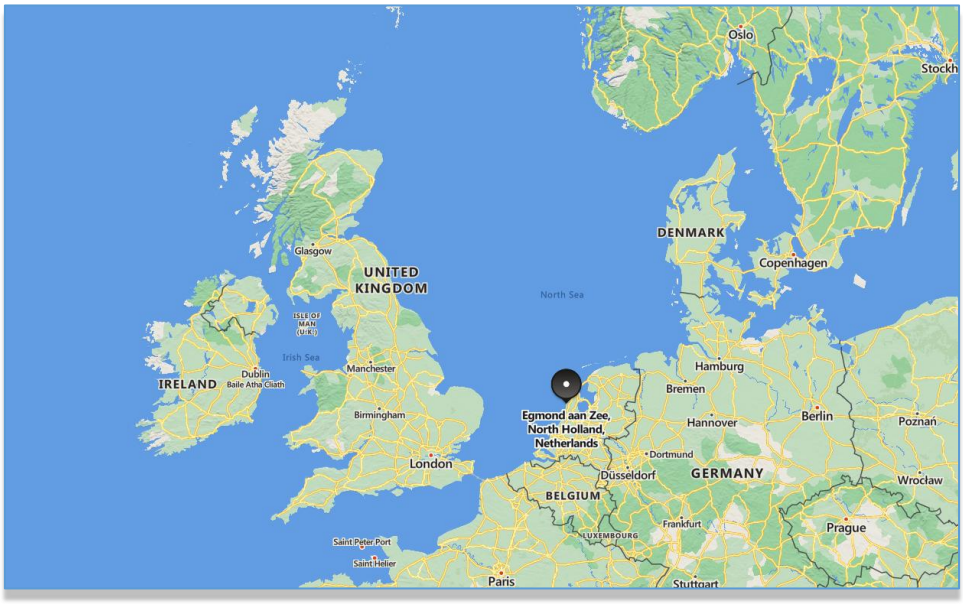


Figure 1 - HOLLANDSE KUST NOORD WIND PARK Location Map

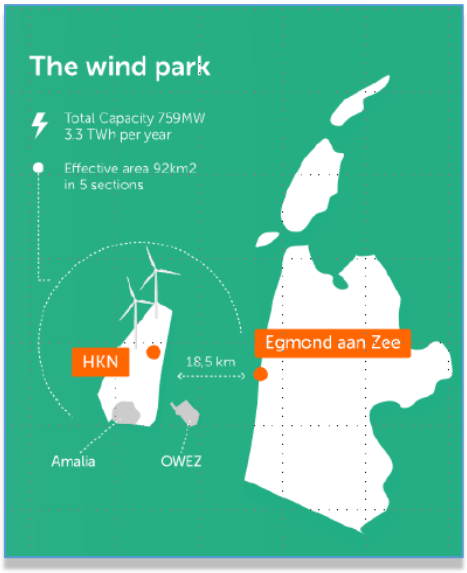


Figure 2 - Wind Park Details

The wind farm will consist of No. 69 x 11.5MW wind turbine generators each to be installed on a dedicated monopile structure. A 70th monopile located on coordinates E 590719.1, N 5841602.3 is reserved for installing the platform accommodating the BLPH. The monopile structure was designed and installed by Van Oord Offshore Wind (VooW) and therefore not part of the BLPH scope.

1.1.2 Project Concept

All components included in the BLPH will be integrated onshore on a topsides and installed in an offshore location within the boundaries of the HKN wind farm. At its simplest, the BLPH will store energy during periods of high electricity generation from renewable sources (a wind turbine generator and the floating solar PV farm) and release it during periods of low generation. In practice. It is expected that the energy stored will supplement generation from renewable sources to ensure that at least 1.0MW of power is exported to the electrical grid regardless of wind/solar availability.

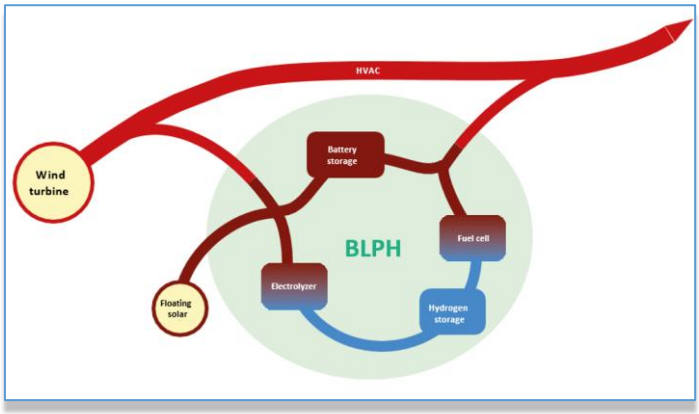


Figure 3 – BLPH Concept

Electricity in the BLPH will be stored in the form of electrons in a battery energy storage system (BESS) as well as converted into green hydrogen via water electrolysis. When the power output from the connecting wind turbine drops to below 1 MWe, the BLPH will return its stored energy to supplement the remaining power output. This will be by discharging the BESS, while stored hydrogen will be converted back into electricity using a fuel cell to extend the discharge duration.

The purpose of the BLPH is to function as a testbed for the integration of energy storage technologies with renewable generation. It is expected that equipment installed on the BLPH will operate as Normally Unmanned Installation for at least two (2) years with no or minimal maintenance and it will have its own independent control room with the ability to communicate with Crosswind's control room.

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

2 DOCUMENT SCOPE

The purpose of this document is to provide essential Instructions for Operation and Maintenance (IOM) of Yokogawa ProSafe-RS based Safety Instrumented System (SIS) and Fire & Gas System (FGS) for BLPH of HOLLANDSE KUST NOORD WIND PARK Project.

The following subjects are covered under this document:

- Instructions for operations
- Instructions for maintenance
- Instructions for proof testing
- Instructions for troubleshooting

Note that this document is not meant to supplant the actual Operations and Maintenance Procedure of the facility. It serves only as a guideline to highlight the salient points to be considered in the development of the Operations and Maintenance Procedure which falls under the authority of the Employer

2.1 REFERENCES

2.1.1 Project Reference Documents

Doc. No.	Description
K559-2254-IC-SPE-001	System specification for Main Automation Contractor
K559-2254-IC-PHI-001	Control System Philosophy
1724000594-IN-DD-00015	System Architecture
1724000594-IN-LIS-00003	Bill of Material
1724000594-IN-LIS-00004	PCS and Safety System IO List (HW and SW)
1724000594-IN-LIS-00005	EMCS IO List (HW and SW)
1724000594-IN-CA-00006	Power Consumption and Heat Dissipation
1724000594-IN-LIS-00007	Systems Cables List
1724000594-IN-RE-00008	Safety Controller loading estimation
1724000594-IN-DA-00009	PCS CABINETS GENERAL ARRANGEMENT DRAWINGS AND INTERNAL LAYOUT
1724000594-IN-DA-00010	SAFETY SYSTEMS CABINETS (SIS AND FGS) GENERAL ARRANGEMENT DRAWINGS AND INTERNAL LAYOUT
1724000594-IN-DA-00011	NETWORK AND SERVER CABINETS IN ITER ROOM GENERAL ARRANGEMENT DRAWINGS AND INTERNAL LAYOUT

1724000594-IN-DA-00012	NETWORK AND SERVER CABINETS IN OER ROOM GENERAL ARRANGEMENT DRAWINGS AND INTERNAL LAYOUT
1724000594-IN-DG-00016	Network Connection Diagram
1724000594-IN-DG-00020	PCS CABINETS WIRING DIAGRAMS AND TERMINAL STRIPS
1724000594-IN-DG-00021	SAFETY SYSTEMS CABINETS (SIS AND FGS) WIRING DIAGRAMS AND TERMINAL STRIPS
1724000594-IN-DG-00022	NETWORK AND SERVER CABINETS IN ITER ROOM WIRING DIAGRAMS AND TERMINAL STRIPS
1724000594-IN-DG-00023	NETWORK AND SERVER CABINETS IN OER ROOM WIRING DIAGRAMS AND TERMINAL STRIPS
1724000594-QC-PRO-00030	HW FACTORY ACCEPTANCE TEST (FAT) PROCEDURE

Table 1 – Project Reference Documents

2.1.2 Yokogawa Reference Document

Doc. No.	Description
IM 32P01B10-01EN	ProSafe-RS User's Guide
IM 32P01C10-01EN	Engineering Guide Vol.1
IM 32P01C20-01EN	Engineering Guide Vol.2
IM 32P01C50-01EN	Installation Guide
IM 32P01C60-01EN	License Management Guide
IM 32P01C70-01EN	ProSafe-RS Security Guide
IM 32P01S10-01EN	Safety Manual
IM 32P02B10-01EN	Messages Reference Manual
IM 32P04B10-01EN	Engineer's Reference Manual
IM 32P06C10-01EN	Hardware User's Guide
GS 36K01A10-01EN	Collaborative Information Server
GS 33J60E10-01EN	Field Node Unit, Duplexed Field Node Unit (for FIO, 19-inch Rack Mountable Type)
GS 33J60F20-01EN	ESB Bus Node Units (for N-IO/FIO)
GS 33J60E50-01EN	ESB Bus Coupler Module (for N-IO/FIO, 1-Port)
GS 33J60J10-01EN	Cables (for FIO)

GS 33J60G11-01EN	Ethernet Communication Module (for N-IO/FIO)
GS 33J60G90-01EN	PROFINET Communication Module (for N-IO/FIO)
GS 33J60F60-01EN	Analog I/O Modules (for FIO)
GS 33J60F70-01EN	Digital I/O Modules (for FIO)
GS 33J60H51-01EN	Terminal Boards (for FIO)
GS 33J50C10-01EN	Vnet/IP Interface Card
GS 32P06D10-01EN	ProSafe-RS Safety Node Unit, Duplexed Safety Node Unit (for N-IO/FIO, Rack Mountable Type)
GS 32Q06K10-31E	ProSafe-RS Safety Node Unit (Rack Mountable Type)
GS 32Q06L11-31E	ProSafe-RS ESB Bus Coupler Module
GS 32Q06K30-31E	ProSafe-RS Analog I/O Modules (for FIO)
GS 32Q06K40-31E	ProSafe-RS Digital I/O Modules (for FIO)
GS 32Q06M10-31E	ProSafe-RS/ProSafe-RS Lite Cable
GS 32Q06L20-31E	ProSafe-RS/ProSafe-RS Lite Terminal Boards/Relay Boards
TI 32P01A10-01EN	Safety Instrumented System ProSafe-RS System Overview
TI 32P01J10-01EN	ProSafe-RS Installation Guidance
TI 33Y01B30-01E	Security Standard of System Product

Table 2 – Yokogawa Reference Documents.

2.2 ORDER OF PRECEDENCE

The approved MAC Document Deliverables developed based on the various requirements in the order of priority listed below, this shall be the reference document for all further engineering, manufacturing, FAT and SAT:

1. European directives and supporting standards
2. Dutch legislation
3. End User Technical Standards
4. Referenced Dutch standards
5. Referenced European and International standards
6. Engineering Contractor Standards
7. Project specifications.

If lower-level requirement is more stringent than upper one in the above documents, a request shall be raised to OWNER for written decision before proceeding with the Design, Manufacture or Construction.

2.3 DEFINITIONS AND ABBREVIATIONS

PROJECT:	HOLLANDSE KUST NOORD WIND PARK PROJECT
CONTRACTOR (CTR):	ROSETTI MARINO S.p.A.
COMPANY or Client (CPY):	CROSSWIND
VENDOR	YOKOGAWA ITALIA S.R.L.

Table 3 – Definitions

Doc. No.	Description
ALARP	As Low as Reasonably Possible
AMS	Alarm Management System
ATEX	Appareils destinés à être utilisés en ATmosphères Explosibles (Equipment intended for use in explosive atmospheres)
BESS	Battery Energy Storage System
BLPH	Base Load Power Hub
CAP	Critical Action Panel
CAPEX	Capital Expenditure
CAT	Category
CCN	Central Control Network
CCR	Central Control Room
CCS	Central Control System
CCTV	Closed Circuit Television
COMPANY	Crosswind
CONTRACTOR (CTR)	ROSETTI MARINO S.p.A.
DEM	Design Engineering Manual
DEP	Design and Engineering Practice
DMZ	Demilitarised-Zone
DOCUMENT NAME	Document Title
EMC	Electromagnetic Compatibility

EN	Engineering Notice
EPC	Engineering Procurement Construction
EPIRB	Emergency Position Indicating Radio Beacon
EWS	Engineering Workstation
Ex	Explosion Proof
FC	Fuel Cell
FCS	Field Control Station
FEED	Front End Engineering Design
FEED CONTRACTOR	Organisation contracted directly by COMPANY to provide engineering, design, or other services.
FGS	Fire & Gas System
FIO	Field Input/Output
FNU	Field Node Unit
FO	Fibre Optic
FOPP	Fibre Optic Patch Panel
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positional Satellite
HART	Highway Addressable Remote Transducer
HAZOP	Hazardous Operability Study
HKN	Hollandse Kust Noord
HMI	Human Machine Interface
HV	High Voltage
HVAC	Heating, Ventilation and Air Conditioning
HV-SCADA	The given name for the COMPANY's control system fwind farm infrastructure. BLPH's control system shautonomously but will interface with HV-SCADA.
IACS	Industrial Automation and Control Systems
IAMS	Instrument Asset Management System
ICSS	Integrated Control and Safety System
IDCS	Intrusion Detection Control System
IEC	International Electrotechnical Commission
IP	Ingress Protection

IP	Internet Protocol
IS	Intrinsically Safe
ISO	International Organization for Standardization
ITER	Instrument & Telecoms Equipment Room
LACS	Local Access Control System
LAN	Local Area Network
LOPA	Layers of Protection Analysis
LHVS	Land High Voltage Station
LV	Low Voltage
MAC	Main Automation Contractor, ABB AS
MCC	Motor Control Centre
NAMUR	Interessengemeinschaft Automatisierungstechnik der Prozessindustrie (User Association of Automation Technology in Process Industries)
NIS	Non-Intrinsically Safe
NU	Node Unit
OHVS	Offshore High Voltage Station
OPC	Open Platform Communications
OWS	Operator Workstation
PAGA	Public Address and General Alarm
P&ID	Piping and Instrument Diagram
PACO	Process, Automation, Control and Optimisation (PACO) is the term used to describe all functionality required for the monitoring and controlling of all process, safety and fire and gas systems selected for the project.
PCN	Process Control Network
PROJECT	HOLLANDSE KUST NOORD WIND PARK Project
PURCHASER	The organisation placed a purchase order for the supply of equipment or services for the Project. The Purchaser could be the Company or the Contractor or some other party appointed by the COMPANY or Contractor.
RVO	Rijksdienst voor ondernemend Nederland – The Netherlands Enterprise Agency

SCADA	Supervisory Control and Data Acquisition
SGSI	Shell Global Solutions International
SHALL	An absolute requirement.
SHOULD	This word indicates a recommendation that whilst preferred may not be implemented provided some equivalent is proposed and agreed by COMPANY. The full implications must be understood and carefully weighed before choosing a different course.
SIF	Safety Instrumented Function
SIL	Safety Instrumented Level
SIS	Safety Instrumented System
SNU	Safety Node Unit
TB	Terminal Board
TQ	Technical Query
UHF	Ultra-High Frequency
UPS	Uninterruptible Power Supply
VENDOR	Manufacturer/Supplier of equipment and services to perform the duties specified by the Purchaser.
VLAN	Virtual Local Area Network
VNET	Virtual Network
WAN	Wide Area Network

Table 4 – Abbreviations

3 GENERAL INSTRUCTIONS

This section describes the general instructions for operation and maintenance of the Safety Instrument system (SIS/F&G). supplied for the HOLLANDSE KUST NOORD WIND PART Project.

- "Operations" involve guidelines for the user to evolve procedures for normal operations of the plant and systems. This includes Trip Reset, MOS, Start-up bypass, Emergency operation, Security, Forcing and Monitoring. Refer Sec.5 of this document for more information.
- The "Maintenance" activities can be classified as Preventive Maintenance and Corrective Maintenance.
  - Within Preventive Maintenance, one can distinguish the actions that can be done without disturbing the process (without restrictions), so called "First line Maintenance" and maintenance that will certainly disturb the process or bear a great risk to do so, called "Shutdown Maintenance". Refer Sec.6 of this document for more information.
  - Corrective Maintenance implies the replacement of the defective part, which failed and/or caused a nuisance trip. Due to the unpredictable nature of this type of maintenance this document does not cover this in great depth, but to aid with corrective maintenance a section Troubleshooting has been introduced.
- It is the responsibility of the End-User to ensure that adequate Proof testing is duly carried out throughout the lifetime of the system / facility as per the Proof test interval stipulated in the SIL calculation (if applicable). Yokogawa can assist with proof testing procedures with the end user. Physical installation of equipment in testing shall be by the end user. Refer Sec.7 of this document for more information.
- It is the responsibility of the End-User to ensure that the plant Operations and Maintenance Procedure is kept up to date to reflect the actual status of the Safety System for all "Modifications" implemented at any given time.

3.1 SYSTEMS INVOLVED

System comprises of the following equipment:

- ProSafe-RS System cabinet(s)
- Associated FIO cabinets
- Safety Engineering Workstation (EWS)
- Sequence of Event Viewer

3.2 PREREQUISITES

- All maintenance activities for the Yokogawa safety system must be in line with the regulations of IEC-61508.

- It is to be noted that the responsibility to set up the necessary procedures for operation and maintenance rests with the end user.
- The personnel responsible for the operation and maintenance activities must be competent with the system and project documentation.
- It is the responsibility of the maintenance personnel to refer to the appropriate sections in the manual and to read and understand the requirements before performing the actual maintenance activities.
- During maintenance, put up wrist strap for SIS (Electrostatic Discharge) measures (If applicable).
- There should be a periodic safety check for the system alarms, SOE messages and CPU modes (running or waiting).

3.3 PERSONAL COMPETENCY

As per requirements of IEC-61508, all personnel involved in safety life cycle activities must be competent including product training. Competency must be evaluated and documented before a person is involved in a Safety Lifecycle task. Competency records must be maintained for as long as individual remains involved in a Safety Lifecycle task.

4 SYSTEM POWER-UP

The power supplies that must be available for the system are:

System power supplies:

- SIS : 230 VAC UPS (AC UPS PAS, Line A and Line B) with autonomy of 30 min
- F&G : 230 VAC UPS (AC UPS F&G, Line A and Line B) with autonomy of Full Operation: 8 Hour

Utility power supply:

- One 230 VAC 50Hz

The utility power supply will be used to feed the following equipment per cabinet

- Cabinet fans
- Utility sockets
- Cabinet lighting

The starting point for system power up is:

- All power cables connected.
- All field cables connected (If available during the system start-up).
- All grounding cables connected.
- All interface cables to other systems connected (If available during the system start-up).
- All main switches and circuit breakers switched OFF.

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

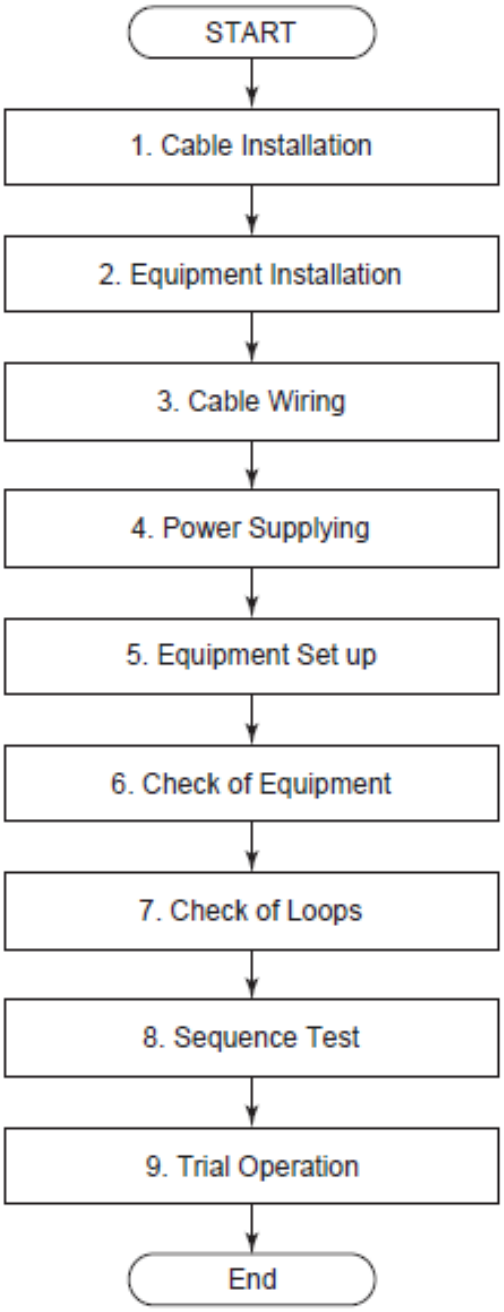


Figure 4 – Start-up

5 OPERATIONS

Operational requirements are defined by the End-user. Normally this will be included in the overall plant operation procedures and manuals. The following paragraphs will provide brief details on the operating procedures of the SIS & FGS. The main functions that are executed by the operator are:

- Trip Reset
- Input Device Maintenance Override
- Start-up Override
- Emergency Operation
- Forcing
- Security
- Operator interfaces and system monitoring

5.1 TRIP RESET

SIS / FGS logic is designed such that if it is de-energized / energised for any reason, it can only be reset or re-energized by deliberate, momentary actuation of a reset button activated at OWS along with a sequence of event log. The SIS / FGS logic can only be reset after the hazardous demand is no longer present. In the case of trip, the operator would be required to reset the highest shutdown Hierarchy first to the lowest. This is only possible when the trip conditions are healthy again. However, in some cases, the operator needs to reset the UZ Group first before being able to reset the individual valve trip.

5.2 MAINTENANCE OVERRIDE

Throughout the operational lifetime of the SIS/FGS, overrides for sensors and other input devices are required from time to time. Maintenance override switches (MOS) shall be used to inhibit trip initiators to enable maintenance or on-line functional testing. For safety reasons, these maintenance overrides shall be allowed for input signals only and not for output signals. Maintenance overrides should not prevent actual input status from being alarmed.

As a MOS effectively renders its associated safety instrumented function (SIF) ineffectual in the event of a hazardous demand (i.e. bypassed), their use shall be strictly governed by review and Contractor's operational procedures (permit to work system) including securing the soft keys from unauthorized access.

The following by-pass and override facilities shall be provided. Two different override functions shall be available:

- Operation Override Switch (OOS)
- Maintenance Override Switch (MOS)

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

5.2.1 MOS Monitoring

The presence of active MOS monitoring is described as below:

- Activation of 'MOS' enable switch shall be communicated to OWS graphic display. Upon detection of a transition to 'MOS' switch enabled state, an alarm shall be generated on OWS & recorded in SOE.
- Each trip initiator's MOS status is indicated on graphics.
- Each trip initiator's MOS status is recorded in SOE.
- If any bypass / MOS action is performed, a common "Maintenance Override "alarm with high priority shall be displayed on OWS graphics displays.

CAUTION

The MOS function is not meant for use during normal operation.

During normal operation, all 'MOS' must be removed after the necessary maintenance works have been completed.

It is the responsibility of the Employer to ensure this is strictly followed throughout the operational lifetime of the facility and is duly incorporated into the plant operations and maintenance manual / procedures.

5.2.2 MOS Activation

The steps involved in activation of new MOS at OWS is described as below:

- Turn associated 'MOS' enable key switch to 'Enable' position.
- Apply 'MOS' to a trip initiator at OWS MOS graphic.

5.2.3 MOS Removal

The MOS condition can be removed either by disabling the respective CAP MOS enable key switch or by individually removing the MOS of each trip initiators from the OWS.

5.2.4 Emergency MOS Removal

On total failure of the OWS & communication, all active MOS's can be removed by pre-determined logic. MOS active status can be observed from the MOS status lamp on the auxiliary panel.

5.2.5 Active MOS Monitoring

The presence of active MOS monitoring is described as below:

- Activation of 'MOS' enable switch shall be communicated to OWS graphic display. Upon detection of a transition to 'MOS' switch enabled state, an alarm shall be generated on OWS & recorded in SOE.
- Each trip initiator's MOS status is indicated on graphics.
- Each trip initiator's MOS status is recorded in SOE.
- If any bypass / MOS action is performed, a common "Maintenance Override "alarm with high priority shall be displayed on OWS graphics displays.

5.3 START-UP OVERRIDE

Start-Up Inhibit is used during Plant Start-Up. When the soft button is pressed in OWS, The Low-Low Alarm will be bypassed to facilitate plant start-up. The procedure for applying a start-up inhibit of SIS system, which is located on the OWS, is as follow:

- When operating the start-up inhibit switch from the OWS, the low-low trip will be bypass.
- Deactivation of the start-up inhibit is either by manual from OWS console, or when a predefine deactivation timer has been reached or when a predefined process value has been reached for a predefined time.

5.3.1 Start-up Override Monitoring

The presence of active Start-Up override monitoring is described as below

Each Start-Up override active status, start-up bypass elapsed (duration) timer shall be monitored in OWS graphics and Process alarm summary. Refer to actual graphic design.

5.4 EQUIPMENT FAILURE HANDLING

It is required to plan the operation procedure beforehand for possible equipment failure.

For Emergency procedures below, refer section. 2.1.2 in this document.

Operation flow during the error occurrence - Engineering Guide Vol.1- IM 32P01C10-01EN.

Operations and recovery procedures during the SCS error occurrence

- Actions taken at Fatal error occurrence and recovery procedure.
- Actions taken at Major error occurrence and recovery procedure.
- Actions taken at Minor error occurrence and recovery procedure.

5.5 VALVE TRIP FACILITY

Blow down valve:

SIS interlock reset, shall be the permissive for the respective.

BDV faceplate having close switch to manually close the BDV valve, during shutdown condition,

BDV close switch on the faceplate shall not be accessible.

Shut down valve:

SDV interlock reset, shall be the permissive for the respective

SDV faceplate having open switch to manually open the SDV valve, during shutdown condition,

SDV open switch on the faceplate shall not be accessible.

5.6 INTERFACES AND SYSTEM MONITORING

The system provides the following interfaces:

- Critical Action Panel (CAP)
- System status on OWS
- System status on EWS
- LED indications on modules

5.6.1 Critical Action Panel (CAP)

A Critical Action Panel (CAP) shall be software-based control located at CCR for SIS and FGS functions. A dedicated tower type PC and screen with installed CI view/License software shall be used to control the action push buttons and monitor the trip status information.

5.6.2 System Status on OWS

The System Status Overview window display the operating mode, scans period and security level along with the operating status and connection status of CPU and I/O modules.

The System Alarm window displays a list of diagnostic information messages that notify hardware, software, and communication errors in the system as system alarm messages.

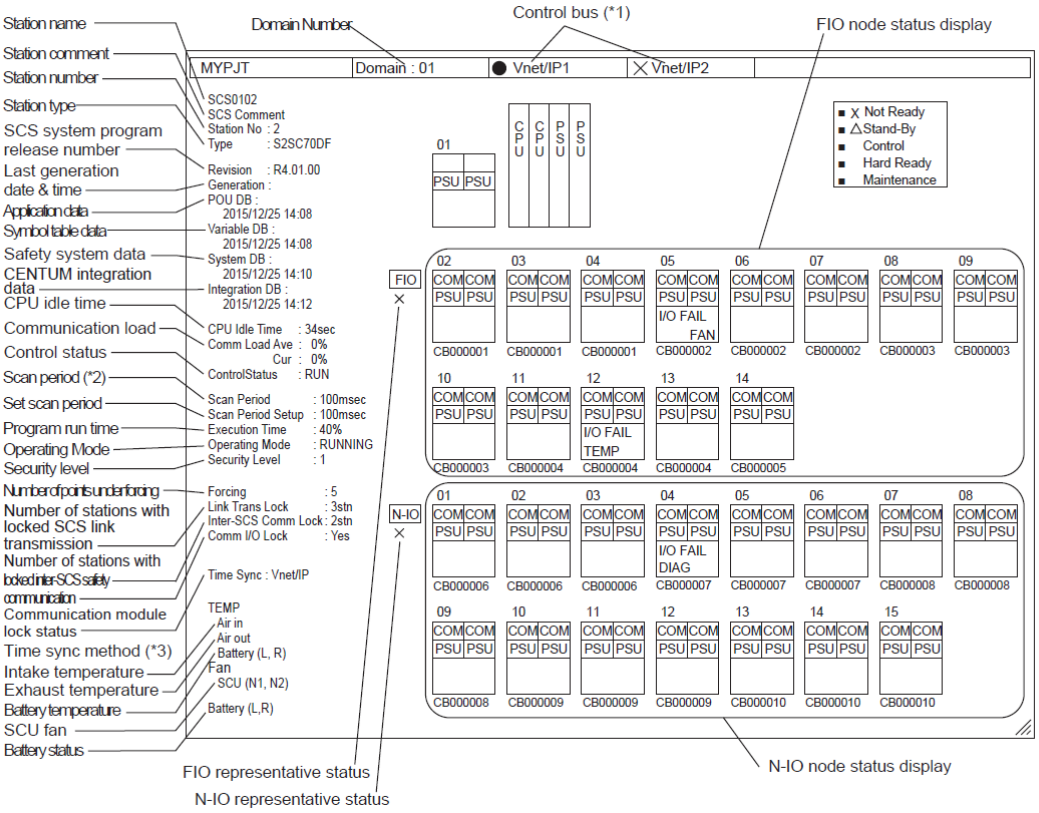


Figure 5 – System Status on OWS

5.6.3 System Status on EWS

The SCS Status Overview window displays a list of SCSs assigned to the given ProSafe-RS project. In addition to the current operating conditions of SCSs, it also displays if there is any diagnostic information message from any of the SCS diagnostic functions; it is easy to know which SCS has errors.

The SCS State Management window displays detailed information about the operating status of CPU modules and input/output modules for a single SCS. If there is an error, the erroneous area is shown using a different colour. It also displays whether there are any messages that have not been acknowledged.

The SCS State Management window allows the user to perform the following operations:

- IOM Download operation, Output Enable Operation and Start Output Module operation
- Display of detailed information of each input/output module.

5.6.4 LED Indication on modules

For health status of module, the following LEDs will be lit:

- Node Power Supplies – SYS and FLD
- Active Controller – SYNC, SCTY, HRDY, RDY, and CTRL
- Standby Controller – SYNC, SCTY, HRDY and RDY
- Active I/O Module – STATUS, ACT and DX
- Standby I/O Module – STATUS and DX

Refer Sec.8.3 for ProSafe-RS system module LED status details

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

6 MAINTENANCE

Maintenance is required to:

- Ensure the lifetime of the system.
- Maintain and detect dormant.
- Correct failures
- Keep the system up to date by updating system software and system documentation.

For the maintenance activities in general, a distinction is made between Preventive and Corrective Maintenance. (Most actions are covered when a Yokogawa maintenance contract is applicable)

6.1 PREREQUISITES

Test equipment, required for maintenance:

{This list of equipment contains the tools needed for the maintenance of the System cabinet. The tools needed for the maintenance of the valves / solenoids and the pressure transmitters should be listed in their respective documentation. If not, these tools should be added to the list here (for example pressure generator with indication}

- Clamp-on current probe
- Multimeter
- Hand tools
- Oscilloscope
- HART Handheld terminal

Note: All measurements must be performed with calibrated tools.

6.2 RECOMMENDATIONS FOR THE END USER

As indicated in the Safety Validation Plan, Yokogawa prefers an approach to safety based on the standards IEC 61508 and 61511. The safety lifecycle in which all activities which are relevant for the safety during the lifetime of the installation (hence during the engineering and construction phase, as well as during commissioning and operation, including maintenance and testing) are planned and performed according to these plans. Also, the activities should be recorded, so that they are traceable.

During the engineering and construction phases of the project Yokogawa adheres to these standards and therefore Yokogawa advises to follow the same approach during the operational life of the system.

On top of that it is required that a Proof test is performed at the intervals as specified in the reliability calculations of the Safety Validation Plan to maintain the required Safety Integrity level (SIL) for the safety loops.

A feasible approach could be the following.

- The assignment of a system custodian to co-ordinate all activities and gather all facts and reports with respect to the system.
- The installation of a system binder which contains all data (like reports of the executed maintenance and loop tests) with respect to the system.
- A maintenance planning to plan ahead for the maintenance activities over the year. Since some activities are likely to disturb the process, these should be scheduled together with a scheduled shutdown of the process. The planning of the loop tests can be combined with the maintenance planning.
- It is essential to log any system anomalies into a system logbook. This logbook typically resides close to the system or with the operators. Before executing the scheduled maintenance, the logbook must be studied to see if there are any follow-up actions.
- The system documentation (Cabinet drawings, functional block diagrams, Loop drawings, cable termination etc.) must be stored in the vicinity of the system for quick access.
- Care must be taken that every modification to the system is marked up in the site master copy of the system documentation. Any mark-ups on system drawings must be processed into revised "as built" drawings. As a minimum the drawings must be inspected on a yearly basis to verify whether updates are required.
- For every modification it must be considered if SIL loops are affected, and Safety Integrity can be guaranteed. The SVP update procedure must be followed if applicable.
- Sufficient maintenance spares must be stored on site.

6.3 PREVENTIVE MAINTENANCE

Preventive maintenance must be carried out on a regular basis to ensure an operational system that meets the requirements as specified by the contractor and / or the end user.

It is recommended to base the ProSafe-RS maintenance schedule for preventive maintenance intervals with reference to ProSafe-RS instruction manuals. A Safety Control Unit and Safety Node Unit include parts having defined life spans, which require periodical replacement.

Refer sec. 2.1.2 for recommended replacement intervals for ProSafe-RS related components - Hardware User's Guide - IM 32P06C10-01.

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Component	Part number	Recommended replacement period	Replacement by user	Remarks
Power supply module (230VAC)	SPW482	8 years	no	
Battery pack	S9185FA	3 years	yes	Average ambient temperature of 30 C or less
		1.5 years	yes	Average ambient temperature of 40 C or less
		9 months	yes	Average ambient temperature of 50 C or less

Table 5 – Life spans for Parts of Safety Control and Node Units.

The maintenance schedule shall include 'maintenance intervals' for peripherals like workstation (EWS), cabinet fans, ventilation louvers, termination board alarms, printers, relay`s, Barriers, PSU`s, network switches & alarm devices etc. Since these components need some regular attention to ensure their lifetime and prevent failures.

It is recommended to base the maintenance intervals based on respective component instruction manuals.

6.4 FIRST LINE MAINTENANCE

The Purpose of first line maintenance is to:

- Detect dormant faults in the system, which are not detected during normal operation.
- Minimize the probability of occurrence of faults / failures from affecting the normal operations.

6.4.1 ProSafe-RS System

The ProSafe-RS system is self-testing (built in diagnostics), due to the fail-safe nature of the cards, i.e., that a failure at any point of the system will cause a trip and thus the operator is warned.

During maintenance undetected defects can be found but could only be non-safety related due to the fail-safe nature of the ProSafe-RS system. They may however have a degrading effect on the system availability due to an increase in nuisance actions.

Refer sec. 2.1.2 for procedures and precautions when maintaining ProSafe-RS devices and field devices - Engineering Guide Vol.1- IM 32P01C10-01EN.

Outputs enable:

When an output channel goes to fault, a channel fault alarm is generated, and the CPU mode changes from 'running' to 'waiting'.

In the event where the outputs (digital output, analogy output) are disabled due to channel fault / failure, the output enable operation needs to be performed upon recovery from the fault. (e.g.: after output card replacement, final element replacement or line fault recovery). This can be performed via EWS.

Refer sec. 2.1.2 of this document for output function in the event of initial power or start-up of controller (cold start) - Engineering Guide Vol.1- IM 32P01C10-01EN,

The system and process alarms are issued upon online diagnostics of any fault in the I/O channel depending on the I/O parameter configuration where the settings are enabled for detection. The outputs are disabled if any fault is detected in the output channel.

The channel fault alarms shall be 'continuously' monitored and attended by plant operation and maintenance team. Upon recovery of output channel fault, it is the plant operational / maintenance responsibility in carrying output reset (output enable) function at engineering station.

I/O Module Handling:

Handling of I/O modules and its connections during maintenance shall be performed cautiously in a simplex configuration to avoid 'spurious' trip.

Online Replacement of Modules:

When system is in operation, if it is necessary to install or remove the modules, cables, connectors, Refer sec. 2.1.2 of this document, which explain how to remove or install the common modules of the Safety Control Unit -Hardware User's Guide - IM 32P06C10-01.

The dual-redundantly configured modules (such as PSU, CPU, ESB Modules) can be removed and installed one by one without turning off the power supply to the safety control unit. The detailed procedures for the following modules are explained therein:

- Power Supply Module
- Processor Module
- ESB Bus Coupler Module
- ESB Module

6.4.2 Power Supply

Measure the voltage on the 24 Volts DC power supply units. Ensure the output of Power supply units is within voltage range specified in the label of the equipment, related documentation, and design setting.

For proper operation of the I/O module, the voltage setting must be as listed below:

- DC operating voltage for I/O module: 24VDC +20% and -10%
- DC operating voltage for safety relay: 24VDC +15% and -10%
- DC output voltage design setting at DC PSU: 22.6 to 28.8VDC
- The design output voltage setting at DC PSU is 22.6 to 28.8V DC considering the voltage drop between PSU output and system / marshalling cabinet wiring field output. This voltage setting is also labelled on the PSU equipment for reference during maintenance.
- DC Voltage (the measurement point is at 24VDC power distribution terminal in each cabinet. Refer to the cabinet drawing for details): 24VDC +20% and -10%
- Use the Cabinet Electrical drawings (refer to respective cabinet drawings) to determine the test points.

Power supply check is advised to be carried out at a frequency as per plant maintenance schedule.

6.4.3 Environmental Conditions

Refer sec. 2.1.2 to document ProSafe-RS installation guidance (TI 32P01J10-01EN) for the Environmental conditions of supplied products for the project. Refer sec 6.4.1

6.4.4 Cleaning

Accumulation of dirt and dust prevents efficient heat dissipation and may cause system failure or equipment breakdown. Cleaning involves brushing or vacuuming to restore cooling efficiency that may have been degraded by accumulated dust.

When cleaning electrical components these components must be isolated from the power supply or must be shut down before cleaning. If this action will certainly disturb the process or bear a great risk doing so, then this activity should be carried out during shutdown maintenance, see Sec.6.5.3. Be careful not to disturb wiring and jumpers on associated hardware.

Clean PC screens with a soft cloth lightly moistened with a mild detergent solution. Do not use any type of abrasive pad, scouring powder or solvent, such as alcohol or benzene. Do not rub, touch, or tap the surface of the screen with sharp or abrasive items, like a ball point pen or a screwdriver. Otherwise, this can result in damages to the screen.

Cleaning is to be carried out as soon as dust accumulation is noticed; inspect at a frequency of once per month or as per plant maintenance schedule.

6.4.5 Air Filters

Air filters in cabinets, PCs and other equipment must be cleaned or replaced regularly to ensure good air flow.

Cleaning or replacement of air filters is to be carried out as soon as dust accumulation is noticed; inspect as per plant maintenance schedule.

6.4.6 Hazardous Area Equipment

Refer to and comply with precautions and conditions for the maintenance of equipment in hazardous area as stated in the certification conditions. In general, the following precautions shall be observed.

Replacement of Fuse:

- The specified fuse must be used for replacement.
- Before replacing the fuse, confirm if there's no dangerous gas, and the power supply is OFF.

Maintenance:

- The maintenance work should be done only by operators who received special training.
- Before starting the maintenance work, confirm that there is no hazardous gas present.

Modification:

In case of any modification in design and components, the hazardous certification must be reassessed by EPC / Employer.

6.4.7 Spare Parts

The Employer must inspect the system spares on their status or have this done by Yokogawa under the maintenance and support agreement.

It is recommended that parts with damaged packing be returned to Yokogawa for re-test and repacking.

Inspection is advised to be carried out at a frequency of once per year or as per plant maintenance schedule.

6.4.8 Routine checks

Routine maintenance is performed by visually checking the status lamps of the equipment or by checking the SCS State Management window

Refer sec. 2.1.2 to document Hardware User`s Guide (IM 32P06C10-01EN) Section E2 for more details. Check the ProSafe-RS system status on the EWS or OWS system alarm and diagnostics display. Investigate and correct any alarms/ errors.

6.4.9 System Documentation

The system documentation is advised to be stored near the system for quick references. Care must be taken that every modification to the system is marked up in the master copy of the system documentation on site. Any mark-ups on system drawings must be processed into revised "as built" drawings. To be able to track any problem that may have occurred during the preceding operational period it is essential to enter any system discrepancy in a system logbook. The assignment of a system custodian on site is recommended to keep track of the system maintenance history.

Inspect drawings and documents on at a frequency of once per six months to verify if updates are required.

6.4.10 Routine PC Housekeeping

To maintain the PCs in good working order, some basic housekeeping activities are recommended.

SOE Message Cache:

The message cache service function continuously collects the SCS SOE and diagnostic information (due to automatic data acquisition configuration) and saves it as cache file at EWS. All the SCS Controllers are configured for automatic data acquisition at EWS.

Make sure that the disk used for DISK Cache by the Message Cache Service always has enough free space. (Default maximum Disk capacity: 800MB) Monitoring for the Maximum Capacity is performed every 30 seconds. If the disk usage for the disk cache exceeds the Maximum Capacity, oldest files are deleted to keep the usage rate of the disk cache at 98% to 100%.

The cache file is stored for each station. “SOE including Trip” and “Diagnostic Information messages” are stored separately in the cache file. If old cache files are required to be retained, manually save the files in a separate folder or media from the [Save Disk Cache] dialog box. To view the disk cache usage rate, use the Message Cache Tool: click [DISK Cache] in the tree view.

Suggest monitoring the Disk Cache usage rate via the Message Cache Tool as per plant maintenance schedule. On reaching 50%, existing files can be backed up and deleted from the hard disk as part of Housekeeping.

6.4.11 Operation History

Access Control and Operation History Management Software Package is used in each ENG to set the operation rights of engineers who operate the safety engineering PC (ENG), as well as to record the operation history. This package is divided into the Access Control function and Operation History Management function.

Operation History Management:

This function is used to record the operation history of software on ENG. It allows an engineer to view the operation history; for example, who operated what, when, how, and why. The recorded operation history can be used for engineer job handover and troubleshooting and analysis. As modification files accumulate in the operation history database, the amount of free disk space gradually decreases. When the remaining free space almost reaches to the specified free disk space, a dialog box appears to alert low disk space. When the remaining free space becomes lower than the specified free disk space, a dialog box appears to prompt backup and further operations to log the operation history cannot be performed. When an alert dialog box appears, the data backup shall be carried out.

Although the modifications activity of safety instrumented system are carried out on demand basis (not regular), the impact on modification file size insignificant.

Suggest monitoring the 'amount of free disk' where 'Operation History' files are stored on quarterly basis or as per plant maintenance schedule. On reaching 50%, existing files can be backed up and deleted from the hard disk as part of Housekeeping.

6.5 SHUTDOWN MAINTENANCE

6.5.1 ProSafe-RS System

In the event of initial power or start-up of controller (cold start), all the outputs (digital output & safety communication outputs) are disabled by system design. This requires the output to enable operations to be performed after completion of system power up and when the system is ready to go into operation.

6.5.2 System status

First check the system status on the Critical Action Panel, EWS diagnostics tool and PCS system. Investigate and correct any failures e.g., fuse failure, line fault, MCB, PSU & ELM fault etc.

6.5.3 Cleaning

Refer Sec.6.4.4 for 'cleaning' to be carried out during shutdown maintenance

Visual / Mechanical inspection

Mechanical inspection includes the following checks for the ProSafe-RS system:

- Check if the terminals are firmly closed.
- Check if electrical wiring and cables are not trapped and firmly connected to their termination assembly.
- Check for signs of corrosion on connecting parts, terminals, etc.

- Check proper function of door hinges and locks.
- Check connection of Communication cables (ESB bus, ESB bus or optical ESB bus, Vnet/IP, etc.).
- Check ELM alarm.

6.5.4 Field Power Supply Redundancy Check

Power check includes the following checks,

- Check the LED status of the primary/redundant power supply.
- Check the voltage levels of both power supply and make sure the power distribution wiring is connected.
- Switch off primary power supply and conduct the check related to system and I/O.
- Once completed the checks, switch on primary power supply.
- Check the voltage levels of both power supply and follow the same for the secondary power supply.
- Check the current of both power supply and follow the same for the secondary power supply.

6.5.5 Functional check of inputs

Test the inputs by simulating an alarm. The actual status will appear on the OWS.

6.5.6 Functional check of outputs

Outputs can be tested without operating the valves or solenoids by removing/ disconnect the related fuse terminals.

6.5.7 Valves and Solenoids

There are probably no actions other than the Proof test actions. Refer the section 7.2

6.5.8 Pressure Transmitters

If the transmitters are in voted configuration, probably all actions are possible to do “without disturbing the process”.

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as “NOT CONTROLLED” copy

7 PROOF TESTING

7.1 GENERAL

In order to maintain the required safety integrity level for the safety loops, proof tests must be performed at intervals as specified in the reliability calculations in the Safety Validation Plan. The proof test frequency can also be found on the Safety Certificate.

It is the End User's responsibility to execute these proof tests and to record the results if they aim to comply with IEC 61508 / IEC 61511. This proof testing must be performed by a well-trained and skilled engineer.

Note that the following instruction provides typical system proof test information. It can be used by the client to develop their detailed proof testing procedures required to maintain the SIL.

It should be noted that according to IEC-61508 the entire safety loop must be proof tested, from field sensors up to and including the final elements.

In analogy with the Maintenance there are tests that can be done without disturbing the process and there are tests that will disturb the process.

7.2 RECOMMENDATIONS FOR THE END USER

Pre-check:

- Permit(s) to work shall be obtained before starting the Proof test.
- Prior to proof testing, confirm preventive maintenance checks (e.g. power supply limits, redundancy check) for systems separately as per detailed in Sec.6.
- For redundant configuration, manufacturer recommendation of Proof test shall be considered. Logic solver shall be tested for redundant configurations as applicable for the project.
- Ensure prior to proof test ensure the healthiness of the system components and components in the loop without any diagnostics error.

Procedures:

- The design of Proof test procedures shall be based on firm understanding of the SIF architecture including dependencies on other SIF and any other precautions.
- Proof testing shall be performed by a well-trained and skilled engineer.
- Output devices undergoing Proof testing may be de-energized or energized depending on type of output logic and fail-safe configurations. Hence End-user shall generate the isolation philosophy (e.g. energized/de-energized state, voting, override and bypass valves) for each SIF to conduct Proof Test at required intervals.
- It is of vital importance to verify that Proof testing will not cause spurious trips or hazardous situations in the field.
- The end user shall decide method of Proof test (e.g. online, offline etc.) depends on isolation philosophy for selected SIF.

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

- Proof test requirements specified in sensor and final element equipment manual shall be taken into consideration while developing Proof test procedures by End User.
- Manual bypass switches (Maintenance override) for sensor overriding shall be used with caution during functional testing as this will override the action of the safety function. Manual bypass switches shall not be used for disabling shutdown valves from closing during the testing of final elements.
- Locking and forcing of inputs or outputs within the logic system to simulate inputs or activate outputs shall not be considered the equivalent of testing and prohibited from using for testing.
- Calibrated test equipment shall be used during Proof testing.
- Proof test shall include confirming SIF response time.

Sensor:

- Proof testing for sensors shall include alarm, trip, fault conditions (e.g open, short, burnout), deviation for voted condition etc.
- Manual overrides for sensors limit the coverage for proof testing and should not be considered for the test strategy unless adequate proof test coverage and overlaps is ensured by alternate test strategies.
- Proof test shall include testing of auxiliary console components (e.g. push buttons, key switches)

Logic Solver:

- Proof test shall include I/O interfaces components (e.g Isolator/barrier, surge arrestor, interposing relay etc). The manufacturer's safety manual and instruction manuals shall be used to develop proof test procedures considering device specific requirements.
- ProSafe-RS test interval is 10 years.
- In practice, shorter Proof test intervals are sometimes required for the input and output field devices (e.g., every 6 months) than for the ProSafe-RS. Testing the entire safety loop together with a field device automatically includes the test of the ProSafe-RS. End-user shall analyze and establish testing procedures for ProSafe-RS in the aspect of full test coverage requirement for ProSafe-RS alone (e.g application logic)

Final Element:

- Proof test shall include testing of auxiliary console components (e.g., lamps and buzzer).
- Partial Stroke Test (PST) is a complementary testing method to the Full Stroke Test (FST). In essence, the partial stroke test is a testing method whereby a portion of the shutdown valve assembly is tested more frequently than the full test rate. The test involves moving the valve a small percentage ranging from 10% to 30%, which tests a portion of the shutdown valve failure modes. The remainder of the failure modes shall be tested during a full-stroke test.
- For those SIS valves with PST function, when performing the valve PST, limit switch status may not be available for the duration of the test.

- The leakage of the shutdown valves must be tested when this valve is in its closed position.
- Proof testing for final element shall include any open discrepancy test, closed discrepancy test, if designed accordingly.

Result:

The results of Proof testing shall be recorded and maintained for the purposes of periodic reporting, audit, and historical analysis.

7.3 PROOF TEST COVERAGE - STRATEGIES FOR PROOF TESTING

It is end user responsibility to identify pipe to pipe testing strategy or segmented testing strategy for each SIF depending on established test procedures.

7.4 RECORDING SIF ACTIVATION DURING PROCESS DEMAND:

It may be noted that when a SIF is activated as a result of a real process demand, the same can be recorded as a proof test of the SIF.

However, this may not provide complete test coverage (like redundant parts of the system) and therefore these should be covered by proof testing procedure.

7.5 SIS TEST (PROSAFE-RS)

To maintain the ProSafe-RS system in a state of good operational readiness, it is essential that proof tests are carried out at intervals to ensure the proper functioning of the systems and associated field devices.

Complete safety critical loop functions of the SIS with their executive actions (activation of relays, solenoid valves, final elements etc.) must be tested including field input devices and final elements to ensure the SIS is maintained in a state of good operational readiness.

7.5.1 Execution of Proof Test

According to IEC-61508, all Safety Loops (SIF) have to be proof tested.

Proof Test Interval requirement for each plants Logic Solver, Sensors & Final Elements are specified in Customer Specification document (e.g. SRS).

The IEC-61508 requires that the complete safety critical loops are tested, including field input devices (e.g. detectors) and final elements (valves etc.). Field and final element equipment is not in scope of Yokogawa reliability calculations, and may have different proof test requirements (e.g. test intervals).

During proof testing of the ProSafe-RS system, trips might be generated. Therefore, a complete proof test can only be done with precautionary measures during shutdown periods.

7.5.2 Proof Test for ProSafe-RS

A proof test is a periodic test to verify that the functions of safety loops, which consist of a sensor, logic solver and final element, work without fails. The proof test items for logic solvers (ProSafe-RS) are explained below.

The ProSafe-RS has been designed to meet the requirements for PFD of SIL 3 that are defined as a fraction of 10-4 to 10-3 in the IEC 61508, with the condition that the interval between proof tests is 10 years.

Checking the Channels of Input / Output Modules:

Change the input value or output value of each channel of the modules and check if the modules work as intended. For dual-redundant modules, check on both modules.

I/O channels are tested as part of SIF proof testing procedures either pipe to pipe test or segmented testing methods.

I/O channel values shall be monitored in safety engineering station maintenance tool (IO lock window, application logic level) and/or operator interfaces (faceplate).

Control Right Switch Over (for Redundant CPU Modules and Input / Output Modules):

To ensure high availability, use the following procedures to check that switch overtakes place properly on dual-redundant modules.

Input/output Modules

Use the IOM Control Right Switching Tool to make switch over on AIO/DIO modules. This tool switches the control right of dual-redundant AIO/DIO modules from the ENG. By using this tool, the control right will be switched over to the modules on the standby side.

It is not recommended to remove the cables or terminal blocks from the active modules for this test so to avoid human mishandling.

Refer Sec. 2.1.2 on the use of the IOM Control Right Switching Tool.

Do not remove and put back the applicable AIO/DIO module while automatic IOM download is being executed, which will lead to module failure. The resolution is to perform manual IOM download at engineering station and then remove and reinsert the module after the completion.

CAUTION

Output devices undergoing proof testing may be de-energized or energized depending on type of output logic and fail-safe configurations. The default design of the SIS outputs are de-energized to safe unless otherwise specific design in a system.

Hence it is of vital importance to verify that this will not cause spurious trips or hazardous situations in the field. If necessary, isolate outputs to the field. The Employer is responsible for necessary procedures and actions to ensure safety.

CPU Modules

To make a switch over, press the START/STOP switch in the front of the control-side CPU Module to stop it. Press the START/STOP switch of the failed module once again to restart it. The module should start up as a standby side.

Do not pull out the CPU module online and turn off the power while the module is writing to the flash memory. Whether the CPU module is wiring can be confirmed by using LED of the CPU module. Ensure 'Vnet/IP' bus cables are always connected either removing or inserting the processor module online.

8 TROUBLE SHOOTING

The ProSafe-RS Safety Control Station (SCS) performs self-diagnosis regularly to detect hardware and software errors. It analyses detected errors and system configuration to determine the error level according to the error occurred and executes error-handling operations according to the error level.

The diagnostic management function saves/manages diagnostic information messages generated by self-diagnosis and manages the SCS status. Moreover, it notifies the operation status of the SCS to the EWS and OWS.

8.1 GENERAL

When an output trips to an (apparent) nuisance failure or when it is not possible to get the system healthy after a shutdown, the following actions can be taken to trace and solve the fault:

1. Verify on SOER which event caused the trip.
2. Verify the system diagnostics report for any error reported
3. Collect all relevant drawings related to the trip and verify that they reflect the as-built system status.
4. Verify that all inputs are in a healthy state.
5. Apply overrides on unhealthy inputs.
6. Reset the system in a hierarchical way.
7. If the fault is still present, verify if reset commands are received by checking the LED's in front of the module.
8. If the system still has not recovered find the improperly functioning module by using the termination drawings. Refer to the IO Database - SIS / F&G document for relevant section listed in Refer Sec. 2.1.2 for more detailed information.
9. Replace the card malfunctioning by another of the same type and start from step 6.

8.2 TROUBLE SHOOTING FACILITIES.

The system is provided with the following tools to find a defective part in the system:

- OWS to monitor SIS status.
- EWS to monitor system status.
- LED indications on modules.
- Inputs override facilities.
- LED Indication on Power supply modules and ELM
- LED Indication on Relay & Barrier.
- Test/disconnect terminals.

8.3 LED INDICATIONS ON PROSAFE-RS MODULES

All ProSafe-RS modules in the system are provided with LED indications. Refer Sec. 2.1.2 document Hardware User`s Guide (IM 32P06C10-01EN) for detailed information regarding the status of each LED.

8.4 EWS/OWS DIAGNOSTICS MANAGEMENT

The diagnostic management function notifies SCS diagnostic information (the diagnostic information messages and error notifications to the application logic corresponding to different levels of errors that may generate in the SCS) in response to requests from windows that handle diagnostic information. This allows checking and manipulating the information from the EWS and OWS.

"State Management Window" provides complete display of ProSafe-RS system status, faults, alarms etc in addition to comprehensive diagnostic information. Also, the software logic, IO and variable values can be monitored on-line by using "Debug" function of the Workbench software

For details regarding diagnostic messages, Refer Sec. 2.1.2 Messages Reference Manual (IM 32P02B10-01) for IOM Module Troubleshoot

This section explains the procedure for ProSafe-RS SCS I/O module failure.

If a problem occurs on I/O module, confirm the error code in the alarm message that is displayed on EWS and OWS. The Error message number is the same for EWS's Diagnostic Information Message and PCS OWS System Alarm Message. For details regarding diagnostic messages, Refer Sec. 2.1.2 for diagnostic Messages Reference Manual (IM 32P02B10-01).

The following information may be required by Yokogawa experts for further analysis of the fault occurred.

8.4.1 IOM Report

SCS Maintenance Support Tool has IOM Report Window that displays the I/O module status in detail. Diagnostic Information Message indicates the node number, slot number and channel number in the message, but the cause of the error is not displayed. IOM report has more detailed information that includes the cause of errors such as short-circuit or open circuit.

IOM report is the most useful information to make investigation. IOM Report Window of EWS has "File" button to save the IOM Report information to a text file. Make the IOM Report text file as follows:

- Save the IOM report text file during the I/O module is failed.
- If the IOM has recovered already, the information saved in IOM report becomes smaller. However, even if the IOM has recovered, make the IOM Report text file anyway.
- In case of the dual redundant configuration, make IOM Report text file for both of Active and Standby modules respectively even though one is in fail and the other one is in operation.

8.4.2 Report from SOE viewer

SOE Viewer has a function to save the SCS log to a CSV file.

- Make sure the Diagnostic Information Message of the failure is included in the SOE log.
- Make sure that the log includes as many events and alarms (Diagnostic Information Message) before and after the failure as possible.

8.4.3 I/O Parameter Settings

I/O module parameter and I/O channel parameter are required to make investigation sometimes. On EWS, I/O Parameter Builder can export CSV file that contains the I/O parameter for all I/O modules of the SCS.

The following procedures detail the export operation:

- Invoke I/O Parameter Builder.
- From File menu, File => External File => Export.
- Export dialogue box appears, then specify the file name, and save the CSV file.

8.5 OVERRIDES

For using overrides refer to section 5.2.

8.6 TEST / DISCONNECT TERMINALS

Each channel of the base plate is equipped with a disconnecting terminal to disconnect

the I/O module from the field terminal and allow for field loop testing. In the case of IS Signals, field connection to be disconnected from Barrier baseplate.

Refer to the documents listed below for more detailed information

- Typical Loop Drawing - SIS/F&G
- Respective Process area IO Database - SIS / F&G document

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

9 ATTACHMENTS

Following are the Safety system hardware components used in BLPH HOLLANDSE KUST NOORD WIND PARK Project.

Attachment no	Model	Description	IM/GS Reference
9.1	-	ProSafe-RS User Guide	IM32P01B10-01EN
9.2	-	Engg Guide Vol-1	IM32P01C10-01EN
9.3	-	Engg Guide Vol-2	IM32P01C20-01EN
9.4	-	Installation Guide	IM32P01C50-01EN
9.5	-	License Management Guide	IM32P01C60-01EN
9.6	-	ProSafe-RS Security Guide	IM32P01C70-01EN
9.7	-	Safety Manual	IM32P01S10-01EN
9.8	-	Message Reference Manual	IM32P02B10-01EN
9.9	-	Engg Reference Manual	IM32P04B10-01EN
9.10	-	Test Function Guide	IM32P03B30-01EN
9.11	-	Hardware User Guide	IM32P06C10-01EN
9.12	-	Safety Instrumented System ProSafe-RS System Overview	TI 32P01A10-01EN
9.13	-	ProSafe-RS Installation Guidance	TI 32P01J10-01EN
9.14	-	Security Standard of System Product	TI 33Y01B30-01E
9.15	Safety Control Station (S2SC70D)	A Safety Control Station (SCS) consists of Safety Node Unit (SNU) that implements safety control function by executing the application programs downloaded from the Safety Engineering Station.	GS 32P06D10-01EN
9.16	Safety Node Unit (SNB10D)	The Safety Node Unit has an interface function to transmit Analog input signals and contact signals from the field to the Safety Node Unit via an ESB bus. It also has a function to supply power to I/O modules.	GS 32Q06K10-31E

Attachment no	Model	Description	IM/GS Reference
9.17	ESB Bus Coupler Module (SEC401-S1)	ESB Bus Coupler Module connects Safety Node Units and safety node units via an ESB bus cable. This module is installed in the Safety Node Unit.	GS 32Q06L11-31E
9.18	Analog Input Module (SAI143-H63)	AI Module inputs 4 to 20mA from the field. This module has HART communication function available. One HART device is connectable for each channel. Each channel is equipped with a power supply function to the HART device. Each module has only one HART modem and is communicable concurrently with only one HART device.	GS 32Q06K30-31E
9.19	Digital Input Module (SDV144-S63)	Digital Input modules SDV144 (24 VDC, 16 channels) will process all Digital Inputs. The signal input shall be a dry contact. Relays suitable for safety operations shall be installed in the termination cabinets suitable for interfacing with the field voltage level.	GS 32Q06K40-31E
	Digital Output Module (SDV541-S63)	The SDV541 (24 VDC, 16 channels) will process all Digital Outputs. Outputs shall be without common wiring. Relays suitable for safety operations shall be installed in the termination cabinets suitable for interfacing with the field voltage level for driving solenoid valves, motors, pumps, and compressors. Digital output modules shall support line monitoring if the safety status require energizing.	
	SCB100	For Detecting disconnection failures	
	SCB110	For Detecting short-circuit failures	
9.20	Enhanced Serial Bus Cable (YCB301)	This connects the Node interface unit to the SCS through the ESB bus coupler Module.	GS 32Q06M10-31E

Attachment no	Model	Description	IM/GS Reference
	Signal Cable for Analog Modules (KS1-10/HF)	Analog Signal Cable for YKO System (for 40-40 Pins)	
	Signal Cable for Digital Modules (AKB331-M010/HF)	Signal Cable (50-50 pin), DIO Cable length 10m, special cable for SDV144 or SDV541 (for ProSafe RS).	
9.21	TB for Analog Modules (SBA4D-06)	Terminal Board for Analog (Single and dual-redundant, 16 channel x 1)	GS 32Q06L20-31E
	TB for Digital Modules (SBD4D-06)	Terminal Board for Digital (Single and dual-redundant, 16 channel x 1)	

Table 6 – Attachments

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Attachment 9.1 ProSafe-RS User Guide

IM32P01B10-01EN

User's
Manual

ProSafe-RS
ProSafe-RS Lite

ProSafe-RS User's Guide

IM 32P01B10-01EN

YOKOGAWA
Yokogawa Electric Corporation

IM 32P01B10-01EN
11th Edition

Introduction

This manual provides the overview of ProSafe-RS. Please read first to understand the product. Links are also listed to guide you to the descriptions of ProSafe-RS usage for each situation.

CI Server Integration also contains FAST/TOOLS Integration function. If FAST/TOOLS Integration is used, replace the term “CI Server” with “FAST/TOOLS” in the user’s manual.

If you are using the Field Commissioning Support Package, replace “FieldMate Validator” in the User's Manual with “Field Commissioning Support Package.”

If you are using YFGW520, replace the term “YFGW510” with “YFGW520” in the User’s Manual.

This manual consists of the following parts:

- Part A Overview of ProSafe-RS
  Provides an overview of the typical functions of ProSafe-RS. ProSafe-RS can be used either on a physical computer or on a virtual computer that is built on a virtualization platform.
- Part B ProSafe-RS Security
  Describes the security function that should first be understood when handling ProSafe-RS products.
- Appendix 1 Glossary
  A glossary of terms used in the user manual
- Appendix 2 List of links
  A list that guides you to the description of ProSafe-RS usage in typical situations.

11th Edition : Dec. 2023 (YK)
All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Safety Precautions for Use

Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Be sure to confirm the specifications and required settings of the devices that are used in combination with the Product by referring to the instruction manual or other documents of the devices.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:



Indicates that caution is required. This symbol for the Product indicates the possibility of dangers such as electric shock on personnel and equipment, and also indicates that the user must refer to the User’s Manuals for necessary actions. In the User’s Manuals, this symbol is used together with a word “CAUTION” or “WARNING” at the locations where precautions for avoiding dangers are described.

<French> Signale qu’il faut faire preuve de prudence. Ce symbole pour le produit signale la possibilité d’un danger pour le personnel et l’équipement comme un choc électrique, et signale également que l’utilisateur doit se référer au Manuel de l’utilisateur afin de prendre les mesures nécessaires. Dans le Manuel de l’utilisateur, ce symbole est utilisé conjointement avec la mention «CAUTION» ou «WARNING» aux endroits où sont décrites les précautions pour éviter les dangers.



Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.

<French> Signale qu'il faut faire preuve de prudence avec la surface brûlante. Les appareils sur lesquels est apposé ce symbole risquent de devenir brûlants. Tout contact physique ou matériel avec ces appareils risque de provoquer des brûlures ou des dommages.



Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.



Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.

~ Indicates an AC supply.

⎓ Indicates a DC supply.

	Indicates that a component such as a power supply switch is turned ON.
◯	Indicates that a component such as a power supply switch is turned OFF.

Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

Warning and Disclaimer

- Except as specified in the warranty terms, YOKOGAWA shall not provide any warranty for the Product.
- YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Product.

Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the Software Product's merchantability or suitability for any particular purpose, except as specified in the warranty terms.
- Purchase the appropriate number of licenses of the Software Product according to the number of computers to be used.
- No copy of the Software Product may be made for any purpose other than backup; otherwise, it is deemed as an infringement of YOKOGAWA's Intellectual Property rights.
- Keep the software medium of the Software Product in a safe place.
- No reverse engineering, reverse compiling, reverse assembling, or converting the Software Product to human-readable format may be performed for the Software Product.
- No part of the Software Product may be transferred, converted, or sublet for use by any third-party, without prior written consent from YOKOGAWA.

Documentation Conventions

Symbols

The following symbols are used in the User's Manuals.



Indicates precautions to avoid a danger that may lead to death or severe injury.



Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.

IMPORTANT

Indicates important information required to understand operations or functions.

TIP

Indicates additional information.

SEE ALSO

Indicates referenced content.

In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

Typographical Conventions

The following typographical conventions are used throughout the User's Manuals.

Commonly Used Conventions throughout the User's Manuals

- Δ Mark
  Indicates that a space must be entered between character strings.
  Example:

  ```
  .ALΔPIC010Δ-SC
  ```

- Character string enclosed by braces { }
  Indicates character strings that may be omitted.

  Example:

  ```
  .PRΔTAG{Δ.sheet name}
  ```

Conventions Used to Show Key or Button Operations

- Characters enclosed by brackets [ ]
  When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a button name in a window, or an item in a list box displayed in a window.

  Example:

  To alter the function, press the [ESC] key.

Conventions of a User-defined Folder

- User-defined folder name enclosed by parenthesis ( )
  User definable path is written in a pair of parentheses.

  Example:

  ```
  (RS Project Folder)\SCS0101
  ```

If the RS Project Folder is `C:\MYRSPJT`, the above path becomes `C:\MYRSPJTSCS0101`.

Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.
If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

Definitions of Node and Module Terms

In the User's Manuals, nodes and modules are referred to by using collective terms, another terms, or abbreviations based on the following definitions:

- Definitions of nodes
  - Node: A node is a collective term for an FIO node and an N-IO node.
  - FIO node: This is a collective term for a safety control unit, a safety node unit, and a unit for optical ESB bus repeater module.
  - CPU node: This is another term for a safety control unit. The abbreviation of safety control unit is SCU.
  - I/O node: This is another term for a safety node unit. The abbreviation of safety node unit is SNU.
  - N-IO node: This is a collective term for a node interface unit and an N-IO I/O unit. The abbreviation of node interface unit is NIU.
- Definitions of modules
  - I/O module: This is a collective term for an FIO I/O module and an N-IO I/O module.
  - FIO I/O module: This is a collective term for an analog I/O module and a digital I/O module for FIO, and a communication module.
  - N-IO I/O module: This is a collective term for the modules that can be mounted on an N-IO I/O unit.
  - AIO/DIO module: This is a collective term for an analog I/O module, a digital I/O module, and a universal type I/O module.
  - Analog I/O module: This is a collective term for an analog input module and an analog output module.
  - Digital I/O module: This is a collective term for a digital input module and a digital output module.
  - Universal type I/O module: This is a collective term for the I/O modules for which the channel signal category can be changed by software.

- Input module: This is a collective term for an analog input module, digital input module, and a universal type I/O module with defined input channels.
- Output module: This is a collective term for an analog output module, digital output module, and a universal type I/O module with defined output channels.
- Communication module: This is a collective term for a serial communication module, an Ethernet communication module, and a fire and gas communication module.

Full Names and Simplified Terms

In the User's Manuals, simplified terms listed in the following table are used.

Table Info-1 Full Names and Simplified Terms

Full Name	Simplified Term
Automation Design Suite	AD Suite
Automation Design Organizer	AD Organizer
Automation Design Server	AD Server
Automation Design project	AD project
Automation Design Master Database	ADMDB
Automation Design Suite Administration Tool	ADS Administration Tool
iDefine for ProSafe-RS	iDefine
Modification Package	ModPack
SCSV1-S (SCS supporting the SSC10S/SSC10D safety control units)	SCSV1
SCSP1-S (SCS supporting the SSC50S/SSC50D safety control units)	SCSP1
SCSP2-S (SCS supporting the SSC60S/SSC60D safety control units)	SCSP2
SCSP3-S (SCS supporting the S2SC70S/S2SC70D safety control units)	SCSP3
SCSL2-S (SCS supporting the L1SC70S/L1SC70D safety control units)	SCSL2
SCSU1-S (SCS supporting the SSC57S/SSC57D safety control units)	SCSU1

Copyright and Trademark Notices

All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, PRM, Exaopc, FieldMate Validator, and STARDOM are registered trademarks or trademarks of Yokogawa Electric Corporation.
- The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

ProSafe-RS User's Guide

IM 32P01B10-01EN 11th Edition

CONTENTS

PART-A Overview of ProSafe-RS A-1

A1. Requirements A1-1

A1.1 Hardware requirements A1-2

A1.2 Software requirements A1-5

A2. System configuration of ProSafe-RS A2-1

A3. Overview of SCS A3-1

A3.1 SCS hardware configuration A3-4

A3.2 RAS (Reliability, Availability, Serviceability) functions of SCS A3-10

A3.2.1 SCS operating mode A3-12

A3.2.2 Security level of SCS A3-15

A3.2.3 Diagnosis for hardware A3-17

A3.3 Dual-redundancy in the SCS A3-18

A3.3.1 Redundant configuration in SCS A3-19

A3.3.2 CPU redundant status A3-22

A4. Outline of the safety system generation function A4-1

A4.1 Window components common to builders A4-12

A4.2 Types of downloading A4-16

A5. Configuration of maintenance function A5-1

A6. Overview of the SCS Maintenance Support Tool A6-1

A6.1 Relationships among functions of SCS Maintenance Support Tool A6-2

A6.2 Application examples at maintenance A6-4

A6.3 Customization of the SCS Maintenance Support Tool window A6-7

A7. Virtualization platform A7-1

A7.1 Outline of virtualization platform A7-2

A7.2 System configuration of virtualization platform A7-3

A7.2.1 Virtualization host computer A7-4

A7.2.2 Thin client A7-6

A7.3 Software environment A7-7

A7.3.1 Virtualization host computer A7-8

A7.3.2 Thin client A7-10

A7.3.3 License A7-11

A7.4 Precautions on the virtualization platform..... A7-12

A7.4.1 Precautions related to Vnet/IP communication on the virtualization platform..... A7-13

A7.4.2 Precautions on using ProSafe-RS on a virtual machine..... A7-15

ProSafe-RS User's Guide

IM 32P01B10-01EN 11th Edition

CONTENTS

PART-B ProSafe-RS security..... B-1
B1. Overview of ProSafe-RS security..... B1-1
B2. Security for project database..... B2-1
B3. Security of SCS..... B3-1
B4. NIU status and security..... B4-1
B4.1 Status of the NIU maintenance port..... B4-2
B4.2 Operation mode of the NIU..... B4-3
B4.3 Shifting the Status of the NIU..... B4-5
B4.4 Checking the status of the maintenance port of the NIU..... B4-6
B5. Security of SCS Maintenance Support tool..... B5-1
B6. Access control and history management..... B6-1

ProSafe-RS User's Guide

IM 32P01B10-01EN 11th Edition

CONTENTS

Appendix

Appendix 1. Glossary.....App.1-1
Appendix 2. List of links.....App.2-1

A. Overview of ProSafe-RS

ProSafe-RS is the Safety Instrumented System (SIS) comprising Safety Control Station (SCS) and Safety Engineering PC (SENG).

ProSafe-RS is the Safety Instrumented System that meets SIL 3 of the Safety Integrity Level (SIL) defined by IEC 61508. The lineup of products includes ProSafe-RS Lite, which meets Safety Integrity Level up to SIL 2.

In this User's Manual, the name of ProSafe-RS Lite may be used to describe products classified as ProSafe-RS Lite.

This section describes the following topics to give an overview of ProSafe-RS:

- Operating Environment
- System configuration of ProSafe-RS
- Overview of the SCS
- Configuration of safety system engineering function
- Configuration of Maintenance Function
- Configuration of the SCS Maintenance Support Tool
- Virtualization platform

A1. Requirements

This section explains the hardware and software requirements. It also explains the software that can collaborate with ProSafe-RS and software that can co-exist on the same computer.

SEE ALSO For more information about hardware on which the virtualization platform runs, and Yokogawa system products running on virtualization platform virtual machines, refer to:

IA system products virtualization platform (GS 30A05B10-01EN)

A1.1 Hardware requirements

This section describes the hardware environment used in a ProSafe-RS system.

If CENTUM software is also installed on the same computer, the computer must also meet the requirements for CENTUM.

Likewise, if iDefine software is installed on the same computer, the computer must also meet the requirements for iDefine.

SEE ALSO For more information about the hardware requirements of the computer where iDefine is to be installed, refer to:

2., "System Requirements" in iDefine Installation Guide (PR03076-MAN-991_01)

Hardware requirements for SENG

You must ensure that the computer that is used as SENG meets the hardware requirements as shown in the following table. Conditions will differ depending on the package being used.

- When using the Engineering Server Function:

Table A1.1-1 Hardware requirements for SENG (Windows 10)

Component	Requirements
CPU	Intel Core i5 equivalent or above
Main memory	8 GB or more
Hard disk space	Available space of at least 100 MB x the number of SCS units

Table A1.1-2 Hardware requirements for SENG (Windows Server 2016, Windows Server 2019, Windows Server 2022)

Component	Requirements
CPU	Xeon 4 core (2.2 GHz) equivalent or above
Main memory	8 GB or more
Hard disk space	Available space of at least 100 MB x the number of SCS units

- When using the Safety System Engineering and Maintenance Function:
  When installing the Engineering Server Function in the same computer, observe the hardware requirements for the Engineering Server Function. Also be sure to total the required space available for the hard disk space.

Table A1.1-3 Hardware requirements for SENG (Windows 10)

Component	Requirements
CPU	Intel Core i5 equivalent or above
Main memory	8 GB or more
Hard disk space	Available space of at least 60 GB

Table A1.1-4 Hardware requirements for SENG (Windows Server 2016, Windows Server 2019, Windows Server 2022)

Component	Requirements
CPU	Xeon 4 core (2.2 GHz) equivalent or above
Main memory	8 GB or more
Hard disk space	Available space of at least 60 GB

- When using the SOE Viewer Package, SOE OPC Interface Package, and Forced I/O Viewer Package:
  When installing the SOE Viewer Package or the SOE OPC Interface Package on the same computer where the Engineering Server Function, or the Safety System Engineering and Maintenance Function is installed, observe the hardware requirements for each function. Also be sure to total the space required by each function and available for the hard disk space.

Table A1.1-5 Hardware requirements for SENG (Windows 10)

Component	Requirements
CPU	Intel Core 2 Duo processor (2.13 GHz) equivalent or above, or Xeon Dual Core (2.0 GHz) equivalent or above
Main memory	4 GB or more
Hard disk space	• Available space of at least 20 GB (required) • Available space of at least 40 GB (recommended)

Table A1.1-6 Hardware requirements for SENG (Windows Server 2016, Windows Server 2019, Windows Server 2022)

Component	Requirements
CPU	Xeon Dual Core (2.93 GHz) or higher (mandatory)
Main memory	4 GB or more
Hard disk space	• Available space of at least 20 GB (required) • Available space of at least 40 GB (recommended)

The components for which requirements are same irrespective of OS and license conditions are summarized in the following table.

Table A1.1-7 SENG hardware requirements (components for which requirements are the same for all the conditions)

Component	Requirements
Display	• When using a square monitor, a resolution of at least SXGA (1280x1024), True Color (required) • When using a wide-screen monitor, a resolution of at least WXGA+ (1440×900), True color
Graphics	DirectX 9 graphic processing unit or equivalent, and supports the following (mandatory): • Windows Driver Display Model (WDDM) • Pixel Shader 2.0 • 32 bits per pixel • 128 MB graphic memory
Peripheral unit	• DVD-ROM drive (mandatory) • 1 PCI Express slot is necessary for the Vnet/IP interface card (mandatory) (*1) • Mouse (mandatory)

*1: When connecting the computer to the Vnet/IP.

Hardware requirements for a file server

The hardware requirements for the computer used as a file server are as follows:

Table A1.1-8 Hardware requirements for a file server (Windows Server 2016, Windows Server 2019, Windows Server 2022)

Component	Requirements
CPU	2 GHz or higher
Main memory	2 GB or more

Continues on the next page

Table A1.1-8 Hardware requirements for a file server (Windows Server 2016, Windows Server 2019, Windows Server 2022) (Table continued)

Component	Requirements
Hard disk space	• Available space of at least 20 GB (required) • Available space of at least 50 GB (recommended) However, when placing the history management database on the hard disk, an additional available space of at least 60 GB is recommended
Display	SuperVGA (800 x 600) or higher (mandatory)
Peripheral unit	• DVD-ROM drive (mandatory) • Network adapter (mandatory)

A1.2 Software requirements

This section describes the software requirements for SENG. It also explains the software that can collaborate with ProSafe-RS and software that can co-exist on the same computer.

Software requirements for SENG

This section describes the software requirements for SENG.

Supported OS

Windows OS versions to be supported by ProSafe-RS are as follows:

- Windows 10 Enterprise 2016 LTSB (64-bit) (*1) (*2)
- Windows 10 IoT Enterprise 2016 LTSB (64-bit) (*1)
- Windows 10 Enterprise LTSC 2019 (64-bit) (*1) (*2)
- Windows 10 IoT Enterprise LTSC 2019 (64-bit) (*1)
- Windows 10 Enterprise LTSC 2021 (64-bit) (*1)(*2)
- Windows 10 IoT Enterprise LTSC 2021 (64-bit) (*1)
- Windows Server 2016 Standard (64-bit)
- Windows Server 2019 Standard (64-bit)
- Windows Server IoT 2019 Standard (64-bit)
- Windows Server 2022 Standard (64-bit)
- Windows Server IoT 2022 Standard (64-bit)

*1: For these models, functions are not updated and only security patches and hotfixes are provided. Exercise caution because these models are functionally different from other Windows 10 models.
*2: These models are sold only with volume licenses.

Before installing ProSafe-RS, make sure that a Windows OS version and service pack appropriate for the ProSafe-RS software release number are installed on the computer.

In this manual, whenever Windows 10, Windows Server 2019, or Windows Server 2022 is mentioned in the explanations hereafter, the IoT versions are also included.

IMPORTANT

- On a Windows pre-installed computer, various Windows utilities and other software may have been installed in addition to the Windows OS. These additional functions are not only unnecessary for SENG but also can disturb its operations. To avoid disturbance to operations, reinstall the Windows OS.
- It is assumed that security patches are applied according to the customer's security policy. YOKOGAWA recommends to apply security patches to ProSafe-RS systems. It is recommended to apply all required security patches before the system goes into operation and also apply security patches that are released after the system went into operation as promptly as possible. YOKOGAWA offers security patch application services. Contact YOKOGAWA Service for more information.
- When using Windows 10 Enterprise 2016 LTSB, Windows 10 Enterprise LTSC 2019, and Windows 10 Enterprise LTSC 2021 computers, customize the Windows settings during installation of Windows 10.

SEE ALSO For more information about the procedure for the customization at installation of Windows 10 Enterprise 2016 LTSB, Windows 10 Enterprise LTSC 2019, and Windows 10 Enterprise LTSC 2019, refer to:

Appendix 5., “Customization at Installation of Windows 10” in Installation Guide (IM 32P01C50-01EN)

.NET Framework

When the ProSafe-RS software is installed, .NET Framework is automatically installed. However, .NET Framework included in the ProSafe-RS software medium will not be installed automatically if a newer version has already been installed in the computer, to avoid downgrading of .NET Framework.

The following table shows the version of supported .NET Framework for each Windows OS.

Table A1.2-1 Version of supported .NET Framework

Windows OS	Version of supported .NET Framework
Windows 10	.NET Framework 4.8
Windows Server 2016	
Windows Server 2019	
Windows Server 2022	

Software that can coexist with ProSafe-RS

The ProSafe-RS software can coexist with the following software programs.

The following table lists the software that has been confirmed to run without affecting the operation of ProSafe-RS when installed on the same computer.

IMPORTANT

Use only the volume license version of Microsoft Word and Microsoft Excel.

Table A1.2-2 List of software that can coexist with ProSafe-RS

Classification	Software name	Version (*1)(*2)(*3)	Remarks
Spread sheet	Microsoft Excel (*4) (*5)	2021, 2019 (*6) (*7), 2016 (*8)	32-bit/64-bit (*9)
Word processor	Microsoft Word (*4) (*5)	2021, 2019 (*6) (*7), 2016 (*8)	32-bit/64-bit (*9)
WWW browser	Microsoft Internet Explorer	11	
	Microsoft Edge (*10)		
Security	Yokogawa standard antivirus software	-	
	Standard Whitelisting Software for Endpoint Security	-	
Document viewer	Adobe Acrobat	2020	Used for the Instruction Manual Package
	Adobe Acrobat Reader	DC, 2020	

*1: Please confirm the required operation environment of each software for OS on which each software operates.
*2: SP is an abbreviation of Service Pack.
*3: The software version has been confirmed at the time of the release of this document. For more information about the latest supported version, contact YOKOGAWA.
*4: If CENTUM software is installed on the same computer, make sure that installed software also meets the software requirements for CENTUM.
*5: Only the volume license version is subject to operation guarantee.
*6: Excel/Word version 2019 or 2021 works only on the following OS:

- Windows 10 Enterprise LTSC 2019
- Windows 10 Enterprise LTSC 2021
- Windows Server 2019
- Windows Server 2022

*7: When installing Excel/Word version 2019 or 2021 from Office, install only the target software with the Office Deployment Tool.
*8: Supports Windows 10 Enterprise 2016 LTSB and Windows Server 2016 only.
*9: To use the 64-bit version of Word/Excel, install it before installing ProSafe-RS. If ProSafe-RS is installed already, uninstall Access Database Engine 2016, then reinstall Word/Excel and then ProSafe-RS.
*10: It is used to display the user-defined action guide. If Microsoft Edge is not installed, use Microsoft Internet Explorer.

TIP

For precautions when using Standard Whitelisting Software for Endpoint Security on virtual machines, contact YOKOGAWA.

CENTUM integration system

When ProSafe-RS is integrated with CENTUM, available ProSafe-RS functions are limited depending on the software release number of CENTUM. This section explains precautions when installing the ProSafe-RS and CENTUM software on separate computers or on the same computer.

SEE ALSO

For more information about integration with CENTUM, refer to:

B., “CENTUM integration” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Relationship between ProSafe-RS functions and CENTUM release numbers

When using ProSafe-RS R4.10.00, CENTUM VP of release number R6.11 or later is recommended.

For the version of the Engineering Server Function, use the version or later included in this version ProSafe-RS. If you use the old versions of the Engineering Server Function, AD Suite will not properly operate.

When using CENTUM VP of the release number that is not recommended, the following restriction applies:

Table A1.2-3 When CENTUM VP is earlier than R6.11

Limitation
• ProSafe-RS and CENTUM VP cannot be installed on the same computer.

Table A1.2-4 When CENTUM VP is earlier than R6.08

Limitation
• SIL 2 SCS cannot be defined on System View. • Operation and monitoring of SIL 2 SCS is not available from HIS.

Table A1.2-5 When CENTUM VP is earlier than R6.07

Limitation
• System alarm messages added in R4.05.00 are not displayed on HIS. The same applies to the messages that are received through an OPC server. • In the SCS Status Display view and SCS Report dialog box, the status of Operation data reset switch is not displayed. • In the SCS Report dialog box, CPU model of S2CP471 is not displayed correctly. • Even if “Skip Password Dialog Box for Manual Operation FB” is enabled in the SCS Constants Builder, the Password Input dialog box displayed when manipulating MV from HIS is not omitted.

Table A1.2-6 When CENTUM VP is earlier than R6.06

Limitation
• The SCS simulation test does not operate correctly.

Table A1.2-7 When CENTUM VP is earlier than R6.05

Limitation
• The tags of the function blocks PSI_I, PSI_R, PNI_I, PNI_R added in R4.03.10 are not displayed on HIS. • System alarm messages added in R4.03.10 are not displayed on HIS. The same applies to the messages that are received through an OPC server. • The system alarm messages to which the string “Safety Subsystem” is added in R4.03.10 is displayed without “Safety Subsystem”. In other words, the legacy message strings are displayed. The same applies to the messages that are received through an OPC server. • In the SCS Status Display view and SCS Report dialog box, number of locked safety subsystem communication I/O is not displayed.

Table A1.2-8 When CENTUM VP is earlier than R6.04

Limitation
• The instrument faceplate of mapping blocks S_HSDTR/S_GASDTR cannot be displayed in HIS. Process alarm messages are not displayed properly. • System alarm messages added in R4.03.00 are not displayed on HIS. Messages through OPC are also not displayed. • System alarm messages that are supposed to be suppressed by the alarm suppression function during device reset are not suppressed and are displayed in HIS. • System alarm messages and process alarm messages that are supposed to be suppressed by the chattering alarm suppression function are not suppressed and are displayed in HIS.

Table A1.2-9 When CENTUM VP is earlier than R6.02

Limitation
• Operation and monitoring of SCSP3 cannot be performed on HIS.

IT security setting

- You can fortify computer security. To fortify the security, select "Standard model" with the IT Security Tool at installation of both ProSafe-RS and CENTUM VP.
- If you integrate ProSafe-RS with CENTUM VP earlier than R5.01, manually relax some security items according to the IT security setting of CENTUM VP.

SEE ALSO For more information about IT Security Tool, refer to:

6.1, “IT Security Tool” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

Coexistence of ProSafe-RS and CENTUM on the same computer

Observe the following precautions when installing the ProSafe-RS and CENTUM VP software on the same computer.

- When installing ProSafe-RS R4.10.00 and CENTUM VP on the same computer, use the software of CENTUM VP R6.11 or later.
- Unless specially instructed, install the control bus driver from the ProSafe-RS software medium.
  If one of the systems has been upgraded, follow the instruction provided for each revision.
- On a computer installed with both the ProSafe-RS and CENTUM software, configure Windows settings according to the instructions in the installation manual of CENTUM.
- PROFIBUS-DP Configurator (SYCON.net/YOKO) and PROFINET Configurator (SYCON.net-A2LP/YOKO) of CENTUM VP, and PROFINET Configurator (SYCON.net-SLP/YOKO) of ProSafe-RS cannot be started simultaneously.

TIP

- PROFIBUS-DP Configurator (SYCON.net/YOKO), PROFINET Configurator (SYCON.net-A2LP/YOKO), and PROFINET Configurator (SYCON.net-SLP/YOKO) are products of Hilscher.
- The features exclusively prepared for ProSafe-RS cannot be used in the commercially available Hilscher SYCON.net.

SEE ALSO

For more information about iDefine version that can coexist with ProSafe-RS and CENTUM VP, refer to:

"■ Use of iDefine" on page A1-10

For more information about installing the control bus driver, refer to:

B3.3.1, "Installing the Control Bus Driver" in Installation Guide (IM 32P01C50-01EN)

For more information about setup of Windows with CENTUM VP, refer to:

B4.2, "Setting Up Windows" in CENTUM VP Installation (IM 33J01C10-01EN)

■ CI Server integration system

● Coexistence of ProSafe-RS and CI Server on the same computer

CI Server and ProSafe-RS software cannot run on the same computer.

● Version

When using ProSafe-RS R4.10.00, the recommended version of CI Server is R1.01 or later. However, CI Server does not support the following devices and functions:

- Mapping blocks S_HSDTR, S_GASDTR
- Fire and gas communication
- Status display of the operation data reset switch of S2CP471

■ FAST/TOOLS integration system

● Coexistence of ProSafe-RS and FAST/TOOLS on the same computer

FAST/TOOLS and ProSafe-RS software cannot run on the same computer.

● Version

When using ProSafe-RS R4.10.00, the recommended version of FAST/TOOLS is R10.04 or later. However, FAST/TOOLS R10.04 does not support the following devices and functions:

- N-IO nodes
- Mapping blocks S_HSDTR, S_GASDTR
- Fire and gas communication
- Status display of the operation data reset switch of S2CP471
- SIL 2 SCS

Use of iDefine

IMPORTANT

When using ProSafe-RS and iDefine, use ProSafe-RS R4.02 to R4.08.

If you want to use SENG to edit engineering data created with iDefine, contact YOKOGAWA.

Coexistence of ProSafe-RS and iDefine on the same computer

When using ProSafe-RS R4.03 or later, iDefine and ProSafe-RS software can coexist.

When using ProSafe-RS R4.05 or later, iDefine software can coexist on the computer where ProSafe-RS and CENTUM VP R6.07 or later software coexist. iDefine and CENTUM VP alone cannot coexist.

IMPORTANT

You cannot install iDefine software on the computer where ProSafe-RS and PRM client software coexist.

Version

The following table shows the version numbers of ProSafe-RS and iDefine that can be used in combination.

Table A1.2-10 Allowed version number combinations of ProSafe-RS and iDefine

ProSafe-RS release number	iDefine version number	Coexistence
R4.02.00	1.16.1	Not allowed
R4.03.00	1.16.2	Allowed
R4.03.10	1.16.3	Allowed
R4.04.00	1.16.4	Allowed
R4.05.00	1.16.5	Allowed, can coexist with CENTUM VP R6.07
R4.06.00	1.16.6	Allowed, can coexist with CENTUM VP R6.08 or R6.09
R4.07.00	1.16.7	Allowed, can coexist with CENTUM VP R6.08 or R6.09
R4.08.00	1.16.7	Allowed, can coexist with CENTUM VP R6.10

iDefine is a product of Trinity Integrated Systems Ltd.

SEE ALSO For more information about the software requirements of the computer where iDefine is to be installed, refer to:

2., "System Requirements" in iDefine Installation Guide (PR03076-MAN-991_01)

Use of PRM

Coexistence of ProSafe-RS and PRM on the same computer

Whether or not the PRM and ProSafe-RS software can run on the same computer is as follows:

- A PRM server and ProSafe-RS software cannot run on the same computer.
- A PRM client and ProSafe-RS software can run on the same computer. Note, however, that a PRM client cannot run on the same computer if the computer has a license of SOE OPC Interface Package of ProSafe-RS.
- If you install the PRM client on SENG that is connected to the narrowband Vnet/IP-Upstream network, you need additional Ethernet wiring for PRM client communications.

IMPORTANT

You cannot install iDefine software on the computer where ProSafe-RS and PRM client software coexist.

Precautions when installing ProSafe-RS and PRM on the same computer

When ProSafe-RS R4.03.10 and PRM are installed on the same computer, occasionally the error messages related to DTM (Device Type Manager) is displayed in the PROFINET Configurator. When you open PROFINET Configurator for the first time, the error messages are displayed in the message area of PROFINET Configurator at the time of registering GSDML.

```
GetInformation failed with device: DTM name
```

You can ignore this error message when the DTM name is not YFGW410.

Version

When using ProSafe-RS R4.10.00, the recommended version of PRM is R4.06 or later. PRM versions earlier than R4.06 cannot be installed on the same computer as ProSafe-RS. PRM versions earlier than R4.05 do not support SCSL2 station. PRM versions earlier than R3.30 do not support SCSP3 station. Also, PRM versions earlier than R3.12 cannot be connected to the narrowband mode of Vnet/IP-Upstream.

Use of Exaopc

Coexistence of ProSafe-RS and Exaopc on the same computer

Exaopc and ProSafe-RS software cannot run on the same computer.

Version

When using ProSafe-RS R4.10.00, the recommended version of Exaopc is R3.81 or later. When using Exaopc of the version that is not recommended, the following restriction applies:

Table A1.2-11 When Exaopc is earlier than R3.78

Limitation
• The system alarm messages newly added to R4.05.00 are not notified to Exaopc Client.

Table A1.2-12 When Exaopc is earlier than R3.77

Limitation
• The system alarm messages added to R4.03.10 are not notified to Exaopc Client. • In R4.03.10, system alarm messages with “Safety Subsystem” mentioned in the legacy message are notified to Exaopc Client as a legacy message without “Safety Subsystem”.

Table A1.2-13 When Exaopc is earlier than R3.76

Limitation
• The system alarm messages added to R4.03.00 are not notified to Exaopc Client. • Process alarm messages generated from mapping blocks S_HSDTR/S_GASDTR are not notified to Exaopc client successfully. • Alarm status added in the R4.03.00 cannot be acquired in the OPC interface related to inquiries of condition name. • A recover alarm message about completion of the suppression period of the chattering alarm suppression function is not notified to Exaopc client.

Table A1.2-14 When Exaopc is earlier than R3.74

Limitation
• N-IO related system alarms are not notified to Exaopc client.

Use of Exaquantum

Coexistence of ProSafe-RS and Exaquantum on the same computer

Exaquantum and ProSafe-RS software cannot run on the same computer.

Version

When using ProSafe-RS R4.10.00, the recommended version of Exaquantum is R3.01 or later. ProSafe-RS can be connected to Exaquantum R2.20 or later. However, because the versions of Exaquantum earlier than R2.60 do not support the IT security function, you must select the Legacy model to use the IT security function of ProSafe-RS.

A2. System configuration of ProSafe-RS

This section describes the following ProSafe-RS system configurations:

- System configuration of SCS that supports SIL 3
- System configuration of SCS that supports SIL 2
- System configuration where exists both SCSs that support SIL 3 and SIL 2

System configuration of SCS that supports SIL 3

SCS that supports SIL 3 consists of hardware for SIL 3. Software license for SIL 3 is used for SENG.

SIL 3 safety communication can be used between SCSs that support SIL 3.

There is also an SCS (S2SC70) that supports N-IO and safety subsystem communication.

The following figure shows an example of the system configuration of SCS that supports SIL 3.

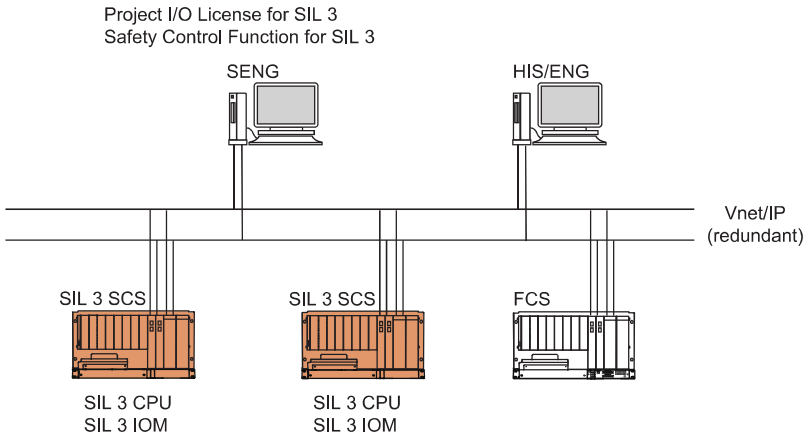


Figure A2-1 Example of the system configuration of SCS that supports SIL 3

System configuration of SCS that supports SIL 2

SCS that supports SIL 2 consists of hardware for SIL 2. Software license for SIL 2 is used for SENG.

SIL 2 safety communication can be used between SCSs that support SIL 2.

The following figure shows an example of the system configuration of SCS that supports SIL 2.

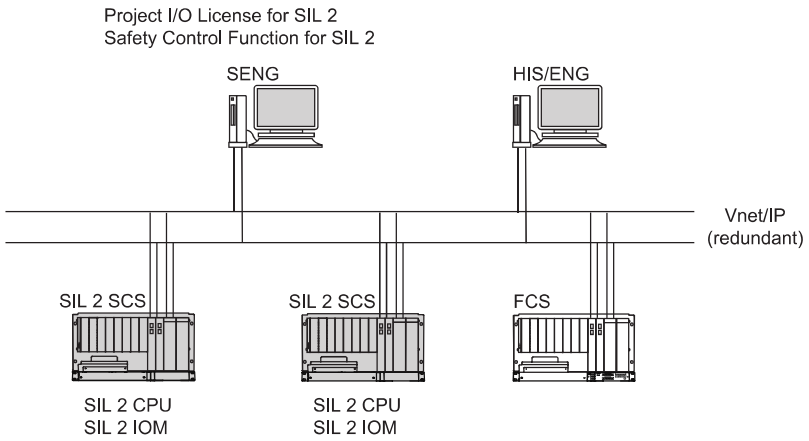


Figure A2-2 Example of the system configuration of SCS that supports SIL 2

System configuration where exists both SCSs that support SIL 3 and SIL 2

SCSs that support SIL 3 and SIL 2 can coexist in the same network.

SCS that supports SIL 3 consists of hardware for SIL 3.

SCS that supports SIL 2 consists of hardware for SIL 2.

Both software licenses for SIL 3 and SIL 2 are used for SENG. Both SCSs that support SIL 3 and SIL 2 can be engineered, tested, and maintained with a single SENG.

If safety communication is used between SCSs that support SIL 3 and SIL 2 respectively, SIL 2 safety communication is adopted.

The following figure shows an example of the system configuration where exists both SCSs that support SIL 3 and SIL 2.

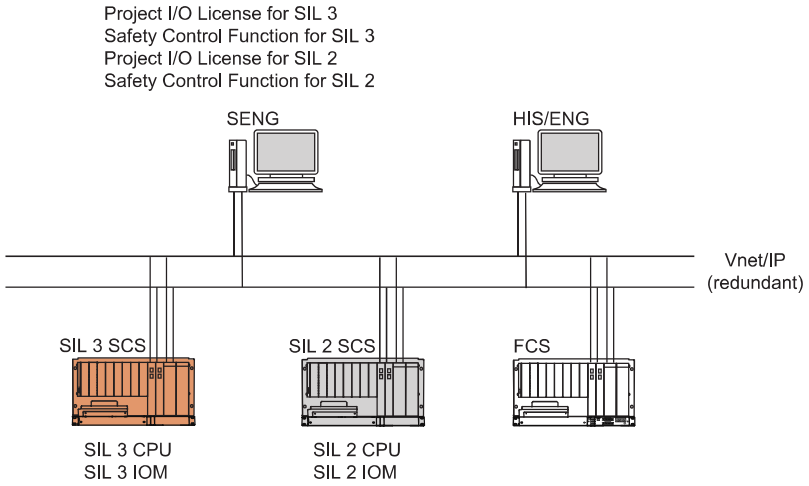


Figure A2-3 Example of the system configuration where exists both SCSs that support SIL 3 and SIL 2

A3. Overview of SCS

The ProSafe-RS SCS (Safety Control Station) is a station dedicated for safety control applications.

The SCS consists of the function that monitors the safety conditions of the plant, the application logic execution function that performs pre-determined safety operations according to each safety control request and the external communication function that communicates information with devices other than SCSs.

Classification of SCS application

In the SCS, you can create the following applications:

- Safety application
  This is an application which executes safety functions. The safety application includes application logic written in the language conforming to the IEC 61131-3 standards.

  The following programming languages defined in IEC 61131-3 are available for the SCS:

  - Function Block Diagram (FBD)
  - Ladder Diagram (LD)
  - Structured Text (ST)

- Application to connect with other systems
  You can create the following applications:

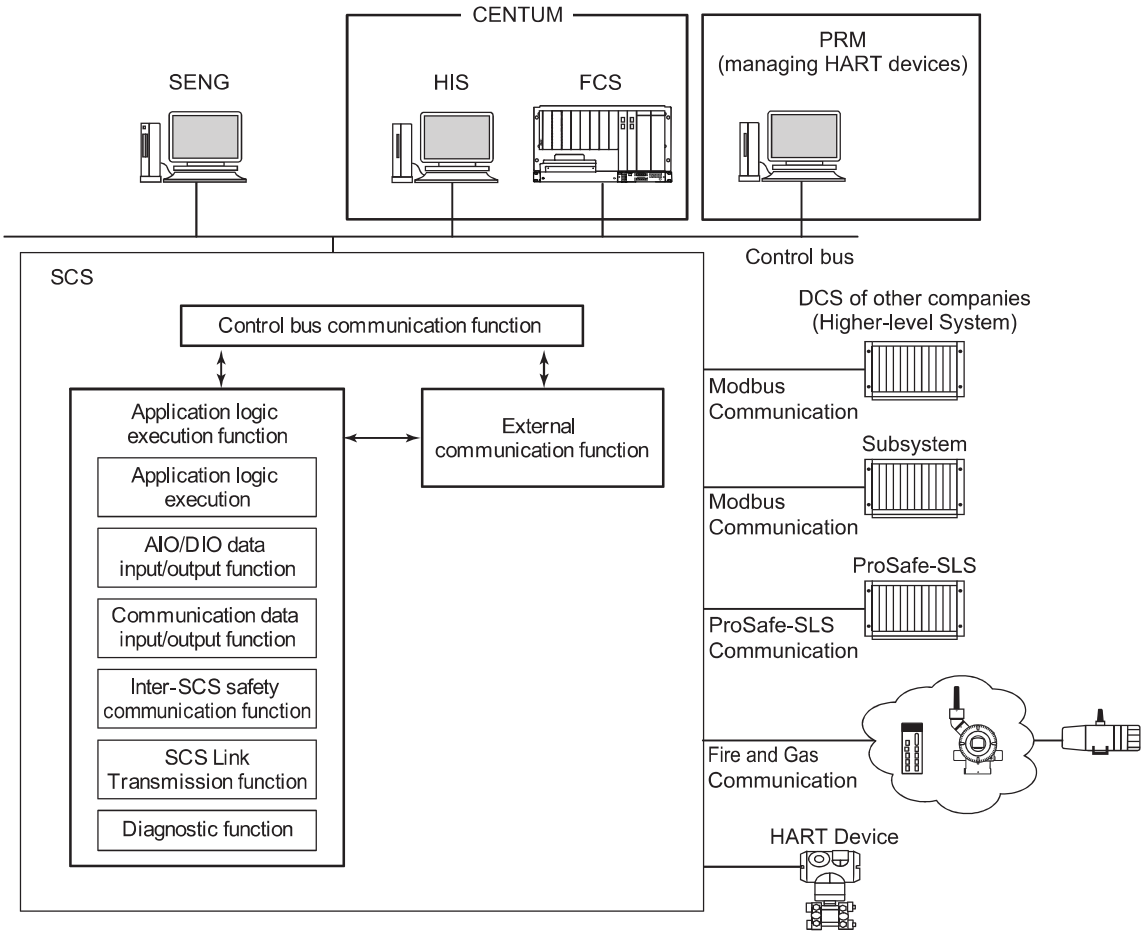
  - CENTUM integration
    This is an application for exchanging data with the CENTUM system.
  - CI Server integration
    This is an application for exchanging data with CI Server. In SCSU1, you can create an application for gas flow calculation in accordance with the specifications of American Gas Association.
  - Subsystem communication
    This is an application for exchanging data with the SCS and the subsystem connected via Modbus. It supports Modbus communications using serial communication module and Ethernet communication module.

    You can create an application that collects events and data from the ProSafe-SLS in serial communication.
  - Safety subsystem communication
    This is an application for safely exchanging data between SCS and subsystem devices. It supports communication using fire and gas communication module.
  - Modbus slave communication
    It is an application that exchanges information between an external device (a Modus master) and the SCS that are connected through Modbus communication. It is compatible for the Modbus communication that exchanges information via serial communication module and Ethernet communication module.
  - DNP3 communication application
    This is an application for communicating between the DNP3 master and SCSU1 connected via DNP3.

Overview of SCS software configuration

SCS is equipped with an application logic execution function for detecting dangerous situations and executing control to prevent or mitigate such situations and an external connection function inclusive of functions for integration with CENTUM which is the production control

system of Yokogawa Electric. Note that these functions exchange data with a station on the control bus via a control bus communication function which serves as an interface. In particular, when data is being written into the application logic execution function, the memory inside the SCS is protected with various functions for ensuring safety with such as security levels.



SENG: Station that handles engineering and maintenance of SCS
HIS: Station that executes operation and monitoring of CENTUM
FCS: Control station of CENTUM
PRM: Plant Resource Manager

Figure A3-1 Overview of SCS function configuration

Application logic execution function

This function monitors the safety condition of the plant and makes the process shift to the safety state on detecting any hazards. It mainly performs the following processing.

- Receiving Analog Input (AI)/Digital Input (DI) data from the field
- Execution of user-defined application logic
- Sending Analog Output (AO)/Digital Output (DO) data to the field
- Inter-SCS safety communication
- SCS link transmission
- Communication data I/O (subsystem communication function, safety subsystem communication function)
- Self-diagnosis

Application logic

An SCS executes application logic written in the IEC 61131-3 program language. The application logic is defined by the user using Multi Language Editor and downloaded to the SCS.

An SCS supports the following three languages of IEC 61131-3:

- Function Block Diagram (FBD)
- Ladder Diagram (LD)
- Structured Text (ST)

TIP

The application logic execution function explained here is not simply a name for a function that handles execution of the application logic; rather, it is a generic name for all the functions explained above, including the actual execution of the application logic. In this manual, this term is used in the following explanation as well.

SEE ALSO

For more information about Structured Text (ST), refer to:

2., “Structured text” in POU Reference Manual (IM 32P03B20-01EN)

For more information about Function Block Diagram (FBD), Ladder Diagram (LD), refer to:

1., “Overview of POU” in POU Reference Manual (IM 32P03B20-01EN)

External communication function

This is a function for exchanging information with external systems connected to an SCS and it does not influence the application logic execution function. Main operations are as follows:

- Diagnostic information collection function
- SOER function
- CENTUM Integration Function
- CI Server integration function (SCSP3, SCSP2, SCSP1, and SCSU1)
- Modbus slave communication function
- PRM-supported HART On-demand Communication
- DNP3 communication function (SCSU1 only)

A3.1 SCS hardware configuration

This section describes the hardware configurations for SCSs that support SIL 3 and SIL 2.

SCS hardware configuration that supports SIL 3

If the safety control unit is S2SC70D or S2SC70S (SCSP3), these three following methods are available to connect the I/O node to the SCSP3:

- N-IO nodes only connection
- Safety node units only connection
- Combined connection of N-IO nodes and safety node units

If the safety control unit is SSC60D or SSC60S (SCSP2), only the safety node unit can be connected.

The following table shows the main hardware names used in SCS that supports SIL 3.

Table A3.1-1 Main hardware names used in SCS that supports SIL 3

Name	Description	Note
SCU	Safety control unit	SSC60D/SSC60S (*1) and S2SC70D/ S2SC70S
SNU	Safety node unit	SNB10D
PSM	Power supply module	SPW481, SPW482, and SPW484. Always redundant.
CPU	Processor module (CPU module)	SCP461 (SSC60 only), SCP461 S2, and S2CP471
SEC401/ SEC402	ESB bus coupler module	Used when SNU and N-IO nodes are used. Installed in slots 7 and 8 of SCU. Always redundant.
SSB401	ESB bus interface module	Always redundant
SNT401/ SNT411	Optical ESB Bus Repeater Master Module	Always redundant
SNT501/ SNT511	Optical ESB Bus Repeater Slave Module	Always redundant
S2EN402/ S2EN404	N-ESB bus coupler module	Used when N-IO node is used. Installed in SCU. Always redundant.
FIO	FIO I/O module	Analog I/O module that supports SIL 3, digital I/O module that supports SIL 3, and communication module
N-IO node	Node for installing N-IO	Configured with node interface unit and N-IO I/O unit.
PSU	Power supply unit for N-IO	S2PW503 and S2PW504. Always redundant.
S2EN501	N-ESB bus module	Used when N-IO node is used. Installed in N-IO node. Always redundant.
N-IO	N-IO I/O module	Universal type I/O module
ESB bus	Bus to connect SCU and SNU	-
N-ESB bus	Bus to connect SCU and N-IO node	-
Optical ESB bus	Bus to connect SCU, SNU, and N-IO node	-

*1: N-IO node is not connectable.

N-IO node only connection

The following configuration are used when connecting only the N-IO nodes to the safety control unit.

When connecting the safety control unit and N-IO nodes by using the N-ESB bus, the S2EN402/S2EN404 is mounted to the safety control unit, and S2EN501 to the N-IO node. When connecting the safety control unit and N-IO node by using the optical ESB bus, the SEC401/SEC402 is mounted to the safety control unit, and S2EN501 to the N-IO node.

The connection between N-IO nodes must be connected with the N-ESB bus or the optical ESB bus.

The following figure shows an example of configuration with N-IO nodes-only connection.

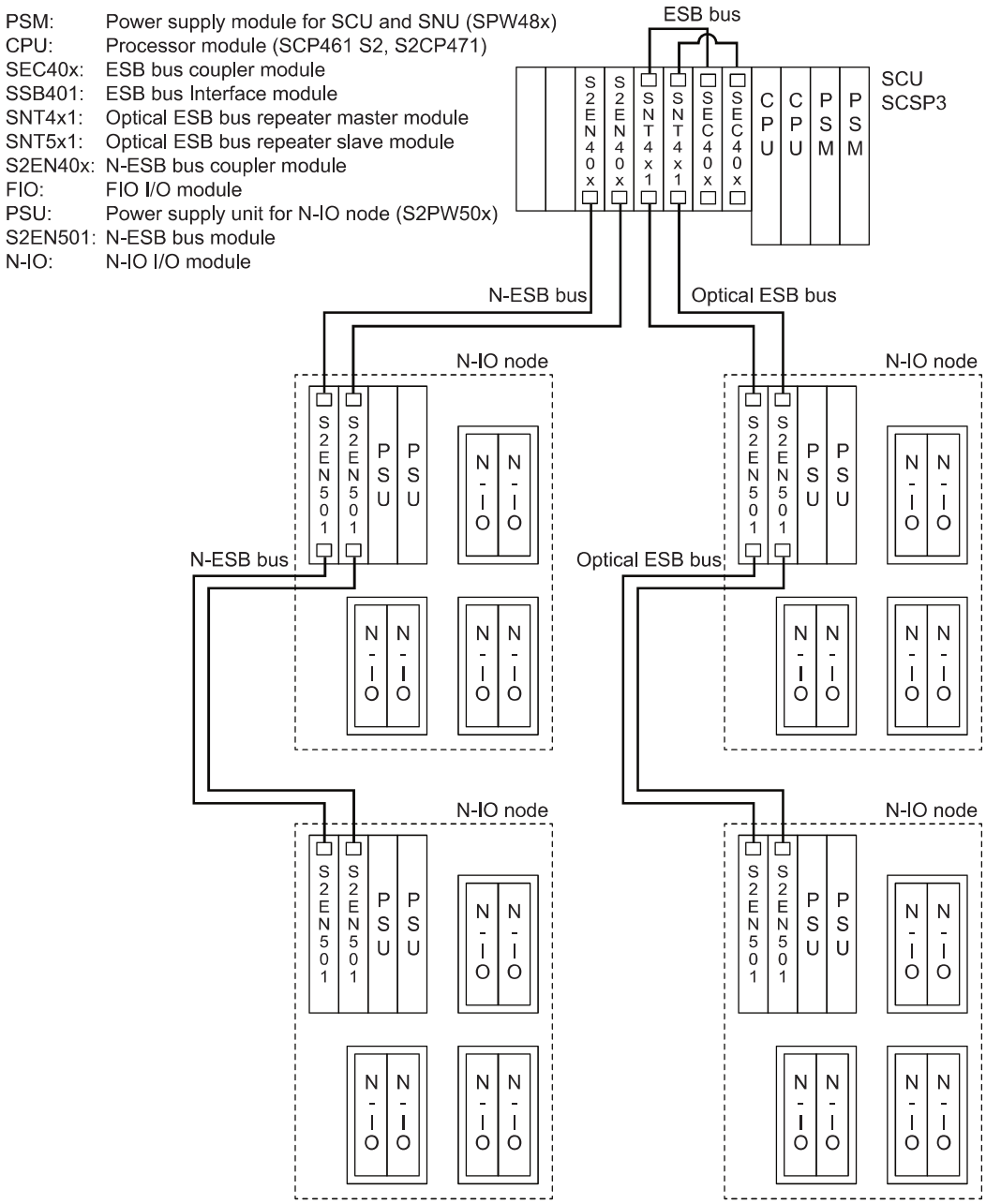


Figure A3.1-1 Configuration example of an N-IO node-only connection

Safety node unit only connection

The following configuration are used when connecting only the safety node units to the safety control unit.

When connecting the safety control unit and safety node unit by using the ESB bus, the SEC401/SEC402 is mounted to the safety control unit, and SSB401 to the safety node unit. When connecting the safety control unit and safety node unit by using the optical ESB bus, the SEC401/SEC402 and SNT401/SNT411 is mounted to the safety control unit, and SNT501/SNT511 and SSB401 to the safety node unit.

The connection between the safety node units must be connected with an ESB bus, or an optical ESB bus through SNT401/SNT411 and SNT501/SNT511.

The following figure shows a configuration example of a safety node units-only connection.

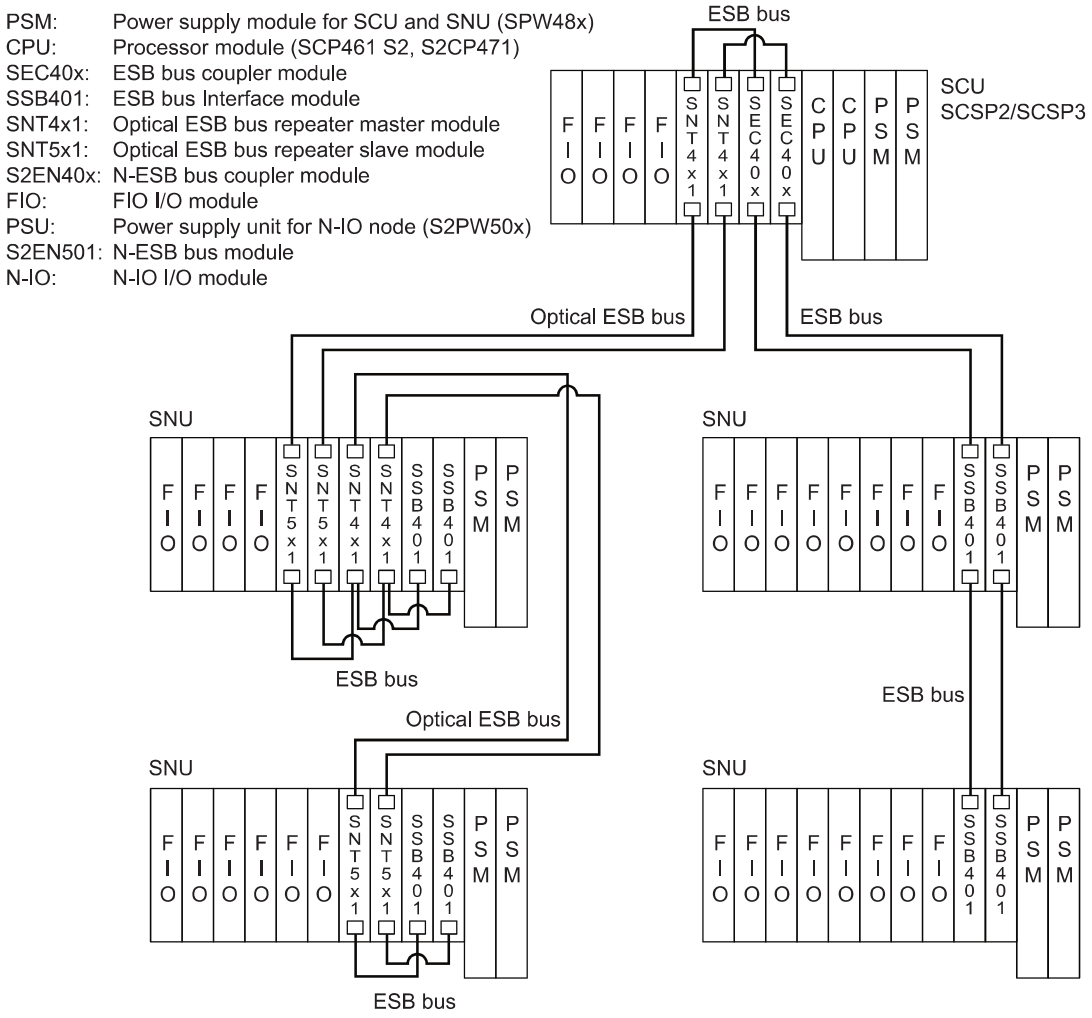


Figure A3.1-2 Configuration example of a safety node units-only connection

Combined connection of N-IO node and safety node unit

N-IO nodes and safety node units can be connected to a single safety control unit. To use both nodes together, you can connect the N-IO node and safety node unit, or separate them.

- Connecting N-IO nodes and safety node units together
  When connecting the safety control unit together with the safety node units and N-IO nodes, connect with the following configuration.

When connecting the safety control unit and N-IO node using the optical ESB bus, the SEC401/SEC402 and SNT401/SNT411 are mounted to the safety control unit, and S2EN501 to the N-IO node.

N-IO node and safety node unit are connected through an optical ESB bus. SNT501/ SNT511 and SSB401 are installed to the safety node unit.

The following figure shows a configuration example of an N-IO node and safety node unit connection.

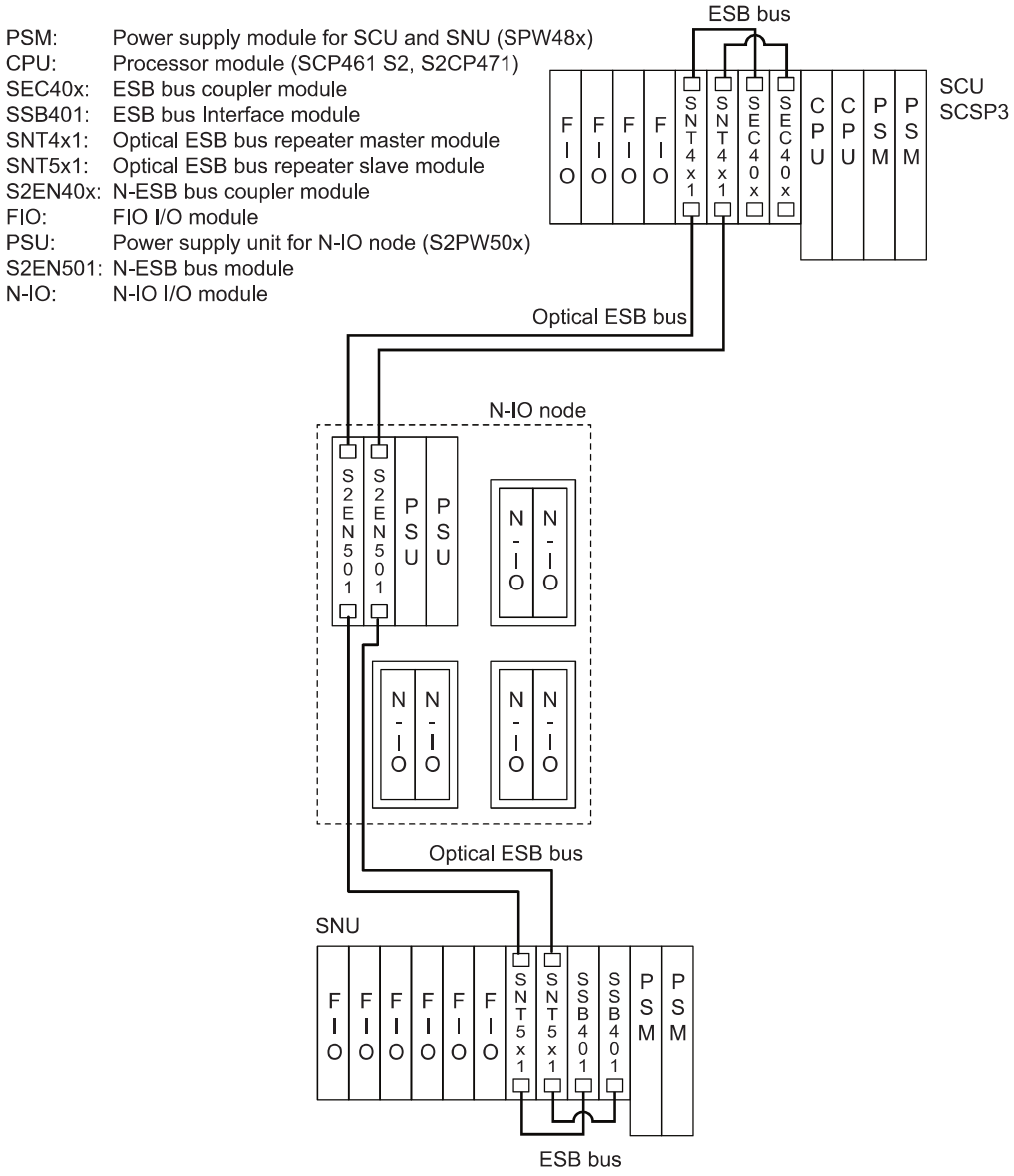


Figure A3.1-3 Configuration example of an N-IO node and safety node unit connection

- Separating N-IO nodes and safety node units, and connecting them together
  When N-IO nodes and safety node units are separated from each other, and they are connected with the safety control unit, the N-IO nodes-only connection and the safety node units-only connection are combined.

  The following figure shows a configuration example when N-IO node and safety node unit are separated and connected together.

PSM: Power supply module for SCU and SNU (SPW48x)
CPU: Processor module (SCP461 S2, S2CP471)
SEC40x: ESB bus coupler module
SSB401: ESB bus Interface module
SNT4x1: Optical ESB bus repeater master module
SNT5x1: Optical ESB bus repeater slave module
S2EN40x: N-ESB bus coupler module
FIO: FIO I/O module
PSU: Power supply unit for N-IO node (S2PW50x)
S2EN501: N-ESB bus module
N-IO: N-IO I/O module

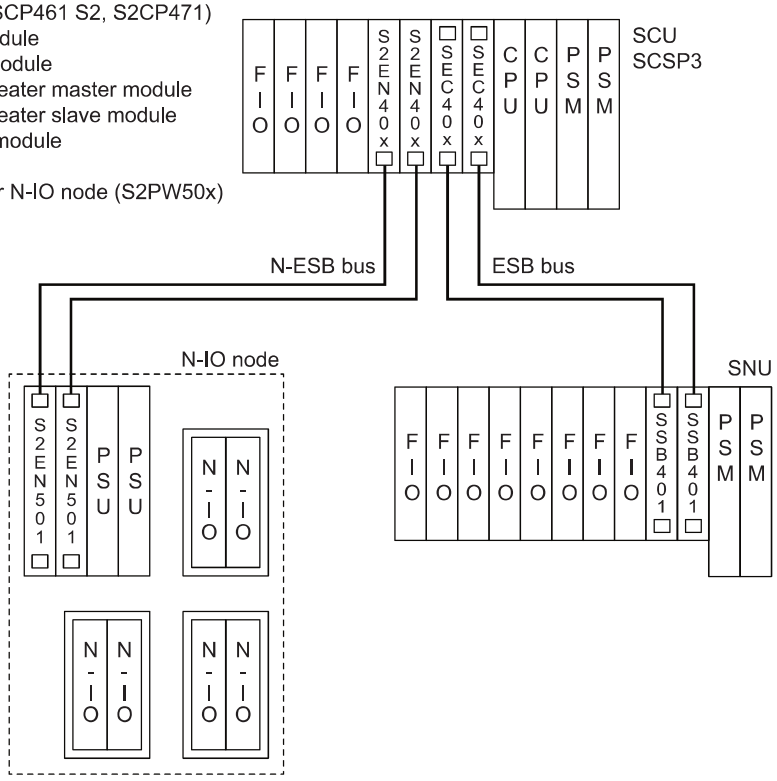


Figure A3.1-4 Configuration example when N-IO node and safety node unit are separated and connected together

SCS hardware configuration that supports SIL 2

If the safety control unit is L1SC70D or L1SC70S (SCSL2), only the safety node unit can be connected.

The following table shows the main hardware names used in SCS that supports SIL 2.

Table A3.1-2 Main hardware names used in SCS that supports SIL 2

Name	Description	Note
SCU	Safety control unit	L1SC70D/L1SC70S
SNU	Safety node unit	L1NB10D
PSM	Power supply module	L1PW481, L1PW482, and L1PW484. Always redundant.
CPU	Processor module (CPU module)	L1CP471
L1EC401/ L1EC402	ESB bus coupler module	Used when SNU is used. Installed in slots 7 and 8 of SCU. Always redundant.
L1SB401	ESB bus interface module	Always redundant
L1NT401/ L1NT411	Optical ESB Bus Repeater Master Module	Always redundant
L1NT501/ L1NT511	Optical ESB Bus Repeater Slave Module	Always redundant
FIO	FIO I/O module	Analog I/O module that supports SIL 2, digital I/O module that supports SIL 2, and communication module
ESB bus	Bus to connect SCU and SNU	-

Continues on the next page

Table A3.1-2 Main hardware names used in SCS that supports SIL 2 (Table continued)

Name	Description	Note
Optical ESB bus	Bus to connect SCU and SNU	-

Safety node unit only connection

The following configuration is used when connecting only the safety node units to the safety control unit.

When connecting the safety control unit and safety node unit by using the ESB bus, the L1EC401/L1EC402 is mounted to the safety control unit, and L1SB401 to the safety node unit. When connecting the safety control unit and safety node unit by using the optical ESB bus, the L1EC401/L1EC402 and L1NT401/L1NT411 are mounted to the safety control unit, and L1NT501/L1NT511 and L1SB401 to the safety node unit.

The connection between the safety node units must be connected with an ESB bus, or an optical ESB bus through L1NT401/L1NT411 and L1NT501/L1NT511.

The following figure shows a configuration example of a safety node units-only connection.

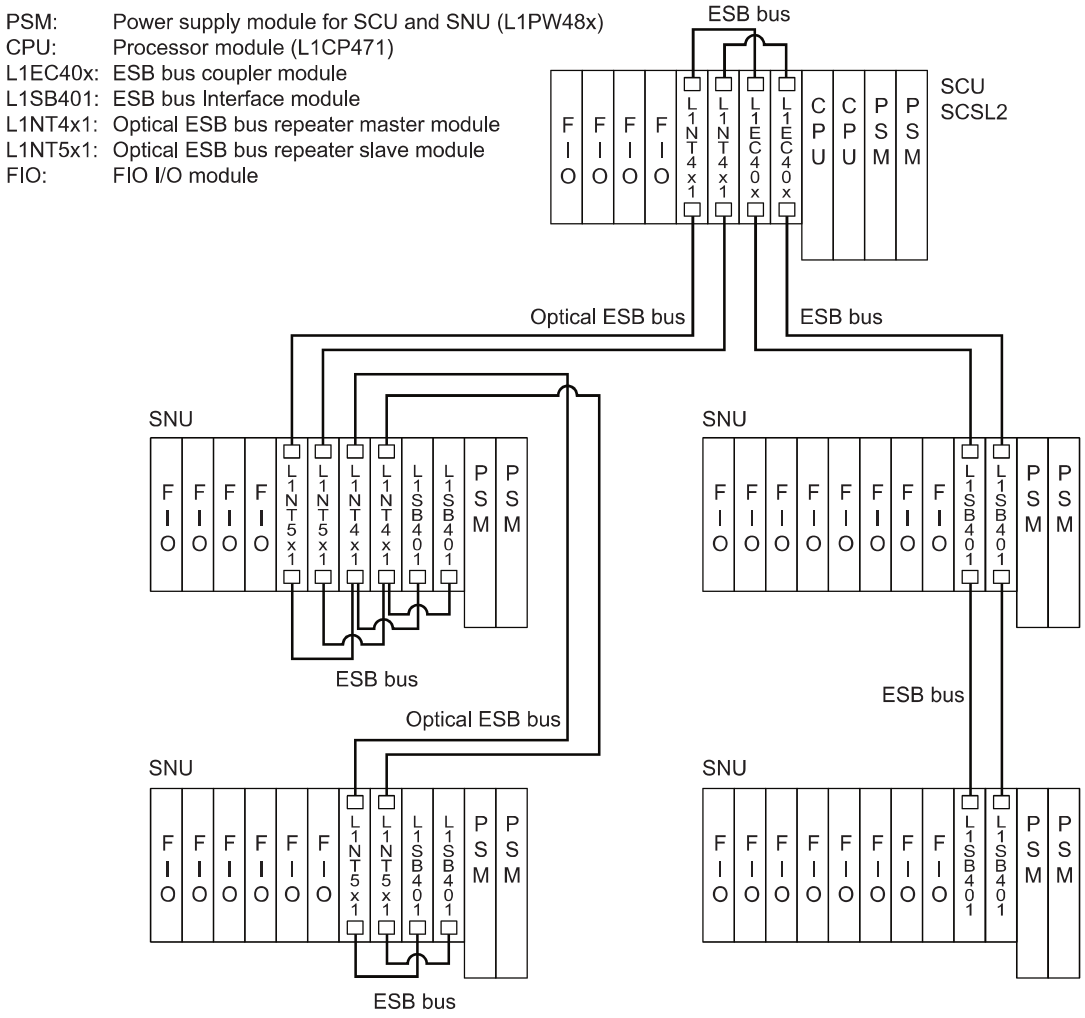


Figure A3.1-5 Configuration example of a safety node units-only connection

A3.2 RAS (Reliability, Availability, Serviceability) functions of SCS

This section explains functions related to reliability, availability and serviceability of the SCS (hereinafter referred to as RAS in this manual). Moreover, it is a function that implements safety. The function includes the ability to shift to a safe state in a fast and reliable manner when an error occurs in the plant or system.

The RAS functions of the SCS are as follows:

- Operating mode
- Security level
- Diagnostic management function, diagnostic information messages
- Operation during start, and operation during error
- Dual redundancy

SEE ALSO For more information about the functions for checking the SCS status, refer to:

H., “Monitoring the SCS status” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about the operations upon SCS error occurrence and recovery procedures, refer to:

G2., “Operations and recovery procedures during the SCS error occurrence” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Positioning of RAS function

RAS stands for Reliability, Availability and Serviceability, and is an important index when evaluating the system performance. Reliability means robustness against error occurrence, availability means shortness of downtime and serviceability means ease of repair at failure.

Functional relation of software

The RAS function diagnoses whether hardware and software are running normally and handles maintenance of them if any errors are detected. Since this function is able to shut the system down and change the SCS status as required, it is one of the most essential SCS functions.

Relationship with other hardware

The RAS function collects hardware error information concerning the I/O modules and other components in the station. The RAS function organizes hardware error information and executes pre-defined safety operations accordingly, such as shutting down. Error information is sent to the SENG and HIS as diagnostic information messages. The SCS saves diagnostic information generated internally. And the information can be referenced from SENG. You can delete saved diagnostic information messages from SENG.

The figure below shows how the RAS function of the SCS is positioned.

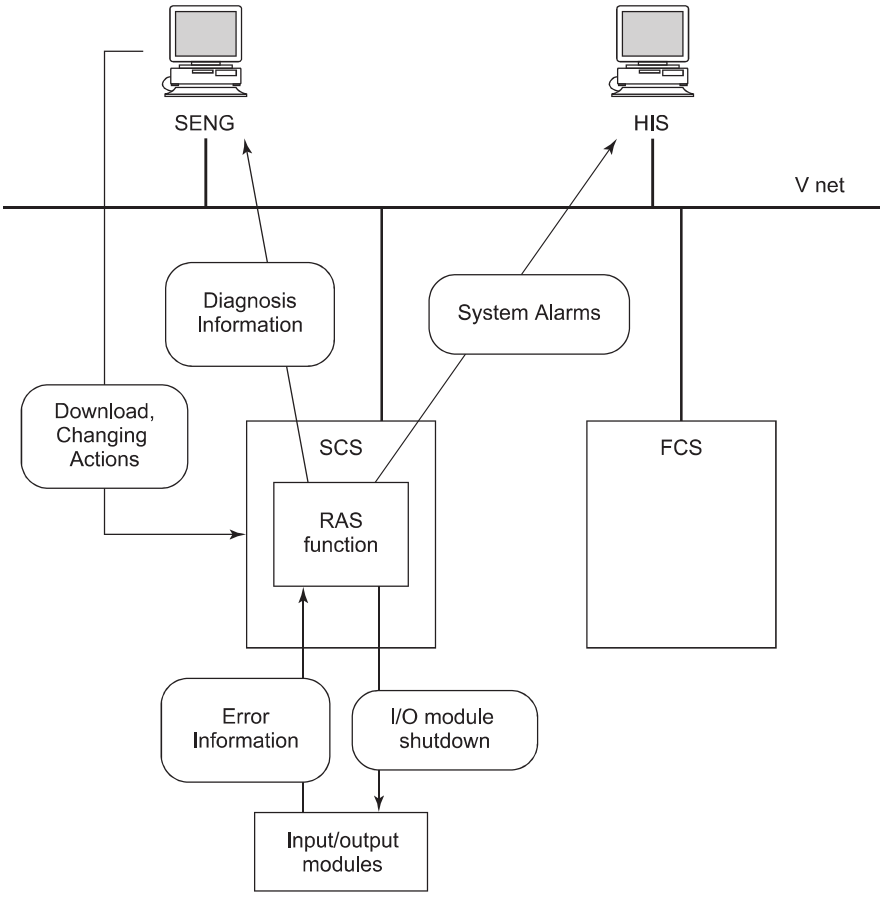


Figure A3.2-1 Positioning of RAS function

A3.2.1 SCS operating mode

The operating mode indicates the operation status of an SCS. Operations of the functions that are implemented by the system program of the SCS are determined by the operating mode. The operating mode is outlined as follows:

- The operating mode indicates the overall operating status of SCS, not the status of individual output modules.
- The operating mode indicates the status of a single SCS, regardless of whether the CPU configuration of the SCS is single or dual-redundant.
- For an SCS with dual-redundant CPU, the operating mode remains the same before and after a control right switchover of the CPU.

There are five SCS operating modes: Stop mode, Loading mode, Initial mode, Waiting mode, and Running mode

The following figure shows the transitions between operating modes. Note that it is possible to shift to the Stop mode from all other modes, but the arrows indicating these shifts are omitted for the sake of clarity.

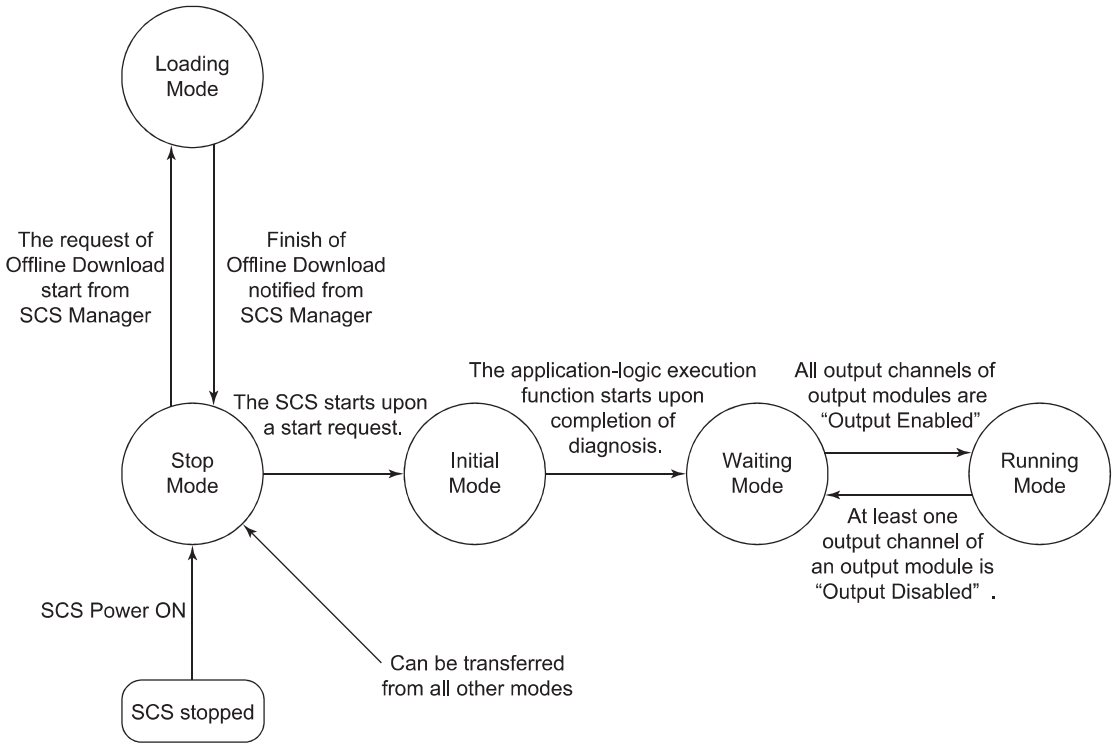


Figure A3.2.1-1 Transitions between operating modes

Stop mode (stopped status)

This is the initial state of the SCS.

Loading mode (during offline download)

In this mode, program and database are being downloaded from the SCS Manager to the SCS.

Initial mode (initializing status)

In this mode, the SCS is initializing databases, processing the diagnostic at startup, and starting the I/O modules as follows:

- Input modules
  If started successfully, input values are set to applicable input variables. If the startup of any module has failed, an error is recognized for the module.
- Output modules
  The outputs of all channels remain disabled after the startup is completed, so that the output values from the application logic will not be sent to the field immediately.
- Subsystem communication modules
  Receives only the input from subsystems while having an output that is invalid.
- Fire and gas communication modules
  If the startup process is successfully completed, fire and gas communication modules receive only the input from subsystems. If the startup process ends in an error, the SCS handles the fire and gas communication modules as erroneous.

Waiting mode (waiting for output enable request)

Application logic is periodically executed on each scan period. However, the output channel will not output the application logic value if the status is set to "Output Disable". The waiting mode status can be checked in the SCS State Management window and the LED display of the CPU module.

When "Output enable operation" is performed, the outputs on the normal channels of output modules are enabled. If you execute the "Output enable operation" just after starting up the SCS, the SCS also enables the output of inter-SCS safety communication, SCS link transmission and subsystem communication.

TIP

- Failure on the output channel should be removed, then perform "Output enable operation".
- Even when the channel is set to "Output Disabled", if the physical data is rewritten using the forcing function, the output value from the output channel changes.

SEE ALSO

For more information about Data value in unlocked / locked status and output disable / enable status, refer to:

A6.2, “I/O variable” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about Output enable operation, refer to:

C8., “Output enable operation” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about SCS State Management Window, refer to:

H1.2, “SCS State Management window” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Running mode (controlling status)

This mode indicates that the SCS is running normally. All output channels of output modules are outputting the output values from the application logic. The Running mode status can be checked with the SCS State Management Window and LED display of the CPU module.

Output status monitoring

All output channels of output modules are monitored. If any of the channels becomes Output Disable status due to a failure in the corresponding module or in the output channel itself, or after adding new channels during online modification, the SCS will change its operating mode to the Waiting mode. The operating mode changes to the Running mode when the cause of the channel failure is removed, the output enable operation is completed and all output channels are placed in the Output Enable status.

Checking of operation mode

The operating mode of SCS can be checked with the following methods.

- It is possible to check that the operating mode is either the Waiting or Running mode with the SCS State Management window of the SCS Maintenance Support Tool, the SCS Status Display view of HIS and the LED display of a CPU module.
- If the operating mode is either the Waiting or Running mode, the operating mode can be referenced from the application logic as well.

Influence on operating mode

Engineering and occurrence of errors can affect the operating mode as follows.

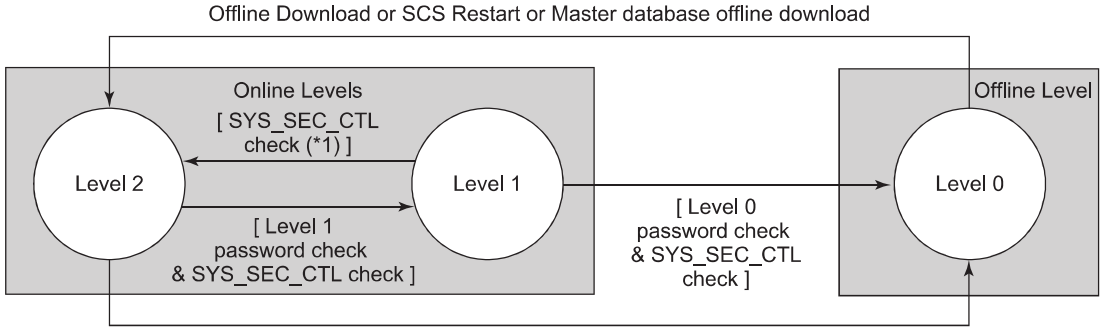
- The operating mode is not affected even if a subsystem communication error, safety subsystem communication error, or communication module error occurs.
- Occurrence of errors in SCS link transmission has no influence on the operating mode.
- If output modules/channels are added via online change download, the added modules/channels are started from the Output Disable status. If the operation mode was Running mode previously, it changes to Waiting mode. Perform the output enable operation.
- If channels in the Output Disable status or output modules that include such channels are deleted via online changes and there are no longer any channels in the Output Disable status in SCS, the operating mode shifts from Waiting mode to Running mode.
- If a single output module is changed to dual redundant configuration by online change download, IOM download is executed in order to initialize the modules. The outputs of the target modules become disabled after downloading. Since some channels are in the Output Disable status, the operating mode of SCS shifts to the Waiting mode. Perform the output enable operation after the output modules recover to normal.
- It is possible to perform the output enable operation regardless of the status of communication modules.
- It is possible to perform the output enable operation even if the status of communication with sub-systems is BAD. In this case, only outputs that are ready to communicate will start.

A3.2.2 Security level of SCS

The security level of SCS indicates the level of protection against erroneous writing to the memory in SCS from the connected stations or devices. An overview of SCS security level is as follows:

- One SCS has one security level.
- The security level can be confirmed from LED on the CPU module and the SCS State Management window of SCS Maintenance Support Tool or Status Display View of HIS.
- SCS limits changes made from the outside according to security level.
- Security level can be referred to by applicable logic.
- Security level can be changed by an authorized user with the password using the SCS Manager.
- Using the system function block (SYS_SEC_CTL) makes it possible to control whether or not to allow security level change operations from an SENG with an external hardware switch or similar.
- Security level can be changed under the following conditions:
  - The SCS is either in the Waiting or Running mode, AND
  - The SYS_SEC_CTL is set to allow security level changes or is not used.

The following figure illustrates the transition of states of the security level.



*1: It is allowed to reset the security level from Level 1 to Level 2 via the RST input in the SYS_SECURE block, regardless of the security level change enable/disable status of SYS_SEC_CTL.

Figure A3.2.2-1 Transition of security level status

Definition of each security level

There are two classifications of levels; online level and offline level. The Online level is used when SCS is in normal operation. The Offline level is used when SCS is not in normal operation.

Online level

The Online Level is a security level to be used when normal operation is performed in SCS. The SCS itself provides security of the Online Level by controlling access to the memory from the outside.

The Online Level is separated into two levels according to limits of functions which can be used.

Table A3.2.2-1 Online level

Level	Description
Level 2	The highest security level. SCS is usually operated at this security level.
Level 1	A temporary security level used by engineers or authorized users for maintenance of equipment or changing applications online

Offline level

The Offline Level is a security level to be used when a regular operation is not performed in SCS. This is displayed as "Level 0" on the LED of SCS or the SCS State Management window of SENG. In the Offline Level, SCS does not limit access to SCS from the outside. However, information which was used at test may be stored in SCS databases depending on operations performed by those tools.

IMPORTANT

To restore an SCS to Online Level from Offline Level, restart the SCS or do offline download. This ensures that the system returns to the security level for normal operation.

Security level at the start of SCS

The security level is Level 2 when SCS starts normally.

A3.2.3 Diagnosis for hardware

The SCS carries out diagnosis at the following timing to check whether various types of hardware including I/O modules are in the normal state:

- At the start of the hardware
- At specified periodical intervals during operation

This section describes the HKU function in the CPU module, and the cabinet status monitoring function in the N-IO node.

HKU (House Keeping Unit)

The HKU function in the CPU module monitors the operation environment of the CPU module. An error in the CPU operating environment is notified to the user via diagnostic information messages and status display window. The following items are monitored by the HKU function.

- Fan status in the safety control unit
- Surrounding temperature of the safety control unit
- Battery temperature

Cabinet status monitoring

The N-ESB bus module of N-IO node monitors the operating environment of the cabinet. An error in the operating environment of the cabinet is notified to the user via diagnostic information messages and status display window.

Temperature monitoring

The SCS monitors the surrounding temperature of the N-ESB module, as well as the upper limit and lower limit value in the hardware. It monitors whether the temperature exceeds the prescribed value or not.

Power supply diagnosis

The SCS monitors the status of the power supply unit (PSU) connected to the N-ESB module unit. The following are the methods in diagnosing a power supply:

- PSU output stop diagnosis
  The SCS monitors the output voltage in redundant PSUs. It is judged as an error if output in either of the PSUs stops.
- Output over-voltage diagnosis
  The SCS monitors the output voltage of the PSUs, as well as the upper limit and lower limit value in the hardware. It monitors whether the output voltage exceeds the prescribed value or not. It is judged as an error if it exceeds the maximum value.

Input monitoring from external devices

By inputting a single point of discrete signal from an external device, which can detect power supply and fan abnormalities, in an external alarm input of the base plate, errors from the external device can be notified.

The safety control unit outputs the diagnostic information message according to the discrete signal that is inputted from the external device.

Because this function is interference-free, it cannot be used for safety logic.

A3.3 Dual-redundancy in the SCS

ProSafe-RS supports dual-redundant configurations of SCS CPU modules and input/output modules. With the dual-redundant configuration, the continuous controllability and operating efficiency can be improved. Moreover, with dual-redundantly configured hardware, the continuity of plant safety monitoring will be guaranteed by switching the control rights when an error occurs in the SCS hardware.

A3.3.1 Redundant configuration in SCS

In SCS, redundant configuration can be selected for the CPU module and I/O modules. The control bus, power supply module, ESB bus, ESB bus interface module, optical ESB bus repeater module, N-ESB bus, N-ESB bus module, and F-SB bus are always in redundant configurations.

CPU module

- The CPU module on the standby side performs the same control processing as the control side even while it is in the standby status. For this reason, it is possible to take over outputting data immediately after the control right is switched. Moreover, the operating mode of the SCS does not change.
- Only the CPU on the control side accesses the hardware composing the SCS and the CPU on the standby side always sets the equivalent value as the processing result. Therefore, the CPU modules on both sides always perform processing using the same data.
- In redundant configuration, if the CPU module on the standby side is not in the STBY status and the control right cannot be switched, the same operation as single configuration CPU module is performed.
- SOE data related to discrete inputs might be lost when the control right is switched between the CPU modules.
- With the CPU module of SCSL2 and the CPU module of SCSP2, the data loaded with the previous scan may be used instead of updating the data with the value from the input module when performing a scan immediately after a control right switchover of the CPU. Also note that data loaded from 1 or 2 scans earlier may be used with subsystem communication modules.
- With the CPU module of SCSP3, the data loaded with the previous scan may be used instead of updating the data with the value from the input module or fire and gas communication module when performing a scan immediately after a control right switchover of the CPU. Also note that data loaded from 1 or 2 scans earlier may be used with subsystem communication modules.

FIO I/O modules

Redundant configuration is possible in the FIO node(*1) by mounting the same type of FIO I/O module to two adjacent slots. In the case of redundant configuration, one side becomes the control side and the other becomes the standby side. Switching of the control right is performed by input/output modules. The switching has no influence on the application logic.

*1: An odd-numbered slot and the even-numbered slot obtained by adding 1 to the odd slot number

- It is not allowed to have redundant configuration across two nodes.
- SOE data related to discrete inputs might be lost when the control right is switched between the input modules even though the frequency is low.
- A HART communication error may occur when the control right is switched between analog input/output modules that support HART communication.

Table A3.3.1-1 Operation of redundant AIO/DIO modules

AIO/DIO module	Redundant operation
Analog input module Digital input module	The input data of the input module on the control side is stored in the input variable.

Continues on the next page

Table A3.3.1-1 Operation of redundant AIO/DIO modules (Table continued)

AIO/DIO module	Redundant operation
Analog output module Digital output module	The SCS outputs the same value for output modules on both the control and standby sides. Only the output module on the control side outputs signals to the field. If an error occurs on the module on the control side, the control right is switched and outputting is continued

SEE ALSO For more information about implementing dual-redundant subsystem communication, refer to:

D1.2, "Dual-redundant communication" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about implementing dual-redundant Modbus slave communication, refer to:

"■ Redundancy of Modbus communication" in F4., "Precautions for engineering" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

■ NIO I/O modules

Redundant configuration is possible in the N-IO node by mounting the same type of N-IO I/O module to two adjacent slots. In the case of redundant configuration, one side becomes the control side and the other becomes the standby side. Switching of the control right is performed by input/output modules. The switching has no influence on the application logic.

- SOE data related to discrete inputs might be lost when the control right is switched between the input modules even though the frequency is low.
- A HART communication error may occur when the control right is switched between analog input/output modules that support HART communication.

Table A3.3.1-2 Redundant operation in N-IO I/O modules

Signal type	Redundant operation
AI/DI	The input data of the input module on the control side is stored in the input variable.
AO/DO	The SCS outputs the same value for output modules on both the control and standby sides. Only the output module on the control side outputs signals to the field. If an error occurs on the module on the control side, the control right is switched and outputting is continued

■ Optical ESB bus repeater module

The optical ESB bus repeater modules are always used in a redundant configuration.

■ Power supply module

A redundant power supply module is installed on each of CPU nodes, I/O nodes, and N-IO nodes of the SCS. The SCS monitors the status of the power supply at regular intervals and, if an error occurs, it notifies the user about the error via the SCS State Management window of the SENG, the Status Display view of the HIS, and diagnostic information messages. If one of the two power supplies mounted on the CPU node has generated an error, it notifies two diagnostic information messages; one corresponding to the error of the power supply module on the CPU node and the other corresponding to the error of the power supply module on node 1.

■ ESB bus and ESB bus interface module

The ESB bus is redundant. The two ESB buses are connected to their corresponding ESB bus interface modules. The following operations also apply when optical ESB bus repeater devices are present along the communication route.

- Normally, redundant ESB buses are used in an alternating fashion.
- If an error occurs in either ESB bus interface module, the user is notified of the error with a diagnostic information message. If both buses fail, the error is treated as a node failure.
- If an error occurs in one ESB bus or ESB bus interface module, the SCS continues communication by using only the other ESB bus that is normal.
- An erroneous bus is monitored for normal recovery at regular intervals.
- Errors in communication with all I/O nodes, except CPU node, are judged to be ESB bus error.

N-ESB bus and N-ESB bus module

The ESB bus has redundant configuration. Each N-ESB bus module is connected to N-ESB bus, respectively.

- Normally, redundant N-ESB buses are used in an alternating fashion.
- If an error occurs on either N-ESB bus module, the error is notified to the user via a diagnostic information message. If both buses fail, the error is treated as a node failure.
- If an error occurs in either N-ESB bus or N-ESB bus module, the SCS continues communication using only the normal ESB bus on the other side.
- An erroneous N-ESB bus is monitored for normal recovery at regular intervals.

F-SB bus

The F-SB bus has redundant configuration.

- The F-SB bus is normally used at the same time on both sides.
- If an error occurs in either F-SB bus, the SCS continues communication using only the normal ESB bus on the other side.
- An erroneous F-SB bus is monitored for normal recovery at regular intervals.

Vnet/IP communication

Vnet/IP is redundant. Independent subnets using bus 1 and bus 2 comprise redundant buses.

Normally, bus 1 is used for control communication. If a communication error occurs on bus 1, bus 2 is used to perform control communication.

A3.3.2 CPU redundant status

The availability of an SCS can be improved by making CPUs redundant. Each of the redundant CPUs can be in either control or standby states, which are unique to the CPU.

CPU status

In order to show the status of a redundant configuration, it is necessary to indicate the status of each CPU separately. The operating status of the CPU is called the CPU status.

- The CPU status indicates the operating status of the CPU.
- The processing of the SCS references the CPU status as necessary. The user can check the CPU status via the CPU's LED, the SCS State Management window of the SENG, and the Status Display view of HIS.
- If an error occurs in the standby CPU, the FAIL status is notified to the application logic via a system block.

The figure below illustrates the CPU status shift. Note that in order to explain the CPU status, the operating modes it can shift to the Initial mode are called "CTRL" and "STBY." These indicate whether the CPU has the control right and are specific to the redundant status, i.e., not related to the operating mode.

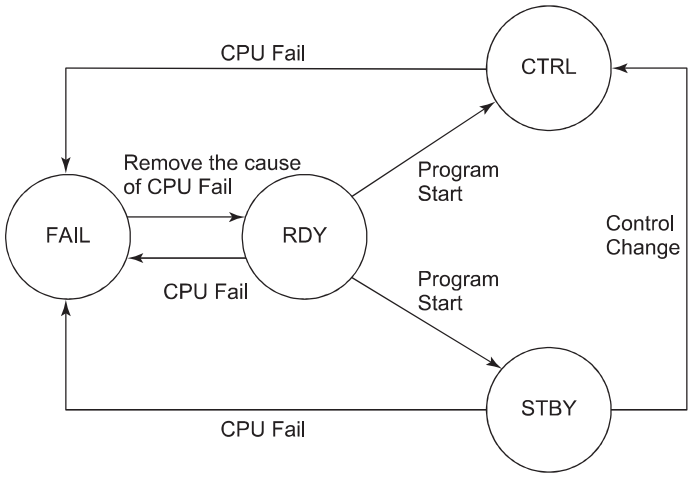


Figure A3.3.2-1 CPU status

FAIL (CPU stopped)

The power is supplied to the CPU, but the software is not running in this status.

RDY (CPU initializing status)

The system program is being set in the main memory in this status.

CTRL (control status)

The system program runs inside the CPU and the CPU has the right to access input/output modules in this status.

STBY (standby status)

The system program runs inside the CPU but the CPU does not have the right to access input/output modules in this status.

CPU status shift in redundant configuration

The figure below illustrates each CPU status and how it may shift in redundant configuration. The thick arrows from (a) to (d) indicate the flow from the startup to normal operation in redundant configuration. Note that the figure below does not represent the status by the mounting positions of the CPUs. Even if the states of the two CPUs are switched, the indication in the figure shows them in the same status.

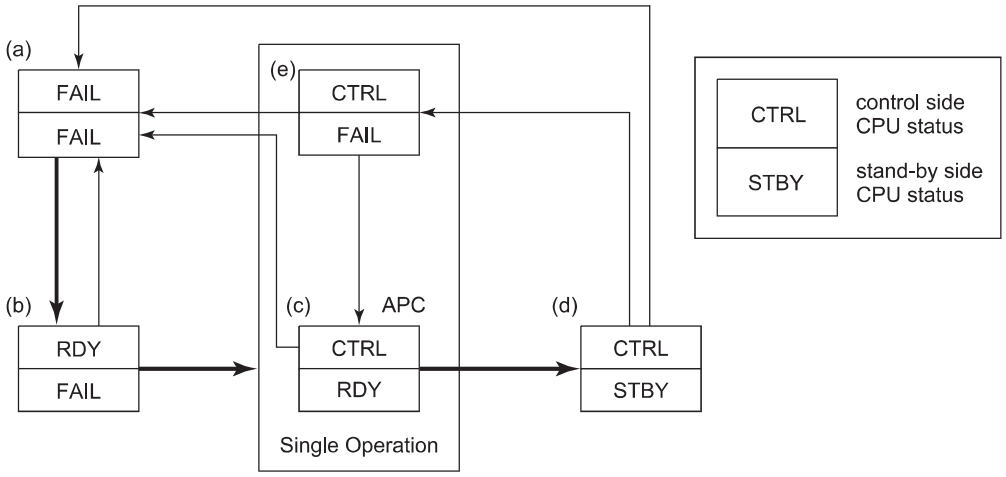


Figure A3.3.2-2 States at redundant configuration

Table A3.3.2-1 CPU status

Status	Description
(a)	CPUs on the both sides stopped.
(b)	The controlling CPU starts up and sets programs and databases in the main memory.
(c) (*1)	The controlling CPU obtains the control right and starts up the standby CPU. Upon launching, the standby CPU copies the image of the main memory of the controlling CPU into its main memory (this status is displayed as "APC" and not the same as status (e)). The controlling CPU executes the user application.
(d)	Both the controlling and standby CPUs operate normally in redundant configuration. This status is called the redundant control status.
(e) (*1)	In this status, the standby CPU is stopped in redundant configuration, or the controlling CPU is stopped and the control right is switched. The same operation as in single configuration is performed.

*1: Single operating status.

The CPU shifts to each status in the following manner.

Table A3.3.2-2 Conditions of CPU status shift

Before	After	Shifting conditions
(a)	(b)	• The power supply to the SCS is started. • SCS offline download is completed. • The system is restarted.
(b)	(c)	The controlling CPU started normally.
(c)	(d)	APC of the standby CPU is completed.
(d)	(e)	The control right is switched due to a failure of the controlling CPU hardware or the standby CPU failed.
(e)	(c)	The standby CPU is replaced or a CPU recovered from transient failure.
(b)	(a)	An error occurred in the self-diagnosis at startup.

Continues on the next page

Table A3.3.2-2 Conditions of CPU status shift (Table continued)

Before	After	Shifting conditions
(c)	(a)	A fatal error occurred while operating in single CPU operation.
(d)	(a)	Power failure occurred in the SCS (including momentary power failure).
(e)	(a)	A fatal error occurred while operating in single CPU operation.

APC status

The APC status refers to the status where the data in the CPU memory is being copied from the control side to the standby side.

The APC status can be checked by the LED on the CPU, the SCS Status Display window of the SENG or the Status Display view on the HIS. The start and end of the APC status are notified via a diagnostic information message.

A4. Outline of the safety system generation function

This section gives an overview of the tools used to configure and maintain a safety system.

It also describes the different types of applications that can be created by using ProSafe-RS.

Recreating an SCS project with R4 and selecting the engineering method

If an SCS project has been recreated, you must select the engineering method based on the presence of a safety I/O list.

Guidelines for selecting an engineering method

The engineering method of the project should be selected based on one of the following guidelines:

If a safety I/O list that is consistent with the SCS project exists, or if you are engineering by using a newly created safety I/O list, the I/O list engineering method is recommended. Select an I/O list engineering when you use iDefine as an engineering tool.

Also, when performing engineering for safety subsystem communication, select I/O list engineering.

If a safety I/O list that is consistent with the SCS project does not exist, or if you are using a SCS project that was created by using an SCS with RS original engineering, choose the RS original engineering method instead.

TIP If you upgrade to version R4, the metered license is applied regardless of the engineering method that you select.

Editor and tools that are used for I/O list engineering

The following table shows the editors and tools used when performing I/O list engineering.

You can start the SCS Manager from the System Structure Navigator in AD Organizer.

Table A4-1 Editor and tools that are used in I/O list engineering

Category	Operation	Means to operate editors and tools SCS Manager/AD Organizer	Editor or tool name	Remarks
Safety application	Safety logic definition	SCS Manager	Multi-Language Editor (*1)	-
	Variables and parameters definition	SCS Manager	Dictionary View (*1)	I/O variables are automatically created from the safety I/O list. Instances of subsystem communication I/O FB, PROFINET communication input FB, and fire and gas communication input FB are automatically generated from the safety communication I/O list. Internal variables and FB instances can be defined by iDefine.
I/O	I/O list definition	AD Organizer	Safety I/O Editor Safety Communication I/O Editor	The following information is generated: • Dictionary View • I/O Wiring View • I/O Parameter Builder • Communication I/O Builder
	Node/IOM detailed definition	AD Organizer	IOM Definition Editor	The information for the following is created: • I/O Wiring View • I/O Parameter Builder
System	Creation of SCS projects	SCS Manager	SCS Manager	The contents will be reflected in the AD Organizer.
	SCS project attribute	SCS Manager	SCS Project Properties	
	SCS constant definition	SCS Manager	SCS Constants Builder	-
	SCS parameter setting	SCS Manager	Hardware Architecture View	-
	POU definition	SCS Manager	Link Architecture View (*1)	-
	Safety communication association	SCS Manager	Binding List View	-
	SCS Link transmission data definition	SCS Manager	SCS Link Transmission Builder	-
RS generation	Database generation	AD Organizer	RS Generation Manager	-
	Authorize	SCS Manager	Integrity Analyzer	-
		SCS Manager	Cross Reference Analyzer	-
Test	Start test function	SCS Manager	SCS Manager (*1)	-

Continues on the next page

Table A4-1 Editor and tools that are used in I/O list engineering (Table continued)

Category	Operation	Means to operate editors and tools SCS Manager/AD Organizer	Editor or tool name	Remarks
Download	Offline download	SCS Manager	SCS Manager	-
	Online download	SCS Manager	SCS Manager	-
CENTUM integration	Tag and annunciator definition	SCS Manager	Tag Name Builder (*1)	-
	Alarm definition	SCS Manager	ProSafe-RS Alarm Priority Builder / Alarm Processing Table Builder	-
MODBUS communication	Definition of addresses of Modbus devices	SCS Manager	Modbus Address Builder	-
Subsystem communication	Communication I/O data definition	AD Organizer	Safety Communication I/O Editor	-
Safety subsystem communication	Communication I/O data definition	AD Organizer	Safety Communication I/O Editor	-
DNP3 communication	DNP3 slave definition	SCS Manager	DNP3 Communication Builder	-

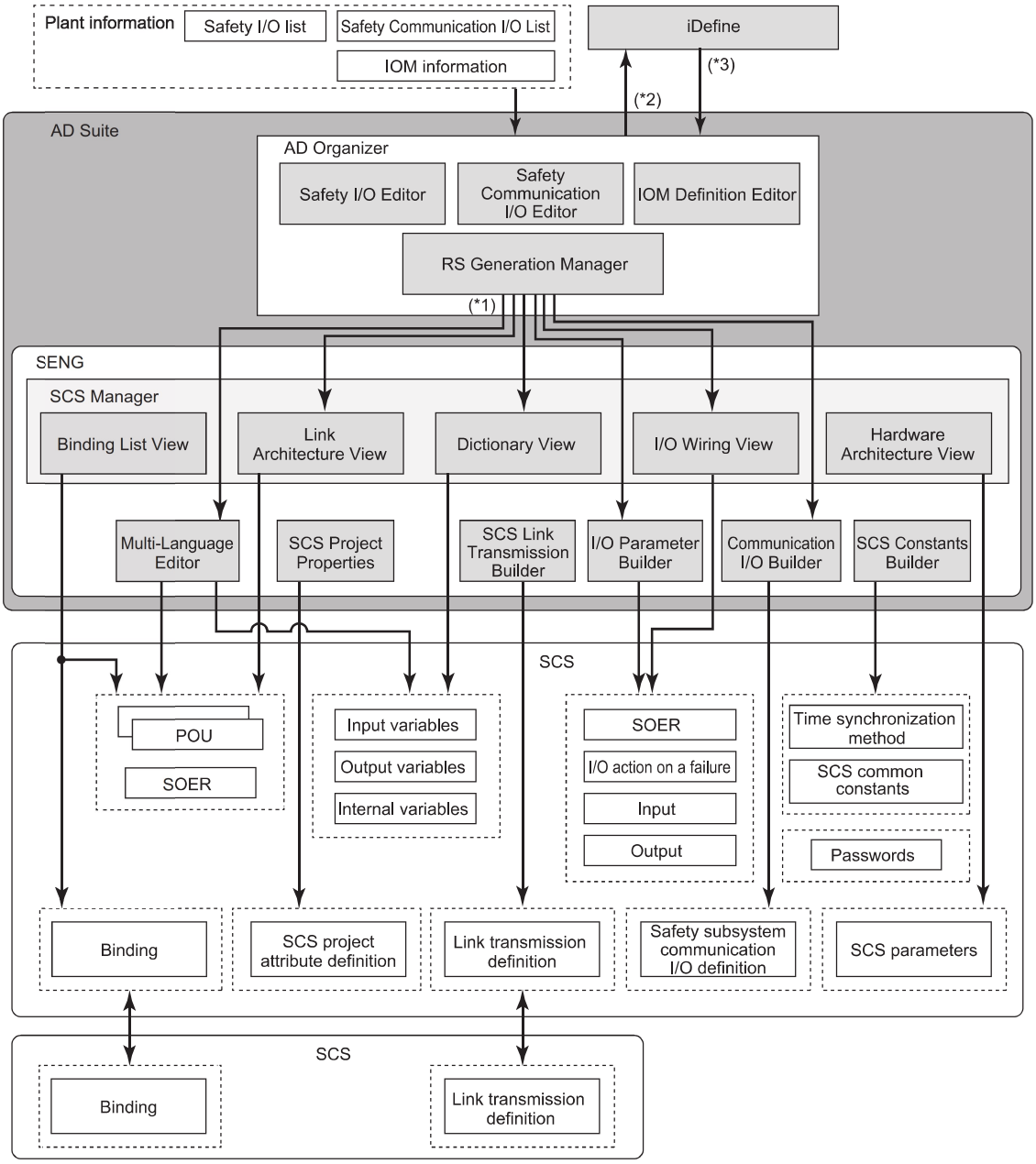
*1: iDefine can be used as well.

Safety application definition

Safety applications are created with tools and builders called from the AD Organizer and the SCS Manager.

When using AD Suite to perform I/O list engineering, you need to use the editors in AD Organizer to set the items instead of using I/O Wiring View, I/O Parameter Builder, and Communication I/O Builder.

If you select I/O list engineering and use iDefine, you can create the application logic by using iDefine based on the ProSafe-RS I/O file that was exported from AD Organizer. The ProSafe-RS I/O file is a file generated for engineering with iDefine based on the safety I/O list, safety communication I/O list, and IOM definition.



*1 : In the case of I/O list engineering, you can reflect the safety I/O list, safety communication I/O list, and IOM definition to the SCS Manager builder by running the reflection process through RS Generation Manager. If you run the reflection process on the engineering data that was created by using iDefine through RS Generation Manager, the application data can be reflected to the Multi-Language Editor and SCS.

*2 : AD Organizer exports the data that was created from the safety I/O list, safety communication I/O list, and IOM definition to iDefine.

*3 : AD Organizer imports the engineering data that was created by using iDefine.

Figure A4-1 Overview of safety application definition

AD Organizer

AD Organizer is installed in the SENG computer. You can perform the ProSafe-RS engineering by using AD Organizer. AD Organizer comes with some built-in engineering tools, and SCS Manager is one of them.

Safety I/O Editor

This is an engineering tool that can be used from AD Organizer.

The tool is used to create safety I/O lists based on plant information data and import them as engineering data.

It is also used to define variables that are related to the safety I/O. You specify the SCS node and IOM applicable to the P&ID tag and the associated connection information based on the information that is displayed in the Safety I/O Editor.

With this editor, you can export a file containing data for engineering with iDefine.

Safety Communication I/O Editor

This is an engineering tool that can be used from AD Organizer.

This tool is used to create safety communication I/O lists based on plant information data and import them as engineering data.

It is also used to define variables that are related to the safety communication I/O. You specify the SCS node and IOM applicable to the P&ID tag and the associated connection information based on the information that is displayed in Safety Communication I/O Editor.

With this editor, you can export a file containing data for engineering with iDefine.

IOM Definition Editor

This is an engineering tool that can be started from AD Organizer.

In the IOM Definition Editor, a list of nodes and I/O modules are displayed with their properties.

You can use the IOM Definition Editor to define the I/O module configuration and set the properties of nodes and I/O modules. If I/O module assignment information is not defined in the safety I/O list or safety communication I/O list, you can define the assignment of I/O modules to nodes by using IOM Definition Editor.

ADMDB

This is the server database that stores all the engineering data that is included in the AD Server. The revision history of the engineering data and the hardware configuration information are also stored in this database.

The AD Server manages the engineering data.

Generation Manager

For SCS projects that are created with I/O list engineering, Generation Manager reflects the information of the safety I/O lists, safety communication I/O lists, and I/O module configuration and builds SCS projects.

Hardware Architecture View

- Set the configuration name.
- Define the IP address of the SCS.

Link Architecture View

- Configuring the security settings of the SCS project.
- Defining the POU.(*1)
- Adding variable groups.
- Starting the Multi-Language Editor to edit the POU that you have defined.

*1: POU: Program Organization Unit It is a generic term for the programs, function blocks (FB), and functions (FU) that are written with the function block diagram (FBD) and ladder diagram (LD)

SCS Project Properties

Defining Project properties including station type, domain number, and station number of SCS.

Designating location of the integrated CENTUM project folder, in the case of CENTUM Integration Configuration.

SCS Constants Builder

Setting SCS common constants and time synchronization method.

Dictionary View

If you select the RS original engineering method, the Dictionary View is used to set the parameters of FUs and FBs and define project variables. If you select the I/O list engineering method, the variables that were defined by using AD Organizer and iDefine are read-only in Dictionary View.

Multi-Language Editor

Edit the POUs for the LBD, LD, and ST.

POUs that were defined by using iDefine are read-only in Multi-Language Editor.

Binding List View

Binding variables from the producer to the consumer of Inter-SCS safety communication.

SCS Link Transmission Builder

Defining SCS link transmission safety communication and SCS global switch communication.

I/O Wiring View

In the SCS project where the RS original engineering method is selected, the I/O Wiring View is used to define the following:

- Analog I/O module, digital I/O module, universal type I/O module (these three types of modules are collectively called "AIO/DIO modules"), and communication module
- Wiring between I/O module channels and I/O variables

If you select I/O list engineering, this builder is read-only.

I/O Parameter Builder

In the SCS project where the RS original engineering method is selected, I/O Parameter Builder is used to configure the node, module, and channel parameters, including the settings for the operation when a fault is detected in an I/O module or channel, and to define SOER collection through DI/DO.

If you select I/O list engineering, this builder is read-only.

Communication I/O Builder

For SCS projects for which I/O list engineering is selected, this builder becomes read-only. Use Safety Communication I/O Editor when you assign communication I/O data for safety subsystem communication and perform wiring of communication I/O variables. The contents of Safety Communication I/O Editor will be reflected in this builder by running a reflection from AD Organizer.

CENTUM integration application definition

The following figure shows the outline of CENTUM integration application definition and the associated builders.

These builders are opened from the engineering launcher of the SCS Manager.

- Tag Name Builder
  This builder defines tag names for FBs and variables which can be used for CENTUM Integration Configuration, and also defines annunciator messages.

  Defining a tag name results in the creation of a mapping block for CENTUM Integration Configuration.

  When engineering by using iDefine, you can also define the tag names for FBs and variables by using iDefine. Use the reflection process from Generation Manager to reflect the definitions in Tag Name Builder. Tag names that were defined by iDefine are read-only in Tag Name Builder.
- Alarm Priority Builder
  This builder defines alarm priority. The condition of alarm activation is set to each alarm priority as in CENTUM.
- Alarm Processing Table Builder
  The Alarm Processing Table Builder is used to import the ‘Alarm Processing Table defined in CENTUM’ to SCS project.

  This table determines the priority of process alarms that are generated from mapping blocks when integrating with CENTUM.

When engineering by using iDefine, you can also configure the tag names in iDefine. The tag names are read-only except for configured tools.

In a CENTUM integration structure, the application of ProSafe-RS needs to be defined with those builders. Furthermore, engineering of CENTUM including SCS definition and tag list generation needs to be executed on CENTUM ENG. This allows HIS to access SCS data with a tag name and to display annunciator messages.

The following figure provides an overview of CENTUM Integration Application Definition.

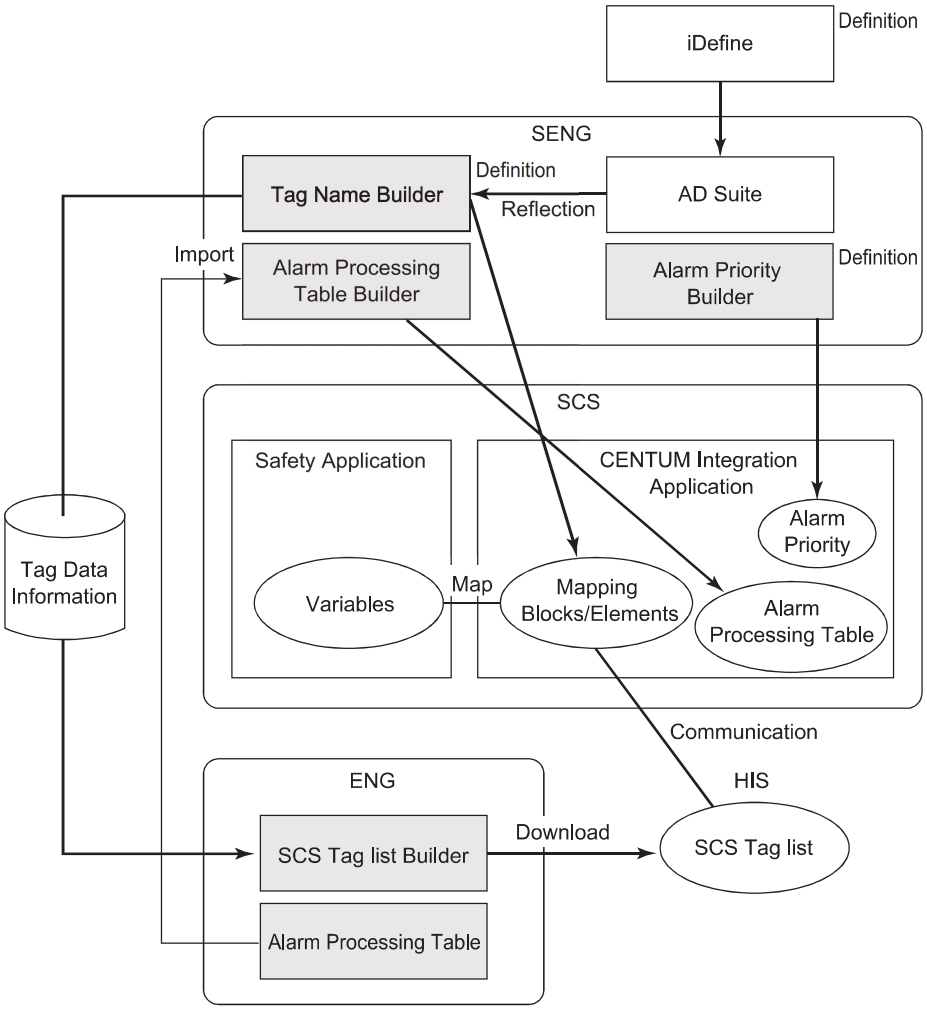


Figure A4-2 Outline of CENTUM Integration Application Definition

Defining applications that use communication modules

In ProSafe-RS, you can create an application that exchanges data with other system through a communication module. Modbus slave communication, Modbus subsystem communication, and safety subsystem communication are supported. Safety subsystem communication can be used with SCSP3 only. In addition, you can create DNP3 communication applications in SCSU1. Modbus slave communication and Modbus subsystem communication are interference-free functions. Safety communication is included in safety subsystem communication.

The following builder is used for Modbus slave communication:

- Modbus Address Builder
  It defines the Modbus device address.

The following figure shows the outline of the definitions of Modbus slave communication application.

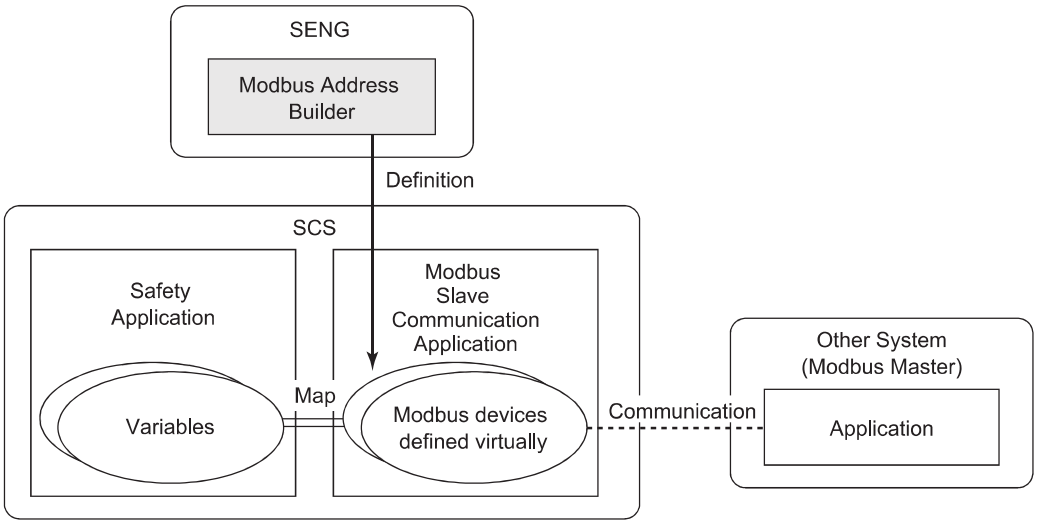


Figure A4-3 Outline of Modbus slave communication application definition

The following builder or editor is used for subsystem communication:

- Communication I/O Builder (for RS original engineering)
- Safety Communication I/O Editor of AD Organizer (for I/O list engineering)
  It defines the communication data, and allocates the communication I/O FB there.

The following two types of subsystem communication are supported:

- Using the serial communication module, you can create an application for subsystem communication between SCS and Modbus PLC. By creating an application for subsystem communication between SCS and ProSafe-SLS, you can acquire events and data of ProSafe-SLS.
- Using Ethernet communication module, you can create an application for the subsystem communication between the SCS and Modbus/TCP PLC.

The following editor is used for fire and gas communication:

- Safety Communication I/O Editor of AD Organizer
  Define communication data and assign the PROFINET communication I/O FB and fire and gas communication FB to the communication data.

  Using fire and gas communication modules, you can create an application for safety subsystem communication between the SCS and fire and gas devices.

The following builder is used to define DNP3 communication applications:

- DNP3 Communication Builder
  This builder enables SCS to act as a DNP3 slave station and associates DNP3 data with application logic variables.

The following figure shows the outline of the DNP3 communication application definitions.

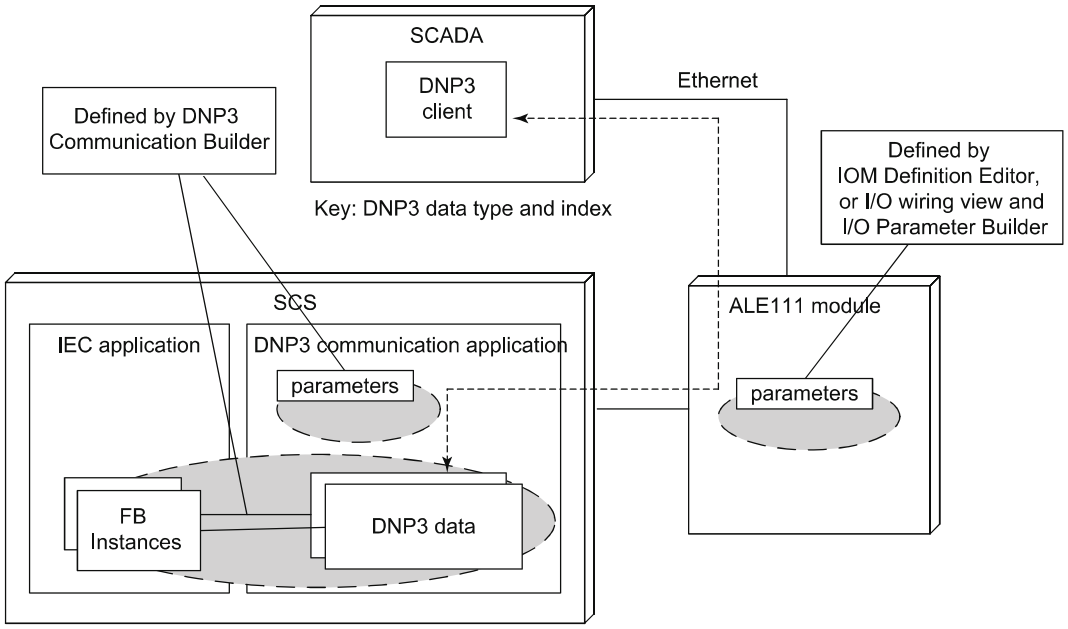


Figure A4-4 Outline of DNP3 communication application definition

CI Server integration application definition

The following describes the builder and outline of the CI Server integration application definitions. CI Server integration is an interference-free function.

In CI Server integration, you can define I/O modules and create function blocks in addition to using the following builders and tools:

- Domain Properties Setting Tool
  It selects the operating mode of Vnet/IP-Upstream.
- Message Cache Tool
  A group is defined when the network configuration of Vnet/IP-Upstream is in the narrow-band mode.
- Tag Name Builder
  You can enter tag name, and other information to the data to be handled in CI Server.

  When engineering by using iDefine, you can also define the tag names for FBs and variables by using iDefine. Use the reflection process from Generation Manager to reflect the definitions in Tag Name Builder. Tag names that were configured by using iDefine are read-only in Tag Name Builder.

Engineering tools

The following describes the tools that are used after you have created a ProSafe-RS application:

Integrity Analyzer

The Integrity Analyzer is used to analyze the safety of existing created application logics. It detects unauthorized FB /FU as the safety function, and outputs results of analyzing on screen or on the analysis report.

Cross Reference Analyzer

It shows, on screen or on the analysis report, the difference between the application previously downloaded (which runs currently on SCS) and the application to be downloaded soon as well as the extent of impact in case of downloading. The Cross Reference Analyzer is for limiting the scope of retesting when application logic is modified.

- ## Self-Documentation function

  This is for printing user applications. The entire definitions of an SCS project or any parts can be selected as a printed item.

- ## Project Attribute Tool

  This tool can be used to display the attribute of an SCS project.

- ## Test Project Creation Tool

  This tool can be used to copy a project that is running at a plant site and create a project for test purpose.

- ## Import/Export function

  Import or export functions can be used to import or export SCS project data. Therefore, these data can be used for test functions or for reusing applications.

- ## Project Comparing Tool

  This tool can be used to detect the difference between two specified SCS projects and to display and print the result.

- ## Version Control Tool

  This is for controlling the version history of an SCS project to support the project updates by users.

  By using Version Control Tool, you can save (check-in) the project data of an SCS project at a certain point upon adding a version number and restore (check-out) project data of a certain version. If you are performing I/O list engineering, start this tool from AD Organizer. If you start it from the Start menu, the data of AD Suite cannot be handled by the tool.

- ## Master Database Restoring Function

  This function is used to restore the contents of the master database as the work database. Use this function to discard changes made to the work database and use the master database as the data subject to engineering (work database). If you are performing I/O list engineering, start this tool from AD Organizer. If you start it from the Start menu, the data of AD Suite cannot be handled by the tool.

- ## Database Validity Check Tool

  The Database Validity Check Tool is used to check the integrity of the database in the work database and master database of SCS project, and SCS database in SCS. The master database can be repaired if the master database has lost validity due to such as an error that has occurred during online change download. This repair function of the tool repairs the master database by replacing it with the work database.

- ## SCS Information

  This function is used to display and print SCS project usage conditions such as POUs used within the SCS and the number of variables. The number of licenses available is displayed separately for SIL 2 and SIL 3. This function can also be used to check the database revisions in the SCS project, number of project I/O licenses and their usage. You need to build an SCS project before using this function.

A4.1 Window components common to builders

Multiple builders are used for engineering applications that will run on the SCS. This section describes the base window layout common to all the builders, taking the SCS Constants Builder window as an example.

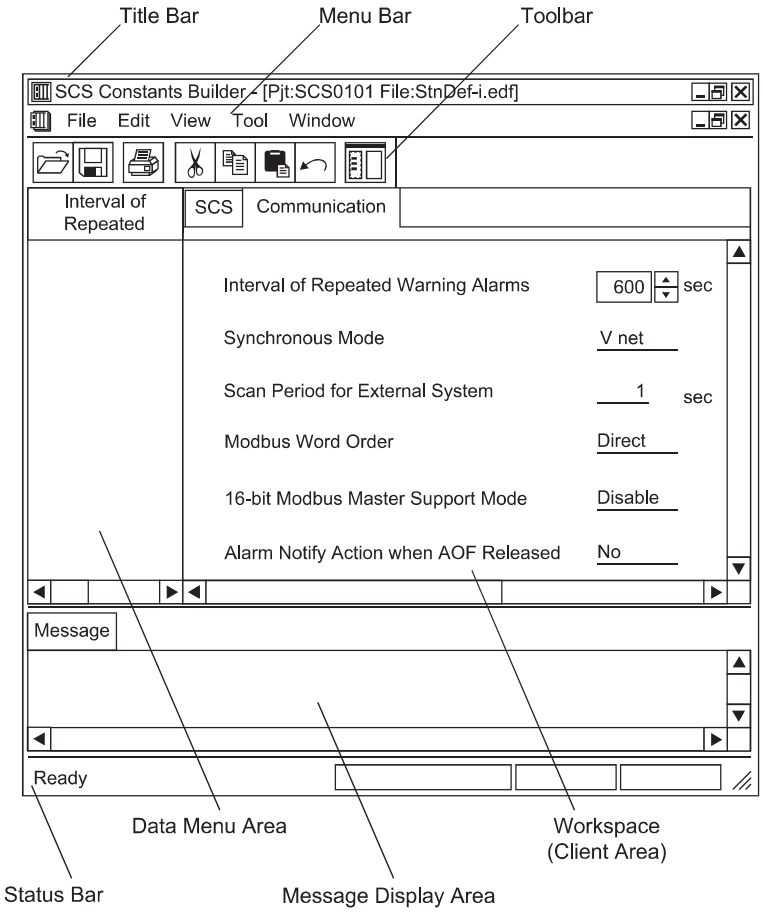


Figure A4.1-1 Window of SCS Constants Builder

Title bar

The title bar displays project name, file name, etc.

Menu bar

The menu bar contains the [Edit], [Tools] and other menus. The menu structure of the menu bar differs depending on the builder; the menu bar used on most builders is as follows.

File menu

Table A4.1-1 File menu

Menu item	Description
Open	Opens a file created by this builder and saved with a specific name (SVA file)
Close	Closes the window
Save	Saves the data displayed in the window in a file
Save As (*1)	Saves the data displayed in the window in a file with a specific name

Continues on the next page

Table A4.1-1 File menu (Table continued)

Menu item		Description
External File ->	Import	Imports the contents saved in a file with a specific format to the currently opened window
	Export	Exports the contents of the currently opened window into a file with the specific format
Properties		Displays a dialog box for displaying and editing information related to the window properties
Print		Launches Document Generator for printing the data displayed in the window
Status Label -> (*2)	Custom Import	Imports the alarm status texts modified on the CENTUM builders.
	Delete	Deletes the alarm status texts imported from the CENTUM builders.
Latest File		Shows a list of files saved with specific names (SVA files) that were opened in the past
Exit SCS Constants Builder (*3)		Closes SCS Constants Builder

*1: On the SCS Constants Builder, you need to save the settings separately on each tab sheet.
*2: Only available on SCS Constants Builder
*3: Builder name is displayed as the affix of the menu name.

TIP If there is no document window, only [Open], [Latest File] and [Exit SCS Constants Builder] are displayed.

Edit menu

Table A4.1-2 Edit menu

Menu item	Description
Undo	Cancels the previously performed edit operation
Cut	Deletes the selected character string and copies it onto the clipboard
Copy	Copies the selected character string onto the clipboard
Paste	Inserts the character string stored in the clipboard
Clear	Clears the character string of the selected field
Find	Displays a dialog box to search for a specified character string set in the builder
Replace	Displays a dialog box to search and replace a specified character string set in the builder

View menu

Table A4.1-3 View menu

Menu item	Description
Toolbar	Determines whether or not to display the toolbar
Status Bar	Determines whether or not to display the status bar
Data Menu Area	Determines whether or not to display the data menu area
Message Display Area	Specifies whether or not to show the message display area

Tools menu

Table A4.1-4 Tools menu

Menu item	Description
Environment Setting...	Starts Builder Environment Tool for setting the operation environment commonly used for builders

Window menu

Table A4.1-5 Window menu

Menu item	Description
Cascade	Arranges document windows so that they overlap
Tile Horizontally	Arranges document windows horizontally
Tile Vertically	Arranges document windows vertically
Arrange Icons	Arranges minimized document windows

Toolbar

The toolbar contains icons representing frequently used functions in the menu bar.

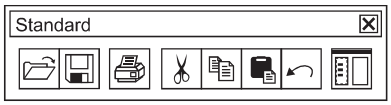


Figure A4.1-2 Toolbar

Table A4.1-6 Functions assigned to the toolbar

Button	Name	Assigned function
	Open	Same as [Open] of the [File] menu
	Save	Same as [Save] of the [File] menu
	Print	Same as [Print] of the [File] menu
	Cut	Same as [Cut] of the [Edit] menu
	Copy	Same as [Copy] of the [Edit] menu
	Paste	Same as [Paste] of the [Edit] menu
	Undo	Same as [Undo] of the [Edit] menu
	Display/Hide Data Menu	Same as [Data Menu Area] of the [View] menu

Data menu area

The data menu area has the following functions.

- Displays input guidelines for the selected data (e.g., meaning of an input item and data input range).
- If data has options, the area displays the option menus and allows selecting an option. In that case, it is also possible to select an option by pressing a key.

- Displays tree view and changes the workspace tabs (excepts for SCS Constants Builder).

Message display area

The message display area displays the execution result of saving files, etc.

A4.2 Types of downloading

The downloading functions transfer SCS execution data which contain application logics to an SCS.

The SCS database is saved as the master database in the SENG and the same data as in the SCS is maintained at all times. There is no function to upload the SCS execution data to the SENG because the SCS execution data is saved in the SENG as the master database.

Overview and types of downloading

Offline download

This function downloads a database generated from application logic created in the SENG. During download, the functions running on the SCS stop and resume operation after the completion of downloading.

Online change download

This function downloads only a portion of database generated from application logic, created in the SENG, that have been updated since the last download. The functions running on the SCS keep operating during the download as well. Note that online change download may not be possible depending on the content of the updates.

Master database offline download

This function downloads the execution data that was active in an SCS again after replacing a CPU module. The SCS database saved in the master database on the SENG is downloaded. This download is performed when replacing hardware. In case of a redundant CPU module, this download is not required if only one module is replaced.

TIP

Close the I/O lock window when performing the following operations.
Otherwise, an error message will be displayed and the downloading will be stopped.

- Online change downloading
- Offline downloading
- Master database offline downloading

IOM download

This function downloads the execution data that was active in an input/output module to a new input/output module after replacing it. The data of the input/output module (part of the SCS database) saved in the master database on the SENG is downloaded.

This download can only be performed when replacing hardware of input/output modules.

Save and download operation marks

The operation marks set on the HIS can be saved in SENG.

The saved operation marks can be downloaded to the SCS.

SEE ALSO

For more information about saving and downloading operation marks, refer to:

B7.1, “Engineering on the SENG side” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Relationship between downloading functions and databases

The destination database for saving varies depending on the type of downloading. The relationship between different types of downloading and databases is explained below.

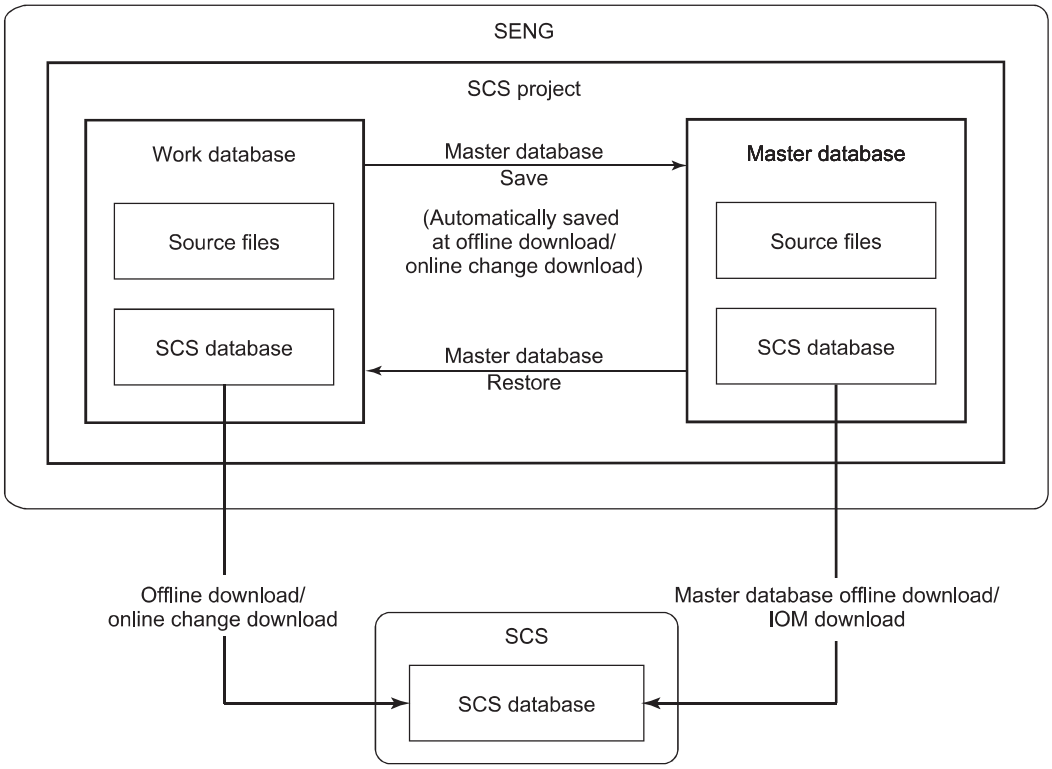


Figure A4.2-1 Relationship between downloading functions and databases

TIP

- Master Database Restoring Function is provided in order to copy the master database to the work database in case a recovery is needed. Do not operate the master database folder/files directly by using Windows explorer, or edit the master database.
- SCS projects are also registered in the ADMDB and managed by the AD Server.

Offline download

The work database generated by building is downloaded to an SCS. The master database is overwritten by the work database.

Online change download

Only differences between the work database generated by building and the master database are downloaded to an SCS. The master database is overwritten by the work database.

Master database offline download

The master database is downloaded to an SCS.

IOM download

Only data in the master database related to input/output modules is downloaded to an SCS.

Relationship between downloading functions and SCS security levels

Since the downloading functions attempt to write data to an SCS, download operations may not be allowed depending on the SCS security level. Before performing the downloading functions, it is necessary to use the SCS security level operation function and change the security level of the SCS.

The table below shows whether or not each type of download is allowed according to the security level.

Table A4.2-1 Relationship between downloading functions and SCS security levels

Security level	Offline download	Online change download	Master database offline download	IOM download	Save and Download Operation Marks
Level 2	-	-	-	Yes (only for failing input/output modules)	Yes
Level 1	-	Yes	-	Yes (only for failing input/output modules)	Yes
Level 0	Yes	Yes	Yes	Yes (only for failing input/output modules)	Yes

A5. Configuration of maintenance function

This section describes the outline of the functions used for maintenance of SCS and field devices.

Outline of functions to use for maintenance

Set SCS security level

This is for changing the SCS security level in the case of downloading the database to the SCS or forcing parameters.

I/O Lock window

This is for locking/unlocking I/O channels during maintenance, and shows the locking status of the I/O channels. When inputs or outputs are locked, it is possible to set their values.

Communication I/O Lock window

This is for locking/unlocking I/O of subsystem communication and safety subsystem communication during maintenance. It shows the locking status of the inputs/outputs. It is possible to set their values when inputs or outputs are locked.

SCS Link Transmission Lock window

During maintenance, locking or unlocking the communication data of link transmission can be performed on this window. The locking and unlocking status can also be monitored. When a communication data is locked, the value of the communication data can be changed.

Inter-SCS Communication Lock window

This is for locking or unlocking inter-SCS safety communication FBs for each SCS during maintenance and shows the locking status of the FBs. When inter-SCS safety communication FBs are locked, it is possible to set their values.

Restart SCS

This is for restarting SCS.

Master database offline download

This is for downloading the master database to SCS and restarting the SCS.

Save operation marks/Download operation marks

Operation marks specified for SCS tags on an HIS in the CENTUM integration structure are initialized and thus lost when offline download to the SCS, master database offline download or SCS restart (including when recovering from power failure) are executed. This function makes it possible to recover initialized operation marks to the status at the last saved operation.

The Save Operation Marks is a function to save operation marks specified for tags on an HIS in the SENG.

The Download Operation Marks is a function to download saved operation marks to the SCS.

SEE ALSO For more information about saving/downloading operation marks, refer to:

B7.2.3, “Other builders” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

A6. Overview of the SCS Maintenance Support Tool

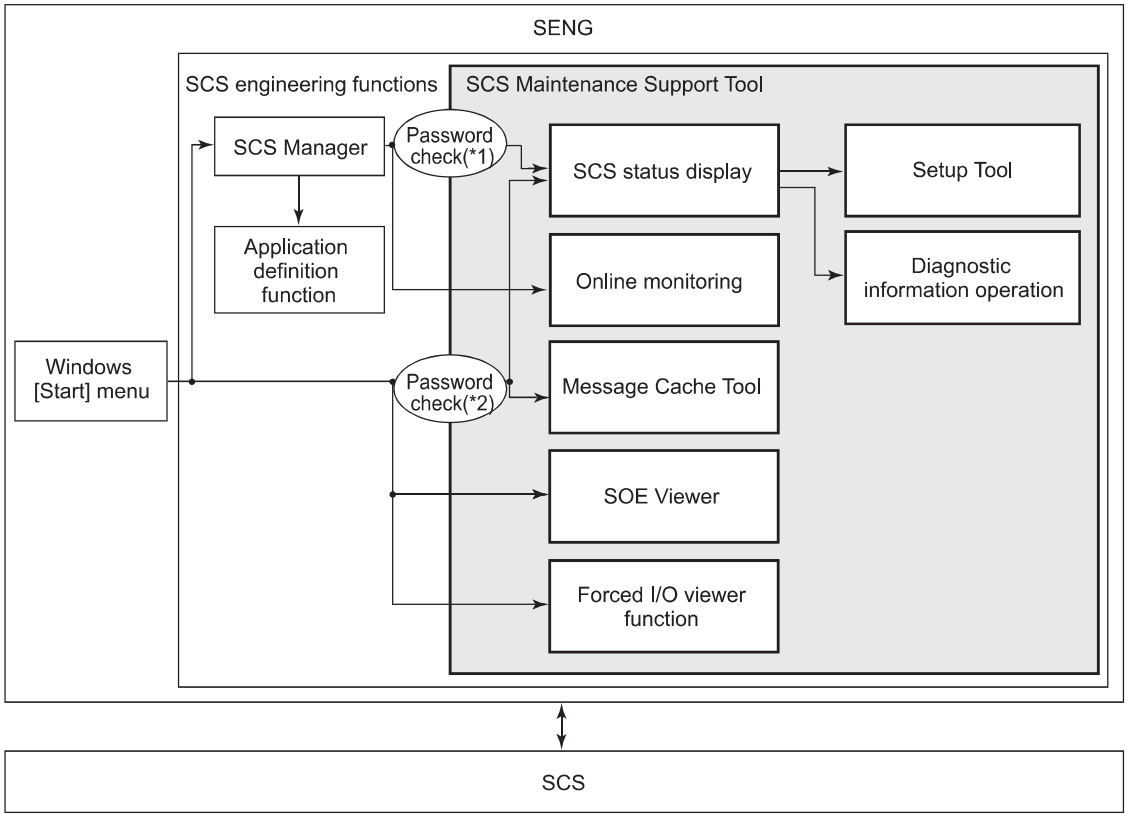
SCS Maintenance Support Tool provides functions to keep track of the SCS status in ProSafe-RS maintenance. For example, SCS Maintenance Support Tool is used for when maintaining applications, analyzing cases of tripping by demand from the plant and analyzing diagnostic information generated in the SCS. SCS Maintenance Support Tool can always be used as long as the SCS is in operation regardless of its security level.

SCS Maintenance Support Tool has the following functions:

- SCS status display
- Diagnostic information operation
- Online monitoring of application logic
- Message Cache Tool
- SOE Viewer
- Forced I/O viewer function

A6.1 Relationships among functions of SCS Maintenance Support Tool

The figure below shows the relationships among the functions included in SCS Maintenance Support Tool.



*1: When the "Access Control and Operation History Management Package" is used, password checking is not performed because user authentication check is done when SCS Manager is started.
*2: When the "Access Control and Operation History Management Package" is used, password checking is not performed because user authentication check is done when the SCS Maintenance Support Tool is started.

Figure A6.1-1 Relationships among functions included in SCS Maintenance Support Tool

SCS status display

The tools for showing the SCS running status include SCS Status Overview window and SCS State Management window.

The SCS Status Overview window and the SCS State Management window are called up from the Maintenance Launcher menu of SCS Manager. The SCS Status Overview window can be launched from the [Start] menu of Windows. Note that the SCS Status Overview window and the SCS State Management window cannot be displayed at the same time. If you call up and display the SCS Status Overview window or the SCS State Management window again from the Maintenance Launcher menu of SCS Manager, the currently displayed window is closed and the newly called window appears.

If you close the SCS Status Overview window or the SCS State Management window, all windows started from that window are closed. The windows related to the SCS Status Overview window or the SCS State Management window will not be closed even if you close the SCS project in SCS Manager.

Diagnostic information operation

The Diagnostic Information window is provided as a tool for displaying diagnostic information stored in SCS.

The Diagnostic Information window is opened from the SCS Status Overview window or the SCS State Management window. The Diagnostic Information window displays diagnostic information in the range selected by the engineer in the SCS State Management window.

Online monitoring

The online monitoring function displays the operating status of the application logic in SCS. Using this function, the user can keep track of the values of variables as well as the condition statuses on FBD and LD.

Message Cache Tool

Message Cache Tool is used for checking the diagnostic information messages and SOE event acquisition conditions. Moreover, it is used to change various Message Cache Service settings and manage the collected data.

SOE Viewer

SOE Viewer is a tool to display event information held by SCS. It also displays the diagnostic information messages. The SOE Viewer is capable of displaying events and messages in chronological order, which helps you analyze messages output from the SCS.

Forced I/O Viewer function

Forced-I/O information is a collection of information such as variables that are locked in the Lock window of SENG by using the forcing function.

Forced I/O Viewer function is a function to display the forced-I/O information in a list. Forced-I/O information of multiple SCSs can be displayed collectively.

Forced I/O Viewer function consists of Forced I/O Viewer that displays the forced-I/O information and Forced I/O Viewer Setup Tool that makes the setting for collecting the forced-I/O information.

Customizing SCS Maintenance Support Tool

Setup Tool is used to customize the display and operation methods of SCS Maintenance Support Tool. Setup Tool allows you to define the settings related to fonts and operations for the SCS Status Overview window, the SCS State Management window and the Diagnostic Information window.

A6.2 Application examples at maintenance

Maintenance can be classified into two types: regularly performed maintenance and maintenance performed when an unexpected error occurs. This section describes how to use SCS Maintenance Support Tool when an unexpected error occurs, for example, in a case where the SCS diagnostic function detects errors in input/output modules.

Maintenance operations are performed by maintenance personnel in most cases. This section assumes that analysis of causes is performed by engineers and tasks of eliminating abnormality is handled by maintenance personnel, and describes the tasks involved separately.

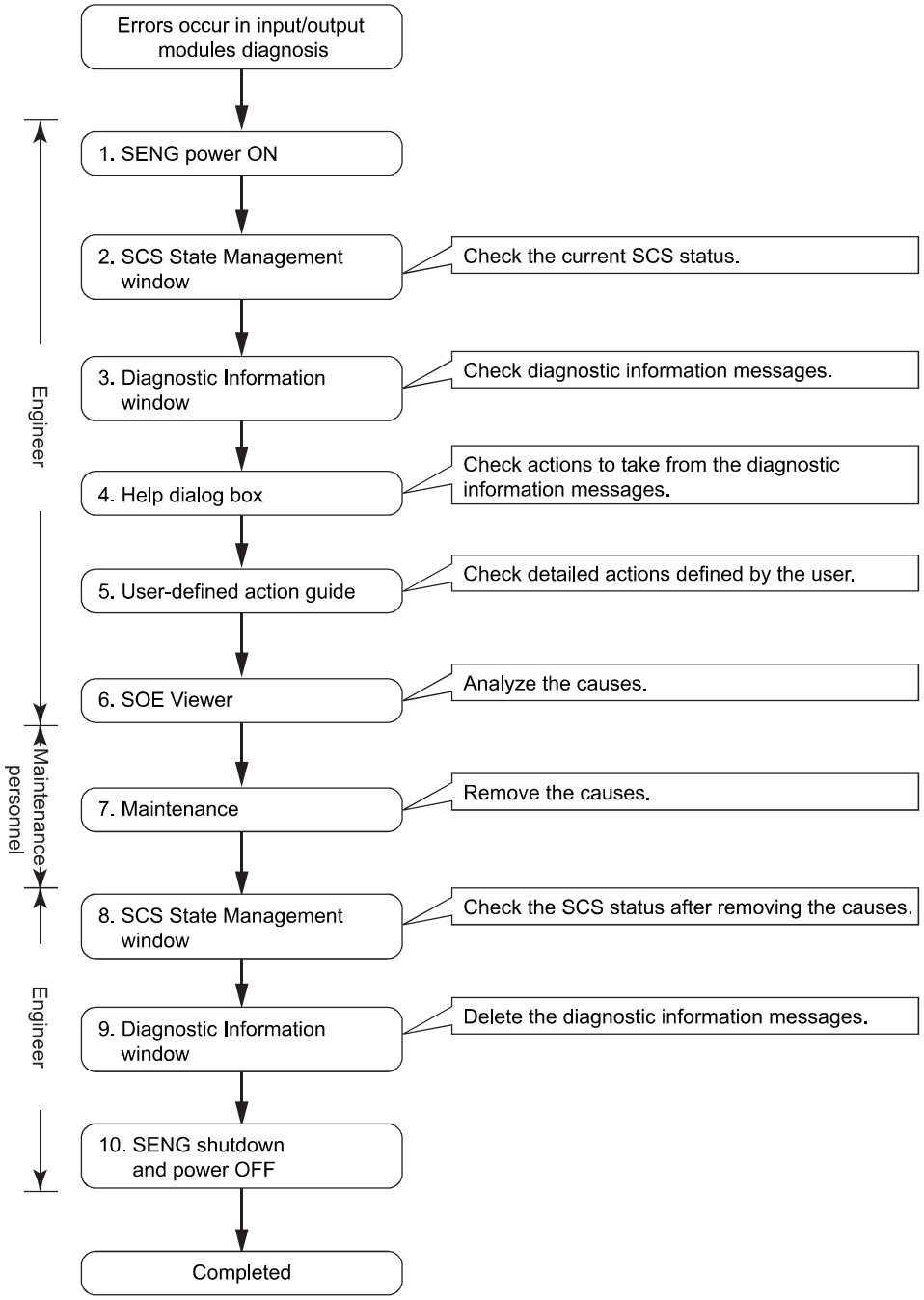


Figure A6.2-1 Workflow for maintenance operation

Step 1: SENG power on

The engineer turns ON the power supply of the SENG in order to analyze the causes of the error diagnosed.

Step 2: SCS State Management window

The engineer launches the SCS State Management window of a station that detected a diagnosed error from SCS Manager. The engineer checks the current status based on the display. The diagnostic information mark is displayed for the input/output modules on which the diagnosed errors occurred. The engineer selects those input/output modules and then displays the Diagnostic Information window in order to check the diagnostic information messages related to those input/output modules.

Step 3: Diagnostic Information window

The engineer checks the messages output by the SCS diagnostic functions. An action to be taken for a diagnostic information message can be checked with a help message displayed by double-clicking the diagnostic information message and displaying the Help dialog box. To acknowledge the diagnostic information message, click the corresponding message in the Diagnostic Information window and then click [Acknowledgement] button on the toolbar. The Acknowledgement dialog box appears. Click the [OK] button in this dialog box; the status of the diagnostic information message is placed in the acknowledged status (operation when acknowledging individually).

Step 4: Help dialog box

The Help dialog box displays help messages corresponding to message numbers. If the counter-actions measures specific to devices are available, the engineer can call the user-defined action guide from the Help dialog box to check actions to take.

Step 5: User-defined action guide

The engineer learns what actions to take against the error from the information of user-defined action guide. Note that the guide must be defined in advance by the engineers.

Step 6: SOE Viewer

The engineer identifies the causes of the error based on the diagnostic information messages and/or SOE event information at the time diagnosed errors occur. The engineer then identifies a procedure to eliminate the causes. It is possible to keep messages as records by saving them in a file.

Step 7: Maintenance

The maintenance personnel removes the causes according to the operation procedure made by the engineer.

Step 8: SCS State Management window

The engineer displays the SCS State Management window and checks that the input/output modules have recovered from the error.

Step 9: Diagnostic Information window

The engineer deletes the messages output by the SCS diagnostic functions. To delete a diagnostic information message, click the corresponding message in the Diagnostic Information window and click [Deletion] button on the toolbar; the Deletion dialog box appears. Click the [OK] button in this dialog box to delete the diagnostic information message (using the operation to delete individual message).

Step 10: SENG shutdown and power off

After analyzing the cause of the diagnosed error and removing the cause, if the SENG is not used normally, the engineer shuts the SENG down and turns the power OFF.

A6.3 Customization of the SCS Maintenance Support Tool window

The operation environment of the SCS Maintenance Support Tool window can be customized.

Items that can be customized

You can use Setup Tool to specify the following operation environment settings:

- Selecting the method of acknowledgment/deletion
  The method to acknowledge/delete diagnostic information messages can be specified.
- Font setting
  The font and font size used in the SCS Maintenance Support Tool window can be specified.
- Color selection
  The background color and text color can be specified.

Setup Tool consists of the following tabs:

- General
  Allows settings for the entire SCS Maintenance Support Tool
- Diagnostic Information
  Allows settings for the Diagnostic Information window

Displaying Setup Tool

Click the [Setup Tool] button on the toolbar of the SCS Status Overview window or the SCS State Management window. SCS Maintenance Setup dialog box appears.

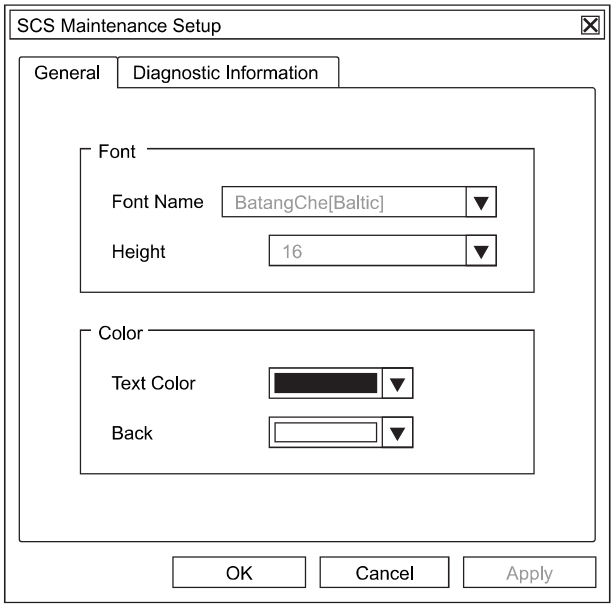


Figure A6.3-1 General Tab of SCS Maintenance Setup Dialog Box

General tab

Make settings related to the overall appearance of the window including font and text color in the "General" tab.

Font

The setting items related to font are as follows.

- Font name
  This item is used to select a font name. The font specified here is used in all windows related to SCS Maintenance Support Tool. The default font installed in SENG becomes the initial font.
- Height
  This item is used to select a font size. The font size specified here is used in all windows related to SCS Maintenance Support Tool.

Color

The setting items related to color are as follows.

- Text color
  This item is used to select a text color. The text color specified here is used in all windows related to SCS Maintenance Support Tool.
- Back
  This item is used to select a text background color. The background color specified here is used in all windows related to SCS Maintenance Support Tool.

Diagnostic Information tab

Make settings for operations specific to the Diagnostic Information window in the "Diagnostic Information" tab.

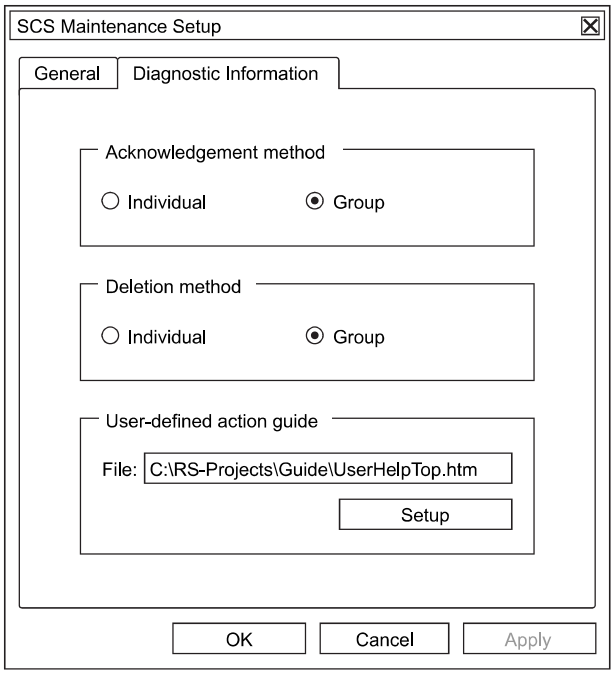


Figure A6.3-2 Diagnostic Information Tab of SCS Maintenance Setup Dialog Box

Method of acknowledgment

The setting items related to the method of acknowledgment are as follows.

- Individual
  Select this option to acknowledge the diagnostic information messages individually. It is recommended to use [Individual] during a normal operation.
- Group

Select this option to acknowledge all diagnostic information messages in a batch.

Method of deletion

The setting items related to the method of deletion are as follows.

- Individual
  Select this option to delete the diagnostic information messages individually. It is recommended to use [Individual] during a normal operation.
- Group
  Select this option to delete all diagnostic information messages in a batch.

IMPORTANT

If you select [Group] as the acknowledgement/deletion method, all diagnostic information messages displayed in the screen become the target of the acknowledging/deleting operation. So, you should not use this function during normal plant operation; use it only temporarily when testing, etc.

User-defined action guide

In the help dialog box for each diagnostic information message, a help text regarding the causes and resolution for the occurred message can be displayed as a guidance. Copying the default User Defined Action Guide and editing the contents can create a new user-defined action guide. The procedure is as follows:

1. Click the [Setup] button. The dialog box is displayed to specify the folder for copying the default action guide.
2. Click the [OK] button after specifying a folder. Then the file will be copied. The file name will be UserHelpTop.htm. The file name should not be changed.
   Edit the copied guide accordingly so as to create a new user-defined action guide.

SEE ALSO For more information about how to create a user-defined action guide, refer to:

"■ User-defined action guide" in H6.3, "Diagnostic information message help function" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

A7. Virtualization platform

ProSafe-RS runs not only on physical computers but also on virtual machines on the virtualization platform. This section describes an outline of the virtualization platform, the system configuration, the software environment, and precautions.

Terminology

This section describes virtualization and related terms.

Virtualization is a technology to make a single unit of physical hardware look like multiple logical units of hardware, or to make multiple units of physical hardware look like a single unit of logical hardware. In this document, we mainly deal with the technique that makes it look like there are multiple computers in the server.

- Virtualization software

  Refers to the software that realizes virtualization.

- Virtualization host computer

  Refers to a server on which virtualization software is installed and that is able to make it look like there are multiple computers in it.

- Virtual machine

  Virtualization can make it look like there are multiple computers on the virtualization host computer, and these pseudo computers are referred to as virtual machines.

- Host OS

  Refers to the OS operating as the foundation on the virtualization host computer.

- Guest OS

  Refers to the OS running the virtual machines.

- Thin client

  Refers to a client computer that contains minimum functions and performance and that is used for user interface.

A7.1 Outline of virtualization platform

In this document, the virtualization platform indicates the platform for integrating multiple computers with Yokogawa system products installed in the server. Hyper-V is used for the virtualization software.

In the virtualization platform, Vnet/IP functions on virtual machines are realized by using generic network card and Vnet/IP Interface Package instead of using Vnet/IP interface card. A virtual machine with this Vnet/IP communication function is referred to as a virtual Vnet/IP station.

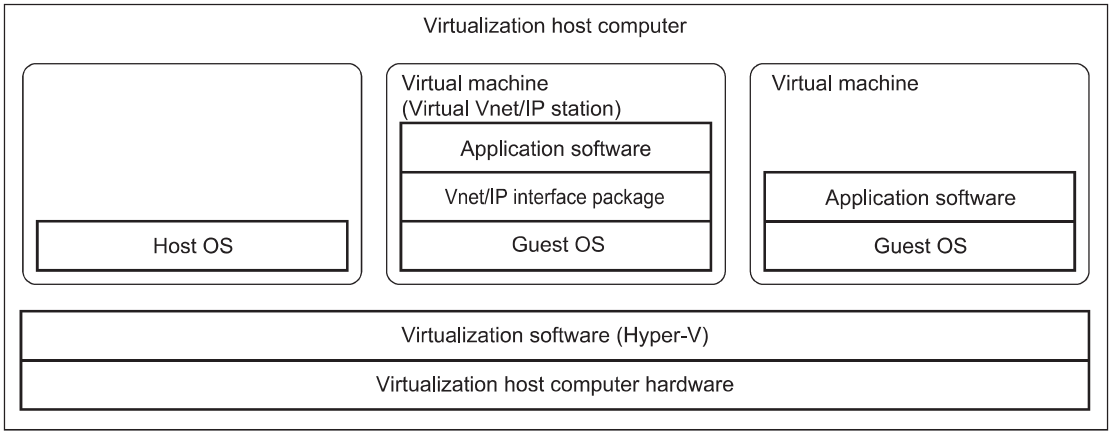


Figure A7.1-1 Hypervisor type virtualization host computer

Operation of the virtual machines on the virtualization host computer is performed on the thin client remotely connected via the network.

SEE ALSO

For more information about detailed functions of virtualization platform, refer to:

A., “Overview” in Virtualization Platform Setup (IM 30A05B20-01EN)

For more information about how to operate the virtualization host computer, refer to:

B., “Operating virtualization host computers” in Virtualization Platform Setup (IM 30A05B20-01EN)

For more information about how to set up a thin client, refer to:

C., “Setting up thin clients” in Virtualization Platform Setup (IM 30A05B20-01EN)

For more information about procedure to set up ProSafe-RS running on virtualization platform, refer to:

A2.2.2, “Setup Procedure for ProSafe-RS Running on a Virtual Machine on the Virtualization Platform” in Installation Guide (IM 32P01C50-01EN)

For more information about virtualization platform IT security setting, refer to:

1., “Overview” in Virtualization Platform Security Guide (IM 30A05B30-01EN)

For more information about IT security setting for ProSafe-RS running on virtualization platform, refer to:

1., “Overview” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

A7.2 System configuration of virtualization platform

The following figure shows an example of the system configuration of the virtualization platform.

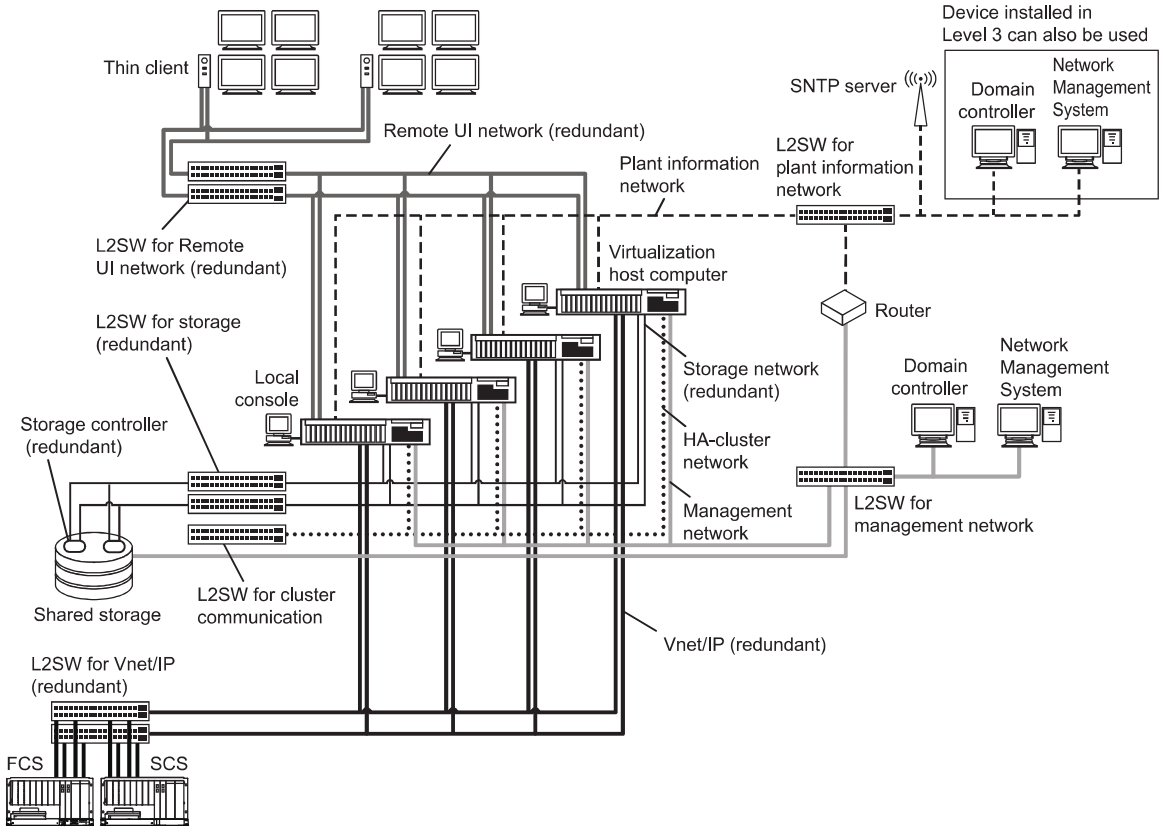


Figure A7.2-1 Example of system configuration of virtualization platform

ProSafe-RS R4.04.00 and later software can run on the virtual machines of the virtualization platform.

SEE ALSO

For more information about hardware on which the virtualization platform runs, and Yokogawa system products running on virtualization platform virtual machines, refer to:

IA system products virtualization platform (GS 30A05B10-01EN)

A7.2.1 Virtualization host computer

Virtualization host computers in the virtualization platform environment have the following structures:

- Single structure
- HA cluster structure (cluster structure with increased availability)

If HA cluster structure is used for increased virtualization server availability, live migration and failover functions can be used.

Live migration

Live migration is a feature that enables you to move active virtual machines to another virtualization host computer without stopping them. With this feature, you can apply security patches to the host OS or replace the hardware of the virtualization host computer without shutting down the virtual machines.

Disabling automatic live migration

In the virtualization platform environment, the default settings are changed to disable automatic live migration.

TIP

Automatic live migration is configured to be disabled in the following scenarios:

- When the resources of virtual machines are over committed in a virtualization host computer that constitute an HA cluster
- When the network that the virtual machines connect is specified in [Protected network] and its communication is interrupted.

However, automatic live migration may not be suppressed sometimes. For example, if you shutdown a host OS while a virtual machine is active in a virtualization host computer that forms a part of an HA cluster, live migration occurs automatically.

Failover

Failover is a function to restart the virtual machines of a virtualization host computer that stops due to an error, on another virtualization host computer in an HA cluster. This function is used to reduce the down time of a system when a virtualization host computer stops due to an error.

Restoration by restarting the virtual machine by using failover runs in the same way as [OS startup after unexpected shutdown].

Apart from the HA cluster failover that is explained in this section, there is another function called replication failover.

Failover conditions

Failover occurs in the following scenarios:

- When an active virtualization host computer stops due to an error.
- When communication is interrupted in both the management network and the HA-cluster network on an HA cluster that consists of three or more virtualization host computers.

Automatic restart of virtual machines

If the guest OS of a virtual machine with failover settings stops responding, the virtual machine restarts automatically. Unlike failover, the virtual machine restarts on the virtualization host computer that the virtual machine is originally allocated.

Restoration by restarting the virtual machine runs in the same way as [OS startup after unexpected shutdown].

Replication

Replication is prohibited for virtual machines where the Engineering Server Function, the Safety System Engineering and Maintenance Function, or iDefine is installed and virtual machines where SCS simulator runs. This is because the replica image created may have a missing or inconsistent database.

So, use the Version Control Tool to make appropriate backups during engineering, and if a storage failure occurs and the project database is corrupted, use the Version Control Tool to restore the projects.

The following table shows the applicability of replication and online backup and the enable/disable of Volume Shadow Copy Service (VSS) for packages other than the above.

Table A7.2.1-1 Applicability of replication for packages

Model	Name	Replication	Online backup	VSS	Remarks
RS4H2100	SOE Viewer Package	Applicable	Applicable	Enable: Applicable Disable: Applicable	
RS4H2200	SOE OPC Interface Package	Follow Exaopc specifications	Follow Exaopc specifications	Follow Exaopc specifications	Exaopc is internally used.
RS4H2300	Forced I/O Viewer Package	Applicable	Applicable	Enable: Applicable Disable: Applicable	

A7.2.2 Thin client

Thin client is a terminal that you use to operate the virtual machines on a virtualization host computer through remote connection. In the virtualization platform environment, Microsoft Remote Desktop Protocol is used as the connection protocol.

Number of virtual machines that you can connect simultaneously from a thin client

You can connect a thin client to multiple virtual machines simultaneously, but this consumes a lot of resources from the thin client. If too much resources are consumed, the remote connection may be disconnected. If that happens, verify the memory usage of the thin client and reduce the number of virtual machines that are simultaneously connected.

TIP

For information on how to check the thin client resource usage, contact YOKOGAWA.

Connecting a virtual machine and the USB devices of a thin client

This section describes whether you can use the USB devices that are connected to a thin client from a virtual machine.

You can use the following thin client USB devices from a virtual machine:

- Speaker
- USB storage devices

You can use these devices by configuring the corresponding settings in the virtual machine and the thin client.

A7.3 Software environment

This section describes the software environment of the components.

A7.3.1 Virtualization host computer

This section describes the software environment of the virtualization host computer.

Host OS

This section describes the software environment of the host OS.

OS

The following operating systems are supported as the host OS:

- Windows Server 2016 Datacenter Edition Desktop Experience
- Windows Server 2019 Datacenter Edition Desktop Experience
- Windows Server 2022 Datacenter Edition Desktop Experience

IT Security Tool

The IT Security Tool, which is used to configure IT security settings of the host OS, is provided in the software medium for the virtualization platform.

Virtual machine

This section describes the software environment of the virtual machine.

OS

The following operating systems are supported for virtual machines:

- Windows Server 2016 Standard Edition Desktop Experience
- Windows Server 2019 Standard Edition Desktop Experience
- Windows Server 2022 Standard Edition Desktop Experience

Available combinations of host OS and virtual machine OS

The following table shows the available host OS and virtual machine OS combinations.

Table A7.3.1-1 Available combinations of host OS and virtual machine OS

Host OS	Virtual machine OS		
	Windows Server 2016 Standard Edition	Windows Server 2019 Standard Edition	Windows Server 2022 Standard Edition
Windows Server 2016 Datacenter Edition	Yes	No	No
Windows Server 2019 Datacenter Edition	Yes	Yes	No
Windows Server 2022 Datacenter Edition	Yes	Yes	Yes

Vnet/IP interface package

In a physical environment, Vnet/IP stations use a dedicated card for Vnet/IP communication. In a virtualization platform environment, Vnet/IP stations use the Vnet/IP interface package and a general network adapter for Vnet/IP communication.

You must install the Vnet/IP interface package on a virtual machine before installing YOKOGAWA system products.

The following sections describe the important notes for Vnet/IP communication in the virtualization platform environment.

SEE ALSO For more information about notes of Vnet/IP communication in virtualization platform environment, refer to:

A7.4.1, “Precautions related to Vnet/IP communication on the virtualization platform” on page A7-13

A7.3.2 Thin client

This section describes the software environment of the thin client.

Operating system

The thin clients that are supported in the virtualization platform environment use the following operating systems:

- Windows 10 IoT Enterprise LTSC 2021
  (hereafter referred to as Windows 10 IoT)
- ThinOS 9.1

Yokogawa RDP Monitoring Software

If you use Windows 10 IoT, YOKOGAWA provides the Yokogawa RDP Monitoring Software in the software medium for virtualization platform. This software detects communication errors between virtualization host computers and thin clients.

The Yokogawa RDP Monitoring Software behaves as follows:

- It considers an interruption in communication for three seconds or more including signing out by user, as a communication error.
- It displays a user notification dialog box when an error is detected.
- It notifies users of errors in all communication channels when multiple virtual machines are connected.

IT Security Tool

The IT Security Tool, which is used to configure IT security settings in Windows 10 IoT, is provided in the software medium for the virtualization platform.

A7.3.3 License

You need a license to use the Vnet/IP interface package. After installing YOKOGAWA system products, assign the license to the virtual machine.

The virtual Vnet/IP stations without licenses are the same as the Vnet/IP stations that are not connected to the Vnet/IP network cable.

SEE ALSO For more information about required OS license for virtualization host computer and thin client, refer to:

IA system products virtualization platform (GS 30A05B10-01EN)

A7.4 Precautions on the virtualization platform

This section describes precautions on Vnet/IP communication on the virtualization platform, and precautions on setting up ProSafe-RS for virtual machines.

A7.4.1 Precautions related to Vnet/IP communication on the virtualization platform

This section describes precautions related to Vnet/IP communication on the virtualization platform

License

You need a license to use the Vnet/IP interface package. After installing YOKOGAWA system products, assign the license to the virtual machine.

The virtual Vnet/IP stations without licenses are the same as the Vnet/IP stations that are not connected to the Vnet/IP network cable.

Security

You must control the administrative privileges of the virtual Vnet/IP station to ensure the security of the Vnet/IP communication.

Functions not supported by the virtualization platform

The virtualization platform does not support the following functions:

Vnet/IP open communication

The virtualization platform uses the plant information network for open communication, and does not use Vnet/IP open communication. Attempting to install the Vnet/IP open communication driver will result in an error and installation will fail.

CI Server integration

The virtualization platform does not support CI Server integration. Also, wide area communication and narrow band communication supported by CI Server integration cannot be used.

Precision of time synchronization

The relative time synchronization precision between virtual Vnet/IP station and other stations are as follows:

- ±50 ms within the domain
- ±75 ms among domains

This precision does not apply to the relative time synchronization between stations other than virtual Vnet/IP stations, and remains the same as earlier.

Limitations related to IP address and network connectivity

The following limitations related to IP address and network connection applies to virtual Vnet/IP stations:

- Do not configure IP addresses 192.168.0.0 to 192.168.255.255 for virtual network adapters that are not used for Vnet/IP communication on the virtual machines.
- The virtual network adapters other than the Vnet/IP virtual network adapter cannot connect to the network in the range from 192.168.0.0 to 192.168.255.255 either directly or through network switches and routers.

L2SW segments within the Vnet/IP domain

The range that is connected to only an L2SW without devices such as layer 3 switches (hereinafter, referred to as L3SW) or V net routers is called the Vnet/IP domain. In the virtualization platform environment, the range connected by including this virtual L2SW is called the Vnet/IP domain.

In a virtualization platform environment, you can install up to seven L2SW segments within the Vnet/IP domain. This does not include virtual L2SW.

Notes when connecting SNTP server to the Vnet/IP network

When you connect the SNTP server to a Vnet/IP network on which virtual Vnet/IP stations are connected, and try to synchronize the network time with the absolute time, adopt any of the following network configurations:

- If a domain with one or more virtual Vnet/IP stations that are installed with Vnet/IP firmware is available, you must connect the SNTP server to that domain.
- If you cannot connect the SNTP server to a domain that satisfies the conditions mentioned earlier, or if the domain to which the Vnet/IP station belongs does not have stations installed with Vnet/IP firmware, configure the network by satisfying all the following conditions:
  - Install the SNTP server in a place where all the Vnet/IP stations that belong to a time group can communicate.
  - In this time group, include a minimum of one station that is installed with Vnet/IP firmware.
  - Specify the IP address of the SNTP server in the time group settings in the properties of the domain that has stations installed with Vnet/IP firmware.

TIP

The following stations are installed with Vnet/IP firmware:

- Stations installed with Vnet/IP interface card
- FCS that can connect to Vnet/IP
- SCS
- Vnet router
- Wide area communication router

A7.4.2 Precautions on using ProSafe-RS on a virtual machine

This section describes precautions on using ProSafe-RS on a virtual machine.

Resources required for a virtual machine

The following table shows an estimation of resources that are required for ProSafe-RS system to run in a virtual machine.

If you install multiple functions on a virtual machine, you must compare resources required for respective functions and assign the maximum value of them to the virtual machine. Ensure to total the required available space for the hard disk space.

If CENTUM VP software is also installed on the same virtual machine, the virtual machine must also meet the requirements for CENTUM VP software.

Table A7.4.2-1 Estimation of resources required for a virtual machine

Function and package	Type of setup	Number of CPU cores	Memory size (GB)	Hard disk space (GB) (*1)	Disk access speed (MB/s)
Engineering Server Function (*2)	Recommended setting	4	8	80	48
Safety System Engineering and Maintenance Function (iDefine not installed in the same virtual machine)	Recommended setting	4	8	80	48
Safety System Engineering and Maintenance Function (iDefine installed in the same virtual machine)	Recommended setting	4	12	80	48
SOE Viewer Package / SOE OPC Interface Package / Forced I/O Viewer Package (*3) (*4)	Recommended setting	2	4	80	16
SCS Simulator	Recommended setting (8 simulators)	3	5	-	16
	Small-scale setting (4 simulators)	2	5	-	16
License Management	Recommended setting	2	4	80	32
	Small-scale setting	1	2	40	8
File Server	Recommended setting	2	4	80	48
iDefine for ProSafe-RS (*5)	Recommended setting	4	8	80	32

*1: If the operation history database of Access Control and Operation History Management Package is placed on the virtual machine, at least 60 GB of additional disk space is required.
*2: Only the license of this package can be distributed alone to a virtual machine and run it as an AD Server.
*3: When installing these packages on the same virtual machine where the Engineering Server Function or the Safety System Engineering and Maintenance Function is installed, observe their operating environment requirements.
*4: The time taken for distribution performed with the Forced I/O Viewer Setup Tool of the Forcing I/O Viewer Package can be improved by increasing the disk access to 32MB/sec.
*5: When installing iDefine for ProSafe-RS in the same virtual machine as the Safety System Engineering and Maintenance Function, refer to the estimation for “Safety System Engineering and Maintenance Function (iDefine installed in the same virtual machine).”

TIP

For resources required when using Standard Whitelisting Software for Endpoint Security on virtual machines, contact YOKOGAWA.

Precautions for running live migration

You must stop SENG programs before you run live migration. If you run live migration while SENG programs are running, problems may occur for example creation of master database fails after online maintenance. To avoid such problems, you must handle a live migration as a maintenance task and prepare a plan to execute it.

Precautions after execution of failover

The virtual machine startup due to failover runs as “OS startup after unexpected shutdown”. After failover runs, perform the following tasks.

Use Project Comparing Tool or Database Validity Check Tool to check the status of database after failover runs. If necessary, roll back SCS project by using the database repair function of Database Validity Check Tool or Version Control Tool and reflect the changes that are made before failover runs to restore the project or the database.

Precautions when connecting remote desktop

Remote desktop connection is required between the virtual machines and the thin clients when using ProSafe-RS on the virtualization platform.

Precautions when connecting the remote desktop on the virtualization platform are as follows:

- Install the remote desktop session host role service on the virtual machines.
- Set the number of remote desktop connection sessions that can be connected to one virtual machine at the same time to 1.
- Disable the limit on the number of connected sessions for each user.
- It is recommended to limit the number of thin clients and users who can remotely connect to virtual machines to the minimum necessary.
- The ProSafe-RS and CENTUM VP remote operation monitoring servers cannot both be installed on the same virtual machine.

IMPORTANT

After setting up the remote desktop connection, follow these steps to apply the registry file:

1. Sign in to the virtual machine as an administrative user.
2. Mount the ProSafe-RS software medium.
3. In Explorer, navigate to the following folder in the ProSafe-RS software medium.
   `<Drive of ProSafe-RS medium>:\ProSafe-RS\RemoteDesktopService`
4. Double-click `Reg_FS_OFF.reg` in the folder.
5. Restart the virtual machine.

SEE ALSO For more information about how to set the number of sessions that can be connected simultaneously on remote desktop, refer to:

B1.6, “Changing session settings in remote connection” in Virtualization Platform Setup (IM 30A05B20-01EN)

For more information about how to grant permission for remote connection with thin clients and how to register users, refer to:

B1.4, “Configuring system products after installing” in Virtualization Platform Setup (IM 30A05B20-01EN)

For more information about setting to limit the number of thin clients and users that can be remotely connected to the minimum, refer to:

B2.5.6, “Limiting connections to virtual machines” in Virtualization Platform Setup (IM 30A05B20-01EN)

Precautions when using shared storage

If the path for shared storage is switched while SCS Test Function Window is being started, the start of SCS Test Function Window may fail.

If the start of SCS Test Function Window failed, restart it.

Precautions when using iDefine in the virtualization platform environment

Dongle Gateway, which is a Windows service, is required to use iDefine in the virtualization platform environment. The license for iDefine is authenticated via Dongle Gateway.

SEE ALSO For more information about Dongle Gateway specifications, refer to:

Dongle Gateway Installation and User Guide (PR03076-MAN-983_01)

Installing Dongle Gateway and inserting a USB dongle

Install Dongle Gateway on thin clients where IT security settings are applied, physical SENGs, or virtual machines with SENG software installed.

Insert a USB dongle into computers where Dongle Gateway is installed. If you install Dongle Gateway on a virtualized SENG, insert a USB dongle in the USB device server and have it recognized via the network.

With one USB dongle, you can use iDefine for the number of licenses granted to the dongle.

The following table shows the combinations of computers that can install Dongle Gateway and where to insert the USB dongle.

Table A7.4.2-2 Computers on which Dongle Gateway can be installed and where to insert the USB dongle

Computers on which Dongle Gateway can be installed	Where to insert the USB dongle	Remarks
Thin client	Thin client	Windows version
Physical SENG	Physical SENG	-
Virtualized SENG	USB Device Server (*1)	-

*1: Please contact YOKOGAWA for recommended products for USB Device Server.

SEE ALSO For more information about Dongle Gateway IT security setting, refer to:

"■ The users for using iDefine in a virtualization environment" in 2.2.3, "User/Group Management" in ProSafe-RS Security Guide (IM 32P01C70-01EN)

For more information about how to install Dongle Gateway, refer to:

Dongle Gateway Installation and User Guide (PR03076-MAN-983_01)

License authentication

To use iDefine in a virtualization platform environment, authenticate the license via Dongle Gateway.

IMPORTANT

- If the iDefine for the number of Dongle Gateway licenses granted to the USB dongle is already connected to the Dongle Gateway at the same time, trying to connect another iDefine will cause license authentication to fail.
- If communications between iDefine and Dongle Gateway are disconnected, such as if there is a communication error or if the USB dongle is pulled out, update of the license information will fail and the iDefine license will be invalidated. If communication between iDefine and Dongle Gateway is restored within 5 minutes and license information can be acquired, the iDefine license is re-activated and iDefine can be used. If the license information cannot be acquired, Dongle Gateway releases the license and becomes available from other iDefine.

SEE ALSO For more information about how to authenticate iDefine license via Dongle Gateway, refer to:

Dongle Gateway Installation and User Guide (PR03076-MAN-983_01)

Transfer of data files

The method to transfer files, such as the safety I/O list and data files to be exchanged with iDefine, to and from the guest OS of virtual machines differs from the method used for physical computers.

SEE ALSO For more information about how to extract and capture data files, refer to:

B2.8, "Copying files" in Virtualization Platform Setup (IM 30A05B20-01EN)

B. ProSafe-RS security

ProSafe-RS has the following security functions to prevent access to the system by unauthorized users and devices, and unintended changes caused by operation mistakes made by users.

- Security for the project database
  You can configure the SENG function so that the user is required to enter a password when changing the project data with SCS Manager. (Recommended)
- Security for access to SCS
  You can limit access to SCS from the outside based on the SCS security level. The user is required to enter a password when changing the SCS security level. (Mandatory)
- Security for the SCS Maintenance Support Tool
  On SENG, you can limit writing to SCS with the SCS Maintenance Support Tool by setting a password. (Recommended)
- Access control and operation history management
  Access control and operation history management can be performed on projects that are saved in the AD Server. You can also use the Access control and operation history management package.
- Countermeasures against threats to IT security
  ProSafe-RS security threats include attacks via the network, direct attacks by executing actions on an SENG, and analysis of important data carried out by stealing an SENG. The security features are designed to take measures against these types of security breaches.

This section provides an overview of the ProSafe-RS security function, and the main procedures for setting passwords and implementing security relating to unauthorized access and protection against unintended operations.

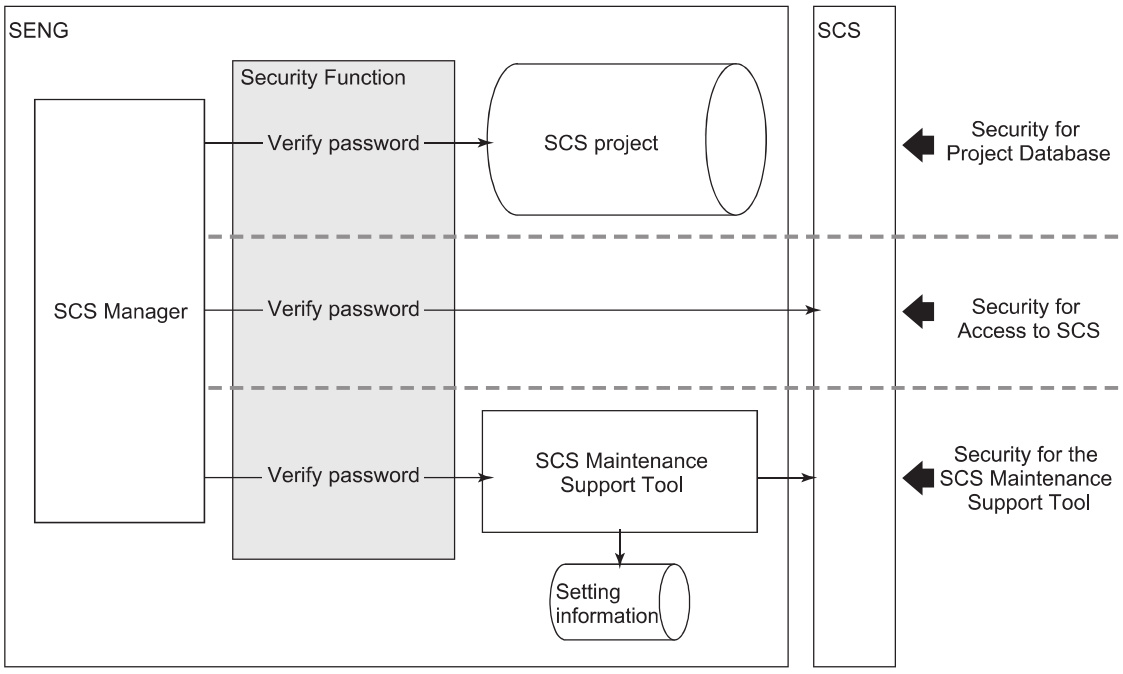


Figure B-1 Password-based security functions

B1. Overview of ProSafe-RS security

The figure below illustrates the security management of SCS and SENG in ProSafe-RS.

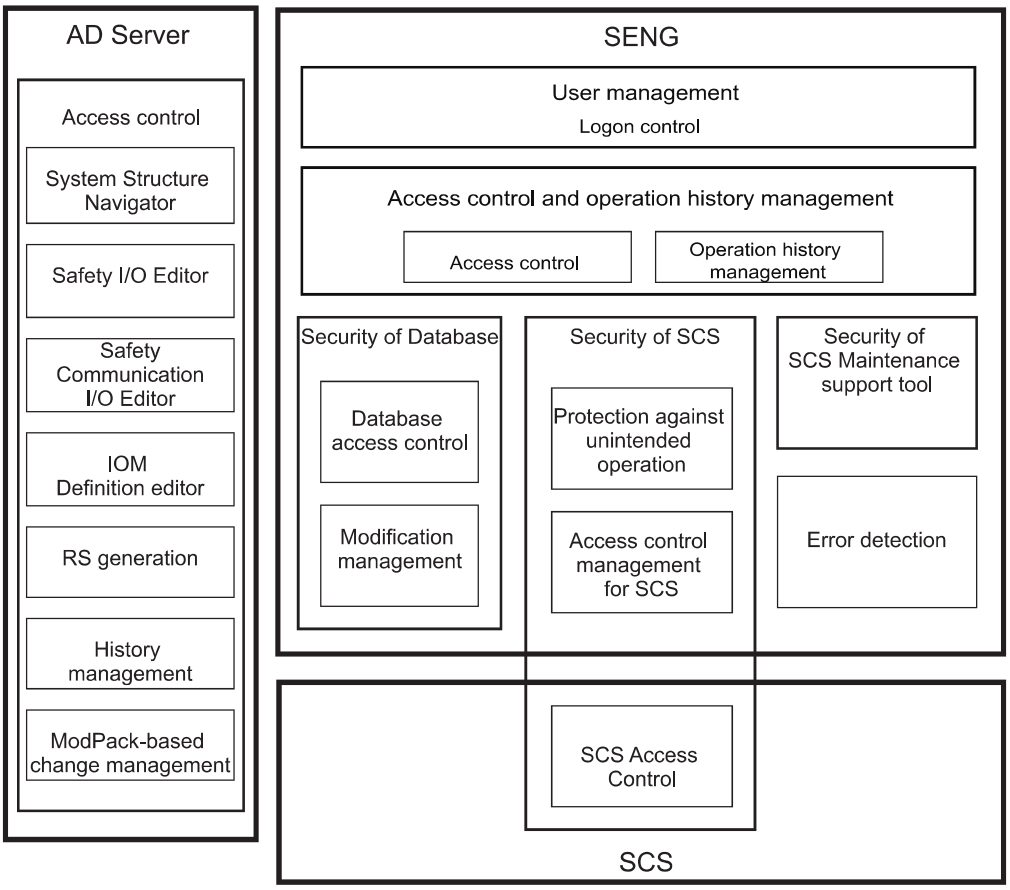


Figure B1-1 Overview of security management

IT security

This section describes the requirements for IT security.

For SENG, Windows OS is used as a platform. Therefore, it is necessary to prevent, detect, and recover from computer viruses and attacks from the external through the network. For example, there are countermeasure such as network access control using firewall and system backup.

In the CENTUM Integration Structure, it is necessary to consider comprehensive IT security including ProSafe-RS system and CENTUM system.

You can harden the security of the PC designated as a SENG terminal to enhance the ProSafe-RS IT security (PC hardening). This section describes the details regarding PC hardening and the setting guidelines.

TIP

When integrating ProSafe-RS with CENTUM VP, configure the security settings during installation of ProSafe-RS and installation of CENTUM VP, respectively.

When integrating ProSafe-RS with CS 3000, select Legacy model in IT security tool.

Configure the IT security of the computer that has iDefine installed by referring to iDefine Security Manual (PR03076-MAN-981_01).

If your security model is a legacy model, anyone will be able to start iDefine Test Manager.

If your security model is a standard or strengthened model, any user that belongs to the PSF_ENGINEER or PSF_ENGINEER_LCL group will be able to start iDefine Test Manager.

An example of registering a user to the user account

IT security enhancement for a PC can protect the ProSafe-RS system from the illegal access by any user other than the user of ProSafe-RS user groups. For protecting the ProSafe-RS system from the accidental mistaken accesses by the users of ProSafe-RS groups, the ProSafe-RS Security features should be used. By combining IT security enhancement for a PC and ProSafe-RS Security, you can fortify security of ProSafe-RS.

The typical examples of registering a ProSafe-RS user to the user groups are shown as follows:

(A) ProSafe-RS Engineer (Integrated with CENTUM VP)

ProSafe-RS Engineer user should be assigned to both PSF_ENGINEER group of ProSafe-RS and CTM_ENGINEER group of CENTUM VP.

(B) ProSafe-RS Engineer (Not Integrated with CENTUM VP)

ProSafe-RS Engineer user should be assigned only to the PSF_ENGINEER group.

(C) Maintenance and service persons

The user who requires the role for upgrading SENG software to newer versions, maintaining or changing the hardware components such as I/O modules should be assigned only to the PSF_MAINTENANCE group.

(D) Network and System Administrator (User who is responsible for network maintenance)

This user is considered as the administrative user of Windows environment in SENG. This user needs to be assigned only to the PSF_MAINTENANCE group.

(E) User account for emergency attention (For domain or parallel management in standard model)

When ProSafe-RS system is running in an Windows domain environment, if the domain controller encounters an abnormality, no one can logon to the SENG with the domain account. You need to prepare the user accounts who are assigned to the PSF_MAINTENANCE_LCL group for an emergency attention. If the domain controller encounters an abnormality, user can logon to the SENG with this user account, then maintain and operate ProSafe-RS.

Though the users in the above groups are all granted with the Write permission to all the Project folders, in the cases of (C) and (D), the Write permission is not required. An engineer should define a password by using the security feature of the project database and keep the password as secret to the users whom you do not grant the Write permission so as to protect the project database. Moreover, ProSafe-RS provides security features for accessing the SCS and for Maintenance Support Tool. These security features can be utilized in accordance with the role of the users so as to protect the database and SCS from the accidental operation mistakes.

SEE ALSO For more information about user groups of ProSafe-RS, refer to:

2.2, “User/Group Management” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

For more information about user groups of CENTUM VP, refer to:

CENTUM VP Installation (IM 33J01C10-01EN)

Database security management

The database has the following security functions.

Access control of the SCS project database

It is possible to set a password for the database used in an SCS project; so that only users who know the password are allowed to make changes to the database. It is also possible to set whether or not to allow users who do not know the password to refer to the database.

Security for AD projects

The following security functions are available for AD projects:

- Management of users who are permitted to access AD projects
- Access control of AD project data

Modification management

This function manages the changes made to SCS projects. It has the following functions:

- Backup
  SCS projects are registered and managed in AD Server.
- Version management
  This function manages the history of changes made to SCS projects.
- Master database management
  SENG always maintains the backup SCS project that keeps the same SCS database with the one running on the SCS.
- Saving modification files
  When you use the Access Control and Operation History Management Package, the changes made to the project database downloaded to the SCS are saved.

Security management of SCS

The SCS has the following security functions.

SEE ALSO For more information about details on the security of SCS, refer to:

B3., “Security of SCS” on page B3-1

Prevention of SCS operation mistakes made by users

When a user attempts to perform the following operations on the SCS, the user is prompted to confirm the execution of the operation in order to prevent operational mistakes.

- Offline download
- Online change download
- Master database offline download
- IOM download

- I/O lock
- SCS security level change

Access control to SCS

- Access control based on the security level
  Access from outside to SCS is controlled by SCS security levels. Password must be set for changing the SCS security levels (to Level 1 or Level 0). The SCS security level can only be operated using the SCS security level operation function, by users who know the password.
- Access control for each user
  When the Access Control and Operation History Management Package is applied, you can control operations on SCS for each user.

Security management of SCS Maintenance Support Tool

In SCS Maintenance Support Tool, write access to SCS is controlled by setting a password. If the Access Control and Operation History Management Package is used, operations of the SCS Maintenance Support Tool can be controlled for each user.

SCS Status Overview window, Diagnostic Information window, Setup Tool

The SCS Status Overview window, Diagnostic Information window and Setup Tool are protected by passwords. Each of these functions is launched as read-only unless the correct password is specified.

In the case of the SCS Status Overview window, the password is checked when calling this window from SCS Manager. The Diagnostic Information window and Setup Tool inherit the password of the SCS Status Overview window when they are launched.

When the Access Control and Operation History Management Package is applied, enter the name and password of the engineer.

Message Cache Tool

Message Cache Tool is protected by a password. It is launched as read-only unless the correct password is specified.

SOE Viewer

No password is set up for SOE Viewer because no writing operations to an SCS are performed on SOE Viewer.

Forced I/O Viewer and Forced I/O Viewer Setup Tool

Forced I/O Viewer and Forced I/O Viewer Setup Tool do not perform password authentication at startup.

Access control of AD server

You can control access to individual files and functions of an AD project for each user. You can also set access rights to the files and folders in AD Server according to the role of the user.

System Structure Navigator

You can set the rights to register, unregister, back up, and restore RS projects, edit RS project comments, and delete SCS.

- **Safety I/O Editor**

  You can set the rights to create and delete safety I/O lists and assign safety I/O.

- **Safety Communication I/O Editor**

  You can set the rights to create and delete safety communication I/O lists and assign safety communication I/O.

- **IOM Definition Editor**

  You can set the rights to create and delete nodes and I/O modules.

- **RS generation**

  You can set the rights to run RS generation.

- **History management**

  You can set the rights to set and delete labels.

- **ModPack change management**

  You can set the rights to perform operations for each ModPack operation category.

B2. Security for project database

This section describes security for project databases.

Setting a password for project databases

You can assign a password to a database to prevent unauthorized users from making changes to the database in SCS projects. Users without entering the password can be given permission for read only operation.

Passwords can be specified for the following.

- For each SCS Project
- For each POU

The reading and writing right for the whole project and the access right for each POU can be controlled using the security function of the SCS project and the security function of each POU.

Set a different password for each SCS Project.

If higher level of security is required, set a password for each important POUs.

You need to set different passwords for each SCS project. These passwords should be different from the one for the SCS security level.

Database files in RS projects should not be changed from tools other than the ProSafe-RS software.

Setting a password for the SCS project

It is possible to set a password for the SCS project so that only authorized users can make changes to the SCS project.

The following settings can be made.

- Password for the SCS Project
  If you set a password for the SCS project, users are asked to enter the password when they open the SCS project.
- Accessing without a password
  If you do not know the password, the SCS project can be opened in read-only mode without entering the password after checking [Read Only].

  In this status, the users are not allowed to edit the application logic or generate databases.

  Operations on the SCS, such as using the forcing function and downloading data, are possible in the read-only status.

TIP

Security for operations on SCSs and security for SCS project databases are not related.

The security against operations on SCSs is changed using the SCS security level operation function. By changing the SCS security level, using the forcing function and downloading data can be allowed.

How to set passwords

1. Select [Project Properties] from the [File] menu of SCS Manager;
   The following dialog box appears.

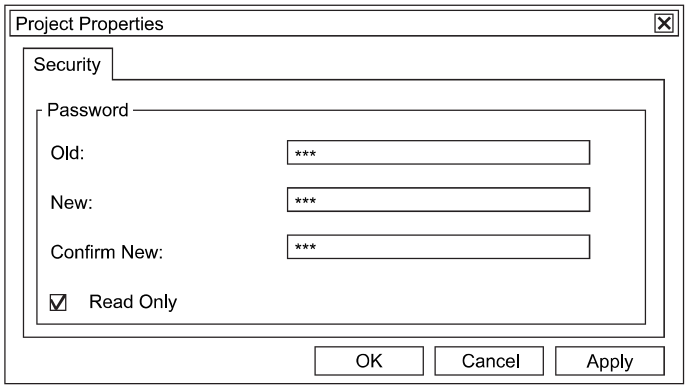


Figure B2-1 Project Properties dialog box

2. Enter the current password in the [Old:] field.
3. Enter a new password in the [New:] field, and once again in the [Confirm New:] field. The password consists of up to eight case-sensitive, alphanumeric characters.
4. If you want to access the project but do not know the password, check [Read Only] option.
5. Click the [OK] button.

Setting password for each POU

It is possible to set a password for each POU so that only the authorized users can reference and change important POUs.

When users attempt to edit a POU for which a password is set, they are required to enter the password. If you do not know the password, you are not allowed to reference or print the POU.

Even when a project is opened in read-only mode, the POU is readable after entering the password of the POU.

How to set passwords

1. Select a POU for which you want to set a password.
2. Select [Properties] from the menu displayed by clicking the right mouse button. The following dialog box appears.

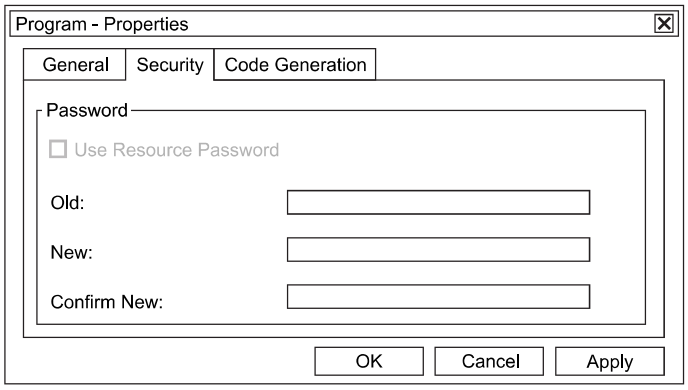


Figure B2-2 Dialog box for setting a password for a POU

3. Enter the current password in the [Old:] field.
4. Enter a new password in the [New:] field, and once again in the [Confirm New:] field. The password consists of up to eight case-sensitive, alphanumeric characters.

5. Click the [OK] button.

B3. Security of SCS

SCS security levels provide adequate security through specifying the passwords. Passwords for different security levels can be set for each SCS.

- Setting and changing passwords
- Changing SCS security levels

Note that it is necessary to return the SCS security level to Level 2 before closing an SCS project.

This section describes how to set passwords for changing SCS security levels and how to change the levels.

IMPORTANT

No password has been set after executing offline download and master database offline download. Make sure to set passwords again.

TIP

The access to SCS is controlled by SCS itself according to its security level. Operations on the SENG is not be prohibited according to the SCS security level, however.

SEE ALSO

For more information about security level of SCS, refer to:

A3.2.2, “Security level of SCS” on page A3-15

How to set and change passwords

The password that is used to change the SCS security level is stored within the SCS. This password can be set or changed from the Set SCS Security Level dialog box.

IMPORTANT

No password has been set after executing offline download and master database offline download. Make sure to set a password at this stage.

1. Select [Maintenance] from the [Tools] menu of SCS Manager.
   The Maintenance Launcher menu appears.
2. Select [Set SCS Security Level] from the Maintenance Launcher menu.
   The Set SCS Security Level dialog box appears.

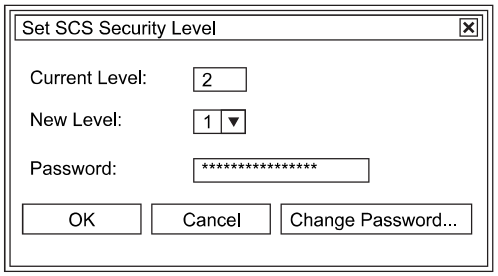


Figure B3-1 Set SCS Security Level dialog box

3. Click the [Change Password] button.

The Change SCS Security Level Password dialog box appears.

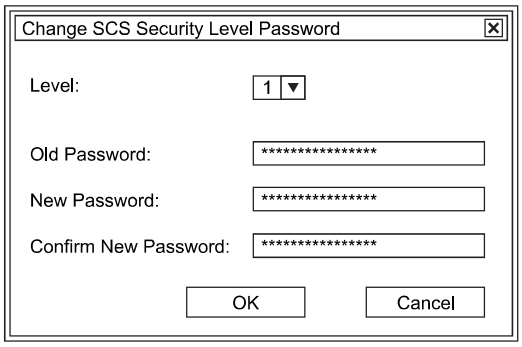


Figure B3-2 Change SCS Security Level Password dialog box

4. Select the security level for which you set a password in [Level:].
   It is necessary to set one password for changing to Level 1 and one for Level 0, respectively.
5. Enter the current password in the [Old Password:] field.
6. Enter a new password in the [New Password:] field, and once again in the [Confirm New Password:] field.
   The passwords you have entered appear as a series of asterisks (*).

   A password is a maximum 16 of single-byte alphanumeric characters and following symbols including a space character. The password is case-sensitive.

   ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~

   You do not need to enter [Old Password:] if you have not set any password before, or if you have just executed an offline download or a master database offline download.
7. Click the [OK] button.
   The confirmation dialog box appears.

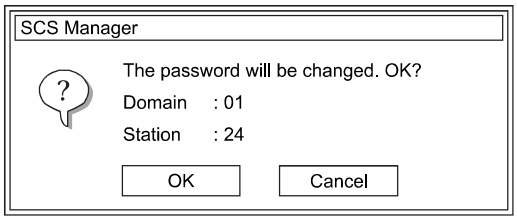


Figure B3-3 Confirmation dialog box

8. Click the [OK] button.
   Both new and old passwords will be sent to SCS. If the password is successfully changed, the dialog box notifying the success appears. The new password becomes valid. If the password change fails, a dialog box will be displayed to notify the failure.

How to change SCS security levels

The SCS security level can be changed in the Set SCS Security Level dialog box of SCS Manager.
The table below shows the combinations of levels for which security level changes are allowed via operations on the Set SCS Security Level dialog box.

Table B3-1 Security levels that can be changed through operations in the Set SCS Security Level dialog box

Current SCS security level	New SCS security level (*1)		
	Level 2	Level 1	Level 0
Level 2	-	Yes (*2)	Yes (*2)
Level 1	Yes (*2)	-	Yes (*2)
Level 0	Yes(*3)	No	-

*1: Yes: The security level can be changed.
No: The security level cannot be changed.
*2: The security level can be changed to the target SCS security level.
*3: Security level changes can be made only in SCS simulator.

To change the security level, you need to enter the password. However, you don't need to enter a password when changing the security level from Level 1 to Level 2.

You cannot raise the security level from Level 0 to Level 2 from the Set SCS Security Level dialog box. In SCS Simulator of SCS Test Functions, however, you can raise from Level 0 to Level 2 on the Set SCS Security Level dialog box. This operation does not require a password.

CAUTION

To set the SCS security level back to Level 2 after changing to Level 0, you must restart the SCS, execute offline download, or execute master database offline download. In particular, be sure to execute offline download if you used break points in debugging of the application logic.

These operations require stopping of the system. When you change the security level to Level 0, do so very carefully considering the consequences of the system stop.

The SCS security level can be changed in the following procedure.

1. In SCS Manager, open an SCS project whose security level you want to change.
2. Select [Maintenance] from the [Tools] menu of SCS Manager.
   The Maintenance Launcher menu appears.
3. Select [Set SCS Security Level] from the Maintenance Launcher menu.
   The Set SCS Security Level dialog box appears. The current security level is displayed in [Current Level:]; this item is display only and cannot be changed.

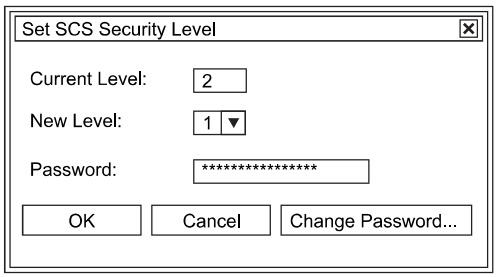


Figure B3-4 Set SCS Security Level dialog box

4. Select the security level you want in [New Level:] and enter the password for the level you want in [Password:] text box.
   All characters you enter are displayed as asterisks (*).
5. Click the [OK] button.
   The confirmation dialog box appears.

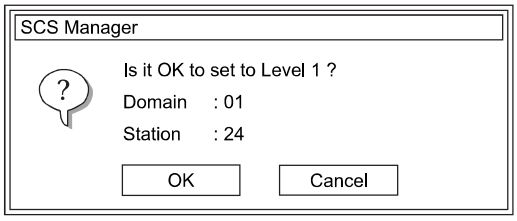


Figure B3-5 Confirmation dialog box (when changing to Level 1 or Level 2)

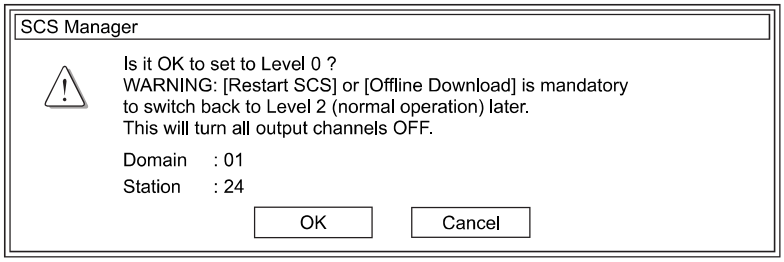


Figure B3-6 Confirmation dialog box (when changing to Level 0)

6. Click the [OK] button.
   When changing the security level to Level 0, the following dialog box appears to confirm the change again. When you set the level back to Level 2 from Level 0, the system stops. Confirm that this does not cause any problems. To proceed with the change, click [OK].

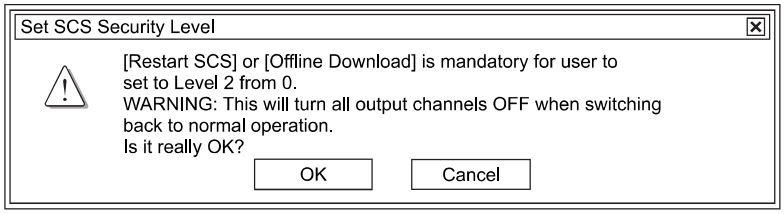


Figure B3-7 Dialog box confirming change to Level 0

If the security level of SCS is changed, the message showing the result of change is displayed.

The error message is displayed if the security level could not be changed.

Confirming the SCS security level reset by SCS Manager

If the security level of SCS project currently opened in SCS Manager is not Level 2, the confirmation dialog box prompting to reset the security level to Level 2 appears when closing it.

IMPORTANT

This dialog box is for confirmation only. Open the corresponding SCS project again and change the security level using the Set SCS Security Level dialog box.

The confirmation dialog box appears in the following timings.

- When closing an SCS project by exiting SCS Manager

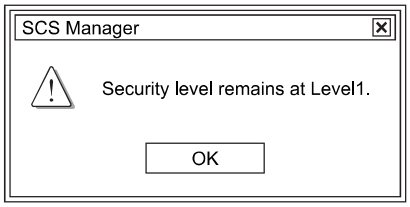


Figure B3-8 Example of Confirmation dialog box (when closing by exiting SCS Manager)

Clicking the [OK] button to exit SCS Manager leaves the security level unchanged.

- When closing an SCS project by opening another SCS project

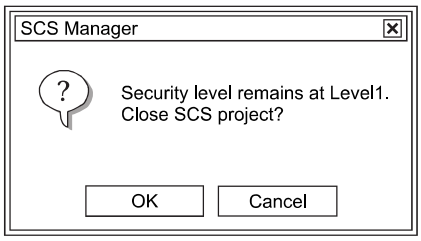


Figure B3-9 Example of Confirmation dialog box (when closing by opening another SCS project)

Click the [OK] button to close the currently opened SCS project without changing its security level, and then open another SCS project.

Click the [Cancel] button to keep the currently opened SCS project opened, and another SCS project will not open.

B4. NIU status and security

The N-ESB bus module (S2EN501) that is installed in the node interface unit (NIU) is equipped with a maintenance port.

For the security reason, you should disable the maintenance port when operating the system.

The status of the NIU is determined by the status of the NIU maintenance port and operating mode of the NIU. This section describes the status of the NIU maintenance port, NIU operating mode, and shifting of the NIU status.

Overview of the NIU status and tools

The status of the NIU is determined by the status of the NIU maintenance port and operating mode.

- Status of the NIU Maintenance Port
  The status of the NIU maintenance port can be either enabled or disabled. The status of the maintenance port can be switched between enabled and disabled by using the NIU maintenance port settings tool that is called from the SCS State Management window in the SCS Maintenance Support Tool.
- Operation mode of the NIU
  The NIU operation mode can be either online mode or maintenance mode. The operation mode can be switched between online mode and maintenance mode by using the N-IO maintenance tool in the computer that is connected to the maintenance port.

  The N-IO maintenance tool can be used if the NIU maintenance port is enabled.

IMPORTANT

The Node number setting tool and FieldMate Validator are included in the N-IO maintenance tool.

B4.1 Status of the NIU maintenance port

You can run the NIU maintenance port settings tool and enable or disable access from an external device such as a computer connected to the maintenance port of the N-ESB bus module.

Disabled status

The disabled status of the maintenance port prohibits access from the maintenance port.

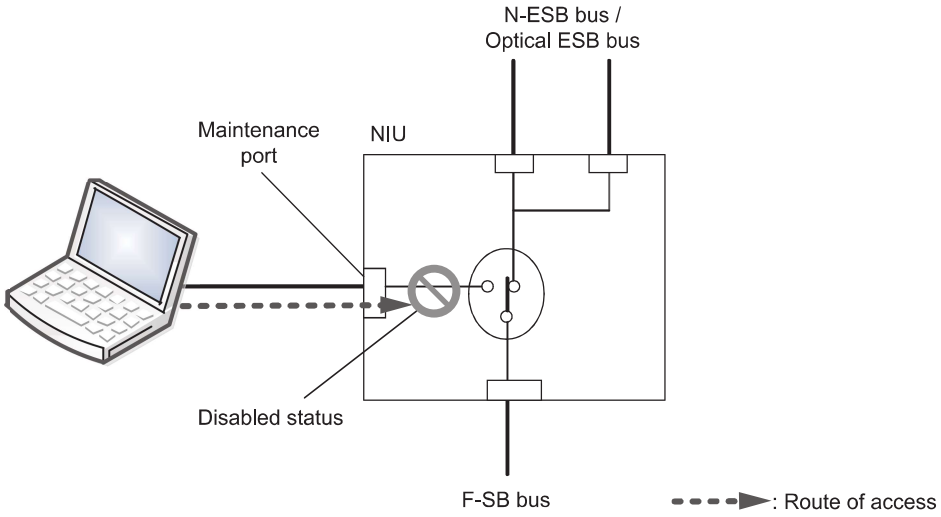


Figure B4.1-1 Disabled status of the maintenance port

Enabled status

The enabled status of the maintenance port allows access from the maintenance port.

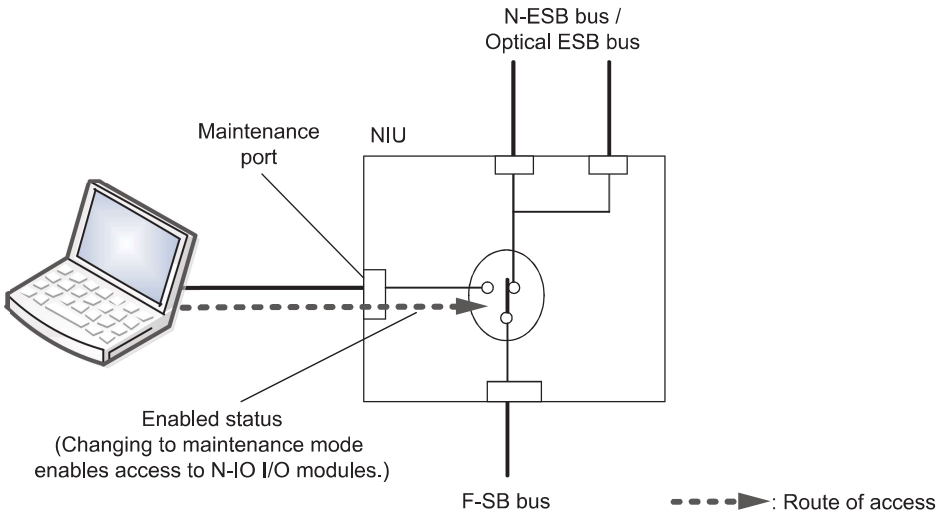


Figure B4.1-2 Enabled status of the maintenance port

SEE ALSO For more information about how to enable/disable the maintenance port, refer to:

I4.5, “NIU maintenance port setting tool” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

B4.2 Operation mode of the NIU

The NIU operation mode can be either online mode or maintenance mode.

Online mode

In online mode, you can access the N-IO I/O modules from the N-ESB bus or the optical ESB bus.

You cannot access the N-IO I/O modules from the maintenance port.

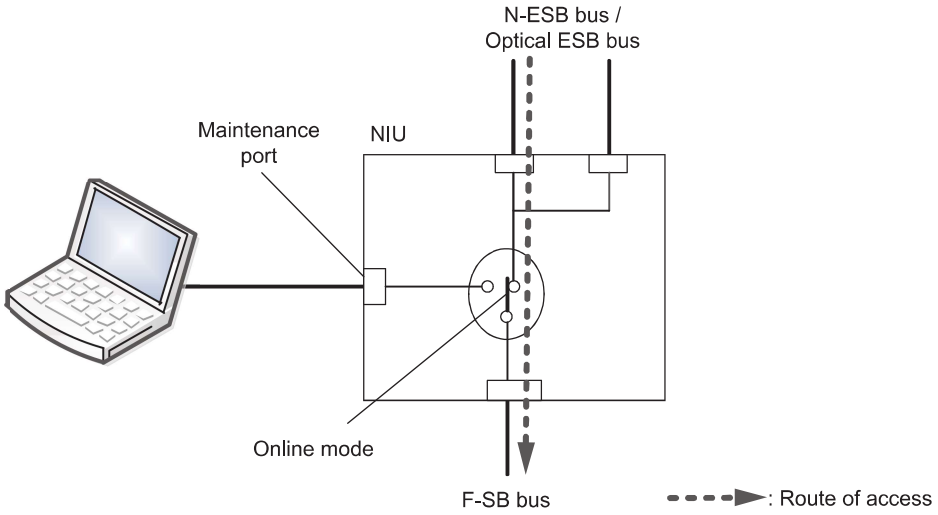


Figure B4.2-1 Online mode

Maintenance mode

In maintenance mode, you can access the N-IO I/O modules from the maintenance port.

You cannot access the N-IO I/O modules from the N-ESB bus or the optical ESB bus.

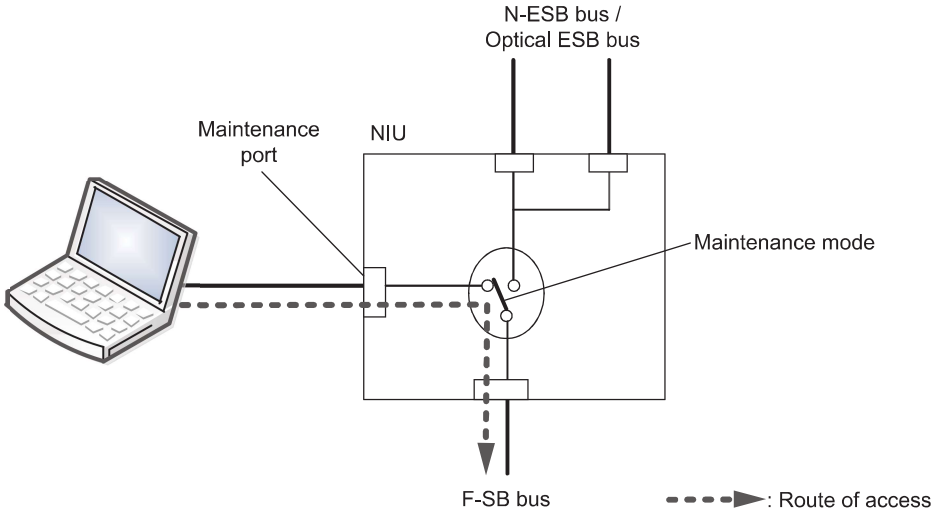


Figure B4.2-2 Maintenance mode

Switching between operation modes

This section describes how to switch between the NIU operation modes.

- Switching from the online mode to the maintenance mode

When the maintenance port is enabled, perform the "maintenance instructions" operation from the N-IO maintenance tool connected to the maintenance port to switch from the online mode to the maintenance mode.

- Switching from the maintenance mode to the online mode.
  Perform on of the following to switching from the maintenance mode to the online mode.
  - Perform the "release maintenance instructions" operation from the N-IO maintenance tool connected to the maintenance port.
  - Disconnect the USB cable that is connected to the maintenance port
  - Turn off the power of the NIU, then turn it on

IMPORTANT

When the node number setting tool is used as a N-IO maintenance tool, the unit will switch to the maintenance mode when a node address is configured. After the node address is configured, the unit will switch to the online mode.

TIP

- Switching the maintenance mode of the dual-redundant N-ESB bus modules
  Because the N-ESB bus modules are dual-redundant, when you change the operation mode on one side, the operation mode of the other side will switch accordingly.

SEE ALSO

For more information about Node number Setting tool, refer to:

F2.1.1, “Using the Node Number Setting Tool” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about FieldMate Validator, refer to:

manual of FieldMate Validator

B4.3 Shifting the Status of the NIU

The following figure shows the status and the operation mode of the NIU maintenance port, and the status shift with regards to external access.

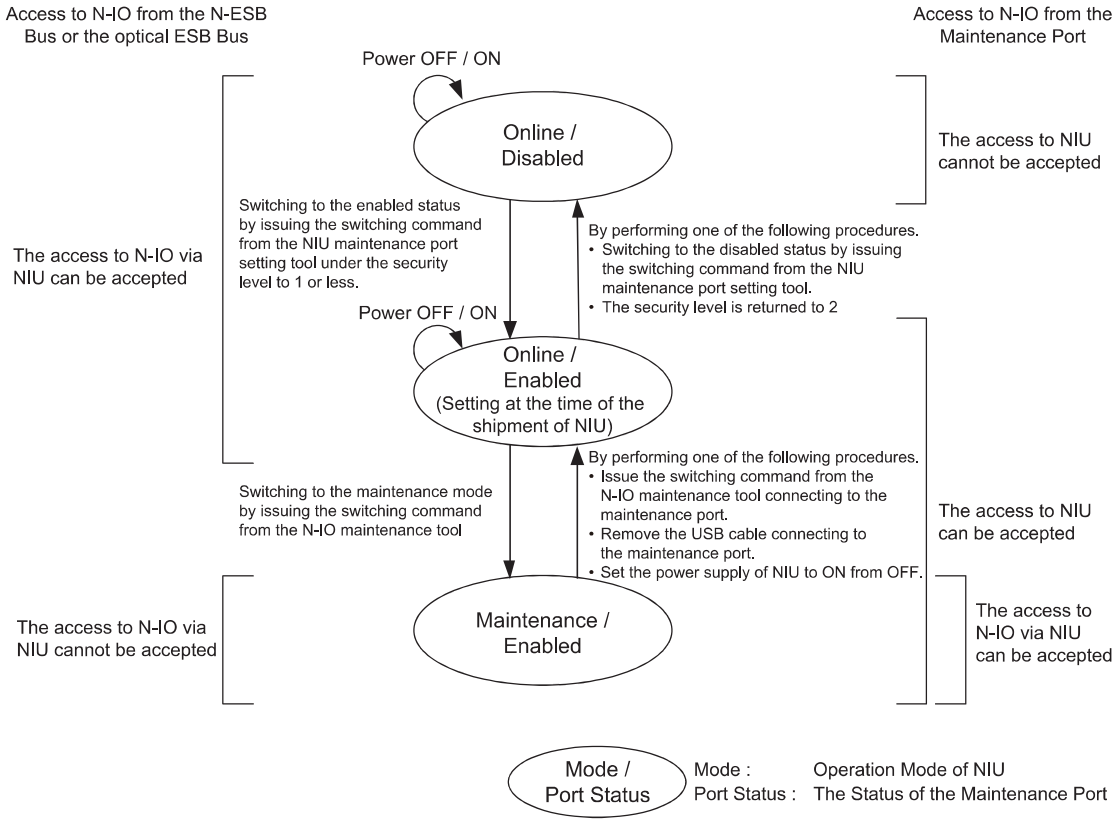


Figure B4.3-1 NIU status shift

The following table shows the factory settings of the N-ESB bus modules (S2EN501) that are installed in the NIU.

Table B4.3-1 NIU factory settings

Target	Setting	Status
Operation mode	Online mode	The CPU module accesses the N-IO modules from the N-ESB bus and optical ESB bus through the NIU.
Status of the maintenance port	Enable	You can access the NIU from the N-IO maintenance tool.
Node number	Not set	The NIU is not operating correctly. You need to set the node number before connecting to the SCU.

B4.4 Checking the status of the maintenance port of the NIU

The status of the NIU maintenance port can be checked through the following tools and functions.

Status display

The status of the NIU maintenance ports can be checked by using the following tools:

- SCS Status Overview window of SENG
- SCS Status Display view of HIS
- SCS Node Status Display dialog box of HIS

Message

The SCS generates the following messages for the status and status change of the NIU maintenance port, and the status change of the NIU operation mode:

- A diagnostic information message that notices the status of the NIU maintenance port
- A safety control station status change message that notices the status change of the NIU maintenance port
- A safety control station status change message that notices the status change of the NIU operation mode

IOM report

The status of the NIU and NIU maintenance port is displayed in the IOM report.

B5. Security of SCS Maintenance Support tool

SCS Maintenance Support Tool has a security by setting a password to be entered when starting related windows. A password is set for each SENG.

This section describes how to set passwords for the SCS Maintenance Support Tool.

The password described in this section is not applicable if the Access Control and Operation History Management Package is used. Instead, the user enters the password that is set for each user in the Access Control and Operation History Management Package when starting the SCS Maintenance Support Tool.

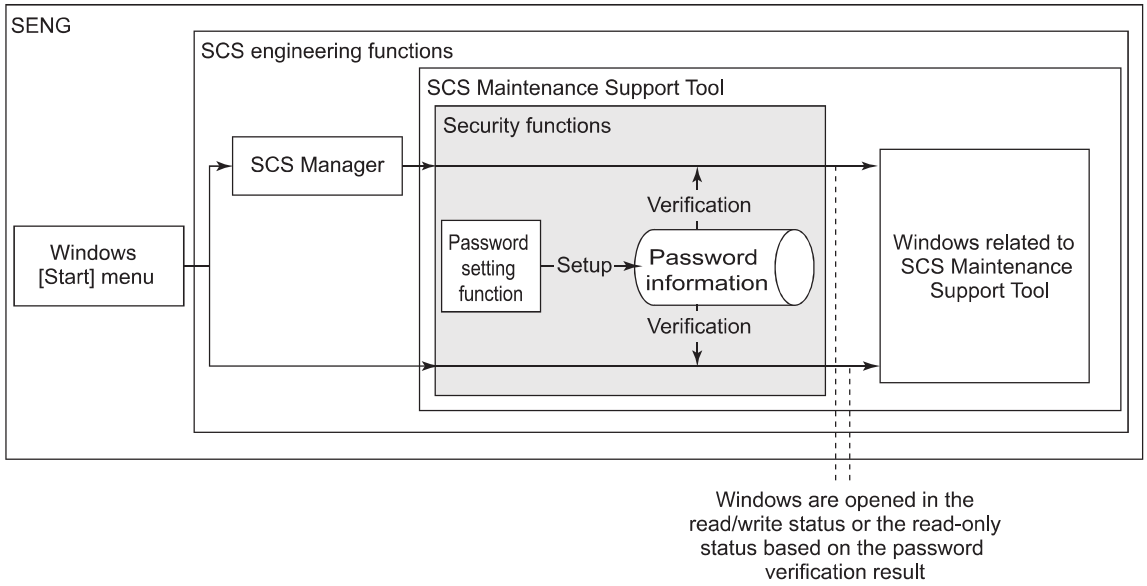


Figure B5-1 Security functions of Maintenance Support tool

TIP

No security is set in order to use SOE Viewer as it only displays information.

Setting a password for the SCS Maintenance Support Tool

The SCS Maintenance Support Tool requires a password entry every time you start a window to ensure the security of the SCS access. Password needs to be set for each SENG.

Each tool in the SCS Maintenance Support Tool can be operated for security by entering a password at the start of each tool. When the password entry is cancelled, the tools' operations are disabled for security and the window is in the read-only mode.

The following table shows whether tools can be operated or not when the password is entered and when password entry is cancelled.

Table B5-1 Operation of SCS Maintenance Support tool

Tool	Operations provided security	Inputting a password	Without inputting a password
SCS State Management Window	IOM Download	Enabling operation	Read Only
	Output Enable Operation	Enabling operation	Read Only
	Output Module Start Operation	Enabling operation	Read Only
	Setting Time	Enabling operation	Read Only
Diagnostic Information Window	Confirmation and Deletion of Diagnostic information	Enabling operation	Read Only
Setup Tool	Setting and change of display font, color and operating methods for confirming or deleting messages	Enabling operation	Read Only
SOE Viewer	Display of events of SCS and generation of report	Enabling operation	Enabling operation
Message Cache Tool	Setting of message collection, initialization of TRIP information in SCS and storage and deletion of cache data.	Enabling operation	Read Only

How to set and change a password for SCS Maintenance Support tool

The Change Maintenance Support Password dialog box is used to specify or change the password that the user must enter when starting the SCS Maintenance Support Tool.
To use SCS Maintenance Support Tool, make sure to set the password first.

TIP

No password is set automatically after installing SENG. Make sure to set a password at this stage.

1. Open the window related to SCS Maintenance Support Tool from SCS Manager or [Start] menu of Windows.
   When the window requiring a password is opened, the Input Maintenance Support Password dialog box appears.

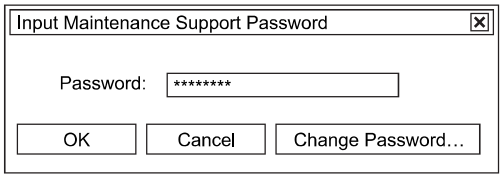


Figure B5-2 Input Maintenance Support Password dialog box

2. Click the [Change Password] button.
   The Change Maintenance Support Password dialog box appears.

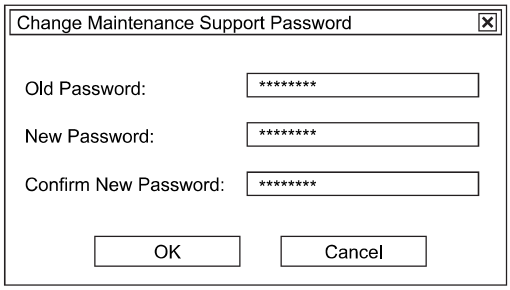


Figure B5-3 Change Maintenance Support Password dialog box

3. Enter the current password in the [Old Password:] field. Enter a new password in the [New Password:] field, and once again in the [Confirm New Password:] field.
   The passwords you have entered appear as a series of asterisks (*).
4. Click [OK].
   The password is set.

Specification for passwords

- A password is a maximum 16 of single-byte alphanumeric characters and following symbols including a space character. The password is case-sensitive.
  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~
- Set a password for each SENG-installed PC.
- There is no password when SENG is installed for the first time.
- Set a password when starting the SCS Maintenance Support Tool for the first time.

How to enter SCS Maintenance Support tool password

To start SCS Maintenance Support Tool, the correct password must be entered.
Once you enter the correct password, you are allowed to perform writing and customization operations using SCS Maintenance Support Tool.

IMPORTANT

If you fail to enter the correct password, SCS Maintenance Support Tool is started in the read-only status.

1. Open the window related to SCS Maintenance Support Tool from SCS Manager or [Start] menu of Windows.
   When the window requiring a password is opened, the Input Maintenance Support Password dialog box appears.

   If the current window is called from another window of SCS Maintenance Support Tool, the Input Maintenance Support Password dialog box does not appear, because the security is inherited.

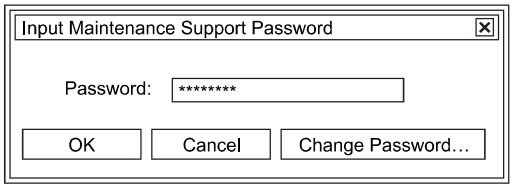


Figure B5-4 Input Maintenance Support Password dialog box

2. Enter a password in [Password:] text box.

All characters you enter are displayed as asterisks (*).

3. Click the [OK] button.
   If you enter the correct password, the window is opened in the read/write status.

   Click the [Cancel] button to start the window related to SCS Maintenance Support Tool in the read-only status.

   Click the [Change Password] button to display the Change Maintenance Support Password dialog box.

B6. Access control and history management

When using the Access Control and Operation History Management Package, the functions that can be used by a user are restricted based on the access rights for that user.

SEE ALSO For more information about Access control and operation history management package, refer to:

E., “Access Control/Operation History Management functions” in Engineer's Reference Manual (IM 32P04B10-01EN)

User management

The package has a function that enables management of the users who work with SCS Manager and the SCS Maintenance Support Tool. In AD Suite, you can set access rights to the targets of operation for each user role. The user management function is used to register and delete engineers and manage the passwords of engineers. It also keeps records of the operations that were performed by each user.

Access control

The access control function enables you to check engineers who operate the SENG, restrict login or operations on the SENG, and control authorization of engineering operations.

In AD Suite, you can define access rights to files and folders on the AD Server and various functions for all users who perform engineering and maintenance of ProSafe-RS.

Operation history management

This function enables to keep a log of the operations performed by an engineer on the SENG and save the changed project information when a download to an SCS is performed.

In AD Suite, operation history management is available for the following editors and features:

- Safety I/O Editor, Safety Communication I/O Editor, and IOM Definition Editor of AD Organizer
- SCS Manager, builders, and tools including the SCS Maintenance Support Tool
- RS Generation Manager

The change history on all builders and editors is saved on the AD Server and can be viewed in the history window of AD Organizer.

Appendix 1. Glossary

The following terminologies are used in the User's Manual of this product.

Table Appendix 1-1 Terminologies used in User's Manual

Terminology	Meaning
Access control	A functionality to restrict user operations in each SENG. A SENG terminal where access control is applied requires an engineer name and password entry to perform particular operations. When an engineer tries to make an engineering operation, the engineer can not execute the desired action unless the engineer has the permission to perform the operation. Access Control and Operation History Management Package is required.
ADL	Inter-station data link block of CENTUM FCS
AIO module	Generic term for analog input/output modules. Universal type I/O modules with defined AI and AO are included.
AIO/DIO module	Generic term for analog input/output modules and discrete input/output modules. Universal type I/O modules with defined AI, AO, DI, and DO are included. Communication modules are not included.
Alarm class	Alarm information added to diagnostic information messages. On SENG, diagnostic information messages are displayed in different colors with different alarm marks according to the alarm class. • Class 1 (serious alarm) • Class 2 (moderate alarm) • Class 3 (minor alarm) • Class 4 (notification alarm)
Alarm priority	Process alarm information that is needed when ProSafe-RS is integrated with CENTUM. Alarm priorities are in five levels: high-priority alarm, medium-priority alarm, low-priority alarm, logging alarm, and reference alarm.
Alarm Priority Builder	The builder used to define process alarm priority levels when ProSafe-RS is integrated with CENTUM. For each alarm priority level, you can define the output style and alarm action on occurrence/recovery of process alarms generated in SCS.
Alarm processing table	The table that defines the process alarms' display color and alarm priority corresponding to the alarm status on CENTUM HIS. On ProSafe-RS, you can import the alarm processing table defined on CENTUM to use it for reference.
Alarm Processing Table Builder	The builder used to import the Alarm Processing Table defined on CENTUM into SCS project.
All output shutdown	To shut down all the output modules when the CPU stops due to a fatal error. During all output shutdown, the fail-safe values are output.
All Program Copy (APC)	In dual-redundant CPU modules, to copy the memory contents of the control-side module to the stand-by-side module.
Analog Input/Output modules with HART function	An analog input/output module that supports HART communication

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Application logic execution function	The function that monitors the safety condition of the plant and performs pre-determined safety operations on detecting any hazards. Specifically, it denotes the following features and is used as the generic term for these features: • Input processing of the process data from the field • Execution of user-defined application logic • Outputting process data to the field • Communication data I/O (Subsystem communication, Safety Subsytem communication) • Inter-SCS safety Communication • SCS Link Transmission • Self-diagnosis
Application run time	The proportion of the time in a scan period of the SCS during which the CPU is working for the application execution functions. (Represented in percentage.)
Automatic IOM download	For dual-redundant AIO/DIO modules of a running SCS, if only the standby-side AIO/DIO module is replaced for maintenance, the configuration information is automatically downloaded from the control-side module to the standby-side module after replacement. This function is called automatic IOM download.
Behavior at abnormal calculation	The setting item of an SCS that specifies whether the SCS is stopped when an abnormal calculation, such as an overflow in floating-point data calculation, has occurred due to a defect in the application logic. It also refers to the behavior of the SCS specified with this setting.
Binding List View	The view on SCS Manager that is used to associate the variables for inter-SCS safety communication between producer SCS and consumer SCS. See Workbench User's Guide for more information.
Binding variable	Variables that link variables of producer SCS and variables of consumer SCS performing inter-SCS safety communication. The producer variables of a producer SCS need to be grouped for each consumer SCS that receives them. The consumer variables of a consumer SCS also need to be grouped for each producer SCS that sends them. These groups are called "binding groups."
Build	The operation that is run on SCS Manager to generate the database to be downloaded to a target SCS.
Burnout	One of input module action specifications when Thermocouple or Resistance Temperature Detector input has an open circuit. Selectable options at open circuit are to clamp the input to an upper or a lower limit or to disable burnout actions. Clamping to an upper limit is called burnout upscale and clamping to a lower limit is called burnout downscale.
CENTUM	In the user's manuals of ProSafe-RS, the generic term that refers to CENTUM VP and CENTUM CS 3000.
CENTUM project folder	The folder storing the data of the CENTUM project to be connected to SCS projects. When the system is integrated with CENTUM, you need to specify this folder in the SCS Project Properties dialog box.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
CI Server	Integrated operation and monitoring system developed by YOKOGAWA
Clean Project	The command on SCS Manager that deletes the files created in the previous run of the build command. After Clean Project is run, only offline downloading is possible.
Communication I/O Lock Window	This SENG window is used to lock/unlock I/O data for subsystem communication and safety subsystem communication. You can set values to the I/O data locked through this window. This window is used on SENG for maintenance and testing purposes.
Communication module	A module used to implement communications with systems (such as PLCs) from other companies. It is treated as one of the input/output modules.
Consumer SCS	SCS which receives data in inter-SCS safety communication.
Control bus driver	A driver software on a PC necessary to perform control bus communications via V net or Vnet/IP network.
Control bus interface card	An interface card installed to a PC to allow it connecting to V net.
CPU module	The main module that works to implement the control performed by SCS.
Cross Reference Analyzer	One of the Safety Analyzers. A Safety Analyzer which shows the following information in the screen or in an analysis report. • Differences between the previously downloaded application (which is currently running on the SCS) and the application that is to be downloaded • The scope that will be affected by downloading the new application This tool enables you to narrow the scope of re-testing when the application logic has been modified.
Cycle Time	Another name for the scan period of application logic execution functions. It is defined by setting the [Cycle Timing] in the Resource Properties dialog box of SCS Manager.
Database Validity Check Tool	The tool that checks the mutual validity of the work database, the master database and the SCS database within an SCS. In addition, database can be repaired.
Debug mode	A mode of SCS Manager that is used in target tests. See Workbench User's Guide for more information.
Defined word	Definition of a constant expression, TRUE/FALSE Boolean expression, or keyword. Defined words are replaced by their corresponding expressions during compiling.
Diagnostic information message	SCS sends diagnostic information messages for detected faults and for the operation on the safety functions to notify user of events. In a system integrated with CENTUM, diagnostic information messages of ProSafe-RS are sent to HIS and treated as system alarms.
Dictionary View	The view on SCS Manager used to set parameters and define variables of POUs. See Workbench User's Guide for more information.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Digital input/output module	The name of the modules that handle discrete inputs/outputs.
DIO module	General term for discrete input/output (digital input/output) modules. Universal type I/O modules with defined DI and DO are included.
Discrete input	Input of a discrete (ON/OFF) signal
Discrete output	Output of a discrete (ON/OFF) signal
DO shutoff switch	A switch that shuts off the output of all DO channels when a critical failure that can prevent normal output with the DO channel of the universal type I/O module has occurred. This switch can be activated automatically by setting the parameter for the DO channel.
ENG	A computer installed with engineering function packages for system generation and maintenance of CENTUM.
Engineers' account builder	The builder used to register engineers that are managed by the access control/operation history management function. It is also used to define access rights of engineers. All the settings made on this builder are saved in the Engineers' account file.
Error level	The level of errors occurred in SCS. Errors are classified in three levels: fatal error, major error, and minor error. With a fatal error, the SCS cannot continue operation. With a major error, the SCS can continue operation but some of the safety functions are disabled. Minor errors do not affect safety functions of the SCS. The users are notified of the error level by diagnostic information message.
ESB bus (Extended serial backboard bus)	The bus for connecting the CPU node and I/O nodes of SCS. ESB bus coupler modules are installed in the CPU node while ESB bus interface modules are installed in I/O nodes. These modules are connected using ESB bus cables.
Ethernet communication module	The name of a module that supports Modbus TCP communication protocol. SCS uses this module to perform Modbus slave communication.
Event log file	The file containing SOE (Sequence Of Event) events which is stored in SCS. You can save this file to SENG.
Expanded test function	The function to perform SCS simulation tests using SCS simulators on multiple computers and running them in coordination. This function is available with the use of the Expanded Test package of CENTUM.
Extend scan period automatically	The function that automatically extends the scan period of application logic execution functions when the load of SCS becomes heavy.
External communication function	The function of SCS for exchanging data with external systems. It is designed so as not to affect the application logic execution functions and comprises the following features: • CENTUM Integration Function • SOER Function • Modbus Slave Communication Function • Diagnostic information collection • PRM-supported HART on-demand communication

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
External communication function block	Function blocks used as the interface for data setting to SCS from Modbus master in Modbus slave connection or data setting to SCS from a CENTUM station when ProSafe-RS is integrated with CENTUM. External communication function blocks are interference-free.
FAST/TOOLS:	SCADA system developed by Yokogawa
FCS simulator	A simulator program offered for CENTUM systems. It simulates the behavior of FCS on a computer.
Field Control Station (FCS)	A component of CENTUM system which performs process control in plants.
Field network	It denotes the network between ProSafe-RS and YFGW410.
Field wireless backbone network	A backbone network stipulated in ISA100.11a. It denotes the network between YFGW410 and YFGW510.
Field wireless network	A field wireless network for industries based on ISA100.11a. It denotes the network between YFGW510 and GS01.
Field wireless system	It denotes the wireless system consisting of YFGW410, YFGW510, GS01, field network, field wireless backbone network and field wireless network.
Fire and gas communication	This function is used for safe communication with GS01 wireless gas detector through management stations for YFGW410 field wireless network and access points for YFGW510 field wireless network, after implementing S2LP131 fire and gas communication module in SCS.
Forcing	The function to lock and change the values of inputs/outputs or variables of SCS. It is used on SENG for maintenance of SCS or debugging of application logic. This function is available while the security level of the target SCS is set to 1 or 0.
Forced I/O Viewer function	The function that displays a list of information such as variables locked in the SENG lock window.
Function Block Diagram (FBD)	A language defined in IEC 61131-3.
Function Block (FB)	POU defined in IEC 61131-3. Constituents incorporated in FBD/LD/ST.
Function (FU)	POU defined in IEC 61131-3. Constituents incorporated in FBD/LD/ST.
Generation time	The time at which build was run for an SCS project to generate SCS database. In the SCS State Management window or a system report, a generation date is shown for each type of database: POU DB, Variable DB, System DB, and Integration DB.
Global switch	An element of CENTUM FCS which can be set to the same logical value in all the FCSs within a domain. By using the SCS global switch communication feature of SCS link transmission, values of some global switches can be sent or received between CENTUM stations (FCS, APCS, or GSGW) and SCS.
Global variable	A variable which can be accessed by any POU.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Grouping override function block	A special type of override function block. Grouping override function blocks belonging to the same group can be controlled so that no more than one function block within the group is overriding at the same time.
Hardware Architecture View	A view on SCS Manager that graphically displays the SCS and the network. See Workbench User's Guide for more information.
High current output function	A functionality that can use several DO channels together to put high current in analog digital I/O module
Human Interface Station (HIS)	A component of CENTUM system. It is a computer installed with a set of operator interface package software that enable operation and monitoring. Monitoring of SCS is also possible from HIS.
iDefine-config file	An XML format file that is created by exporting the ProSafe-RS engineering data edited with iDefine. It contains information on POUs, internal variables, FB instances, parameters, and tag names. The information in this file can be reflected in the SCS project after imported to AD Organizer.
iDefine for ProSafe-RS	A functional safety lifecycle management tool for ProSafe-RS developed by Trinity It has functions such as Cause & Effect and State Analysis. In the ProSafe-RS User's Manual, iDefine for ProSafe-RS is described as iDefine.
iDefine Test Manager	A feature for using the test functions of ProSafe-RS from iDefine. By running iDefine Test Manager, you can test the application logic created with iDefine using the test functions of ProSafe-RS from iDefine. You can perform the logic simulation test, SCS simulation test, and target test of ProSafe-RS.
I/O Lock Window	The window used to lock/unlock the input/output channels of the AIO/DIO modules in SCS. You can set values to the input/output variables connected to the channels that have been locked through this window. This window is used on SENG for maintenance and testing purposes.
I/O Parameter Builder	The builder used to make settings of the parameters (I/O parameters) for nodes, input/output modules, and channels of SCS that specify the behavior of them.
I/O shutoff switch	A switch that shuts off the I/O of AI (2-wire), AO, and DI when a critical failure that can prevent normal output with the AO channel of the universal type I/O module has occurred. When the I/O shutoff switch is activated, the DO shutoff switch is activated at the same time. This switch can be activated automatically by setting the parameter for the AO channel.
I/O Wiring View	The view on SCS Manager used to create or delete input/output modules in SCS, set node addresses, define wiring between channels and variables. See Workbench User's Guide for more information.
Input module	General term for the analog input module, the digital input module, and the universal type I/O module to which input channels are defined.
Input valuable	Variables connected to the channels of an input module, which are used in POUs.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Input value at error occurrence	A predefined value that is output when a value from an input module becomes abnormal.
Input/Output module	Generic term for AIO/DIO modules and communication modules.
Integration with CENTUM	ProSafe-RS can be used by integrating with CENTUM VP or CENTUM CS 3000. In the User's Manuals of ProSafe-RS, the integration with CENTUM VP or CENTUM CS 3000 is referred to as "Integration with CENTUM."
Integrity Analyzer	One of the Safety Analyzers. The tool used to analyze the safety of the created application logic. The users are required to use this tool to detect the use of FB/FU that are unacceptable as safety functions. The results of analysis can be shown on the screen or output in the analysis report.
Interference-free	Does not interfere safety application.
Internal variable	Variables not connected to an input/output module, which are available for use in POUs.
Inter-SCS Communication Lock Window	The window used to lock/unlock the input/output data for inter-SCS safety communication on an SCS by SCS basis. You can set values in the inter-SCS safety communication FB of the SCS locked through this window. This window is used on SENG for maintenance and testing purposes.
Inter-SCS safety communication	Safety communication used to implement safety loops among multiple SCS. Safety communication by SCS link transmission is not included in this communication. Safety loops are implemented by defining the function blocks dedicated for inter-SCS safety communication (producer FB and consumer FB) and binding variables.
IOM Control Right Switching Tool	The tool used for switching the control right of AIO/DIO modules placed in redundant configuration. Redundantly configured communication modules cannot be switched with this tool.
IOM download	Processing which downloads the input/output configuration information such as I/O parameters to input/output modules. This processing may occur during online change download after changing I/O parameters of input/output modules using I/O Parameter Builder.
IOM download tool	A tool that is needed when input/output modules have been replaced due to a malfunction, etc. It is run from the SCS State Management window and downloads the input/output configuration information stored in the master database of the SCS project to the input/output modules.
IOM Report	A dialog box which shows the status and error-related diagnostic information about an individual input/output module. IOM Report is called up from the SCS Maintenance Support Tool.
IOM Reset Function	A function that allows you to restore an I/O module from SENG. Only in the cases when an I/O module stops because of failures on the field side, you can restore the module by manually executing IOM download from SENG.
Ladder Diagram (LD)	A language defined in IEC 61131-3.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Legacy model	A model of information security settings set on SENG. This model should be used when the standard model of security settings is too tight or when compatibility with other system is required.
Library project	A project database that can be used as a library independent of specific SCS. The functions and function blocks that are used in multiple SCSs can be created as library projects and be copied to each SCS project.
Link Architecture View	A view on SCS Manager which graphically shows the resources of SCS project and data links among the resources. On this view, you can define POUs, add variable groups, etc. See Workbench User's Guide for more information.
Local variable	Variables that can be used in only one POU.
Logic simulation test	Tests performed by running a logic simulator from SCS Manager. The logic simulator is a program that simulates the behavior of POUs on a computer.
Logical data	For input variables, the data passed from an input variable to the application logic. For output variables, the data passed from the application logic to an output variable. For internal variables, the data to be output from that internal variable. Normally, the values of physical data and logical data match. However, while a variable is under forcing, the connection between its physical data and logical data is disconnected, and therefore they may not match.
Manual operation function block	Function blocks used to output values to the application logic by manual operation from CENTUM HIS when the system is integrated with CENTUM. These function blocks output either BOOL-type data or analog-type data and can be used for valve operation.
Mapping element/Mapping block	In a system integrated with CENTUM, a mapping element or mapping block is created if you assign a tag name to an internal variable, input/output variable, or a specific type of function block of the application logic using the Tag Name Builder. This scheme enables access to the data in SCS from CENTUM by specifying a tag name.
Master database	The database stored in SENG and is running on a target SCS. It consists of source files containing definitions for the SCS and the SCS database generated by running a build of the source files.
Master database offline download	The function to download, to the CPU modules of an SCS, the SCS database saved on SENG as the master database, which was previously downloaded to the SCS for actual run. You need to run this download when you replace both CPU modules in the SCS. You do not need to run this download when you replace one of the dual-redundant CPU modules.
Master Database Restoring function	This tool restores the SCS project being edited to the state it was last downloaded to the target SCS. It is used to discard the changes made to the work database so far and revert it to the master database as the new work database for engineering. This tool is helpful when you have accidentally changed any settings that require offline download.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Modbus Address Builder	The builder that is used to define Modbus device addresses for Modbus slave connection.
Modbus slave connection	Connection for communications where SCS acts as a Modbus slave and the data in the SCS are read or set by the Modbus master (external device) via Modbus protocol. This communication is called Modbus slave communication.
Modification files viewer	A viewer to view modification files saved in an operation history database.
Multi-Language Editor	The editor used to create and edit application logic for SCS. With the Multi-Language Editor, application logic can be created using the following three languages, which are defined in IEC 61131-3. • Function block diagram (FBD) • Ladder diagram (LD) • Structured Text (ST) See Workbench User's Guide for more information.
Narrowband system	CI Server integrated environment and FAST/TOOLS integrated environment that set the network mode of Vnet/IP-Upstream as narrowband mode.
Network mode	The operating mode of Vnet/IP-Upstream. A mode that supports the network characteristic can be selected from the following modes by using the Domain Property Setting Tool. • Standard mode • Wide-area mode • Narrowband mode
N-IO node	It is an SCSP3 component that consists of the N-IO I/O unit for inserting N-IO and the node interface unit.
Offline download	The function to download the system program of SCS and the database generated using the engineering functions of SENG to a target SCS while the CPU of the SCS is stopped. The SCS is restarted after the offline download is completed.
Online change download	The function to download only the changes made to the application to a target SCS while the CPU of the SCS is running. Online change download is not possible depending on which items of the application have been changed.
Online monitoring function	The function to monitor the application logic running on SCS. You can monitor the values of variables and function blocks of a running program and the status of whether conditions are met or not. The online monitoring function is available through the following windows: FBD window, LD window, and ST window of Multi-Language Editor, Dictionary View, and SPY List Window.
Operating mode	Operating mode of SCS. There are five operating modes: Stop mode, Loading mode, Initial mode, Waiting mode, and Running mode. SCS normally runs in the Running mode.
Operation history database viewer	A viewer to view operation log saved in an operation history database.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Operation history management	Functionality to record operations performed by each SENG user into the operation log. When downloading to SCS, the information of the modified project data (modification file) is saved. These operation log or change information are saved into the operation history database. CHS5170 Access Control and Operation History Management Package is required.
Operation history management setup tool	A tool to setup access control and operation history management functionality.
Operation mark	A frame-shaped mark attached to a faceplate displayed on CENTUM HIS.It is used to make certain elements or function blocks easy to be distinguished. You can save in SENG the operation marks set for elements or function blocks of SCS and download the saved operation marks to SCS.
Optical bus repeater	The device used to extend the distance of V net by using fiber-optic cable.
Optical ESB bus repeater module	Generic term for the modules mounted in nodes in SCS when nodes in the SCS are connected with fiber-optic cables for the purpose of extending the distance of ESB bus. Optical ESB bus repeater master modules can be mounted in CPU nodes or I/O nodes, while Optical ESB bus repeater slave modules can be mounted only in I/O nodes. A master module and a slave module are connected on a one-to-one basis using a fiber-optic cable.
Output disable status	The status of output modules in SCS in which the output values of the application logic are not output from the modules. Channels of all the output modules are in this status immediately after the SCS is started up. To enable outputs from the output modules in this status, it is necessary to perform the output enable operation. The output disable/enable status is controlled for each output channel.
Output enable operation	The operation to connect outputs from the application logic to the channels of output modules. You can perform this operation from the I/O Channels Status dialog box of SCS Maintenance Support Tool on SENG. This operation places all the channels of all the output modules on the SCS in the Output Enable status, and output values of the application logic are output from output channels. However, channels generating errors remain in the Output Disable status. Performing the output enable operation immediately after an SCS is started also initiates inter-SCS safety communication, SCS Link Transmission, and subsystem communication.
Output module	General term for the analog output module, the digital output module, and the universal type I/O module to which output channels are defined.
Output Shutoff Switch	A switch that shuts off the output of a module when a critical failure that can prevent normal output of signals has occurred with the analog output module and the digital output module. This switch can be activated automatically by setting the parameter for the output module.
Output value at fault	The value that is output as the fail-safe value when an output module detects an error.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Output variable	Variables connected to the channels of an output module, which are used in POUs.
Override	The operation to forcibly fix the value of a variable of SCS to a predefined value while the SCS is running normally. In order to enable override operations from CENTUM HIS, create application logic for performing override operation by using override function blocks.
%WB	An element of subsystem communication I/O
%WW	Communication I/O data area of subsystem communication
%XB	An element of safety subsystem communication I/O
%XW	Communication I/O data area of safety subsystem communication
Partial Stroke Test (PST)	Inspection of emergency shutdown valves, which do not need to work in normal conditions. PST is performed by slightly moving the valve to check if the valve is not stuck at one position and that it can work properly when required.
Physical data	For input variables, the data read from an input module. For output variables, the data to be set into an output module. For internal variables, the data input to the variable. Normally, the values of physical data and logical data match. However, while a variable is under forcing, the connection between its physical data and logical data is disconnected, and therefore they may not match.
Plant Resource Manager (PRM)	A software product of Yokogawa that is used to manage field devices and other equipment used in a plant online.
Primary channel	A channel that can set high current output function for several DO together in analog digital I/O module. A channel with the smallest number among several DO used together
Process data	In ProSafe-RS, process data means analog input/output data and discrete input/output data.
Producer SCS	SCS which sends data in inter-SCS safety communication.
Program Organization Unit (POU)	Generic term for program, function block, and function that are defined in IEC 61131-3.
Project Attribute Tool	The tool that shows the attributes of SCS projects. It is mainly used when using test functions.
Project comparing tool	A tool to detect differences between two SCS projects, display and print them. This tool is able to compare work database and the master database of any SCS project.
ProSafe authentication mode	A user authentication mode to provide separate user management for ProSafe-RS users apart from Windows users when using access control and operation history management functionality.
ProSafe-RS	Safety Instrumented System that meets SIL 3 of the Safety Integrity Level (SIL) defined by IEC 61508. Product components of ProSafe-RS Lite are also included.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
ProSafe-RS I/O file	An xslx format file that contains the safety I/O list, safety communication I/O list and I/O module information, which is stored in the ADMDB. You can create this file for each SCS project. You import it to iDefine.
ProSafe-RS Lite	Safety Instrumented System that meets SIL 2 of the Safety Integrity Level (SIL) defined by IEC 61508.
ProSafe-SLS	Safety Instrumented System that meets SIL 4 of the Safety Integrity Level (SIL) defined by IEC 61508.
RAS function	RAS means Reliability, Availability, and Serviceability. This is an important standard when evaluating the system performance. Reliability indicates robustness against error occurrence, availability indicates shortness of downtime and serviceability indicates ease of repair at failure. The RAS function diagnoses whether hardware and software of SCS are running normally and handles maintenance of them if any errors are detected. It is one of the most essential SCS functions which shuts down the system, changes the status of SCS, and takes other actions according to the situation.
Resource	A set of application logic that is defined for a single SCS.
RS Project	A group of SCS projects that is defined in order to manage engineering data of multiple SCS projects together. The status of SCSs belonging to the same RS project can be monitored collectively by using the SCS Maintenance Support Tools.
Safety application	Application which monitors the safety status of the plant and, if any abnormality is detected, performs the safety action that is programmed for the abnormality.
Safety Control Station (SCS)	A station which performs safety control in ProSafe-RS systems. SCS consists of a CPU node and I/O nodes.
Safety Control Unit	The name of the hardware of a component of SCS on which CPU modules are mounted. Abbreviated as SCU. Also referred to as the CPU node.
Safety Engineering Station (SENG)	A computer installed with the SCS engineering functions, test functions, and maintenance functions. On SENG, you can perform engineering works, such as creation, downloading, and testing of the application logic, and maintenance of SCS.
Safety Node Unit	The name of the hardware of a component of SCS on which modules for the FIO other than the CPU modules are mounted. Abbreviated as SNU. Also referred to as the I/O node.
Safety subsystem communication	This function is used for safe communication between SCS of ProSafe-RS and its subsystems, with the SCS acting as the master.
Scan period of the application logic execution function	Of the two types of scan periods of SCS, the scan period at which the application logic execution functions are executed. It is defined by setting the [Cycle Timing] in the Resource Properties dialog box of SCS Manager.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Scan period of the external communication function	Of the two types of scan periods of SCS, the scan period at which the external communication functions are executed. This scan period is defined by setting [Scan Period for External System] on the SCS Constants Builder.
SCS Constants Builder	The builder used to set the constants and the mode of time synchronization of an SCS.
SCS database	Database in a format executable on SCS, which stores the results of engineering works done on SENG. SCS database consists of POU DB, Variable DB, System DB, and Integration DB.
SCS global switch communication	An interference-free type of SCS link transmission that is used to communicate with CENTUM FCS.
SCS Information dialog	The dialog box which shows the numbers of the POUs and variables used in the SCS project or the size of the area for storing them. It is a dialog box of the SCS Maintenance Support Tool.
SCS link transmission	The function of SCS that a local SCS broadcasts its data periodically to other stations within the domain. By using this function, a local SCS can also receive the data broadcasted by other stations and the received data can be referenced by the application logic. SCS link transmission is available in two modes: SCS link transmission safety communication and SCS global switch communication.
SCS Link Transmission Builder	The builder used to define SCS link transmission safety communication and SCS global switch communication.
SCS Link Transmission Lock Window	The window used to lock/unlock the data for SCS link transmission on an SCS by SCS basis. You can set values to the SCS link transmission communication data of the SCS locked through this window. This window is used on SENG for maintenance and testing purposes.
SCS link transmission safety communication	A type of SCS link transmission that can implement safety loops.
SCS Maintenance Support Tool	A set of tools to facilitate maintenance of SCS. These tools are for supporting maintenance tasks and analysis to find out the cause of errors, not provided for the monitoring of SCS by the operator.
SCS Manager	The main window used to define SCS projects. It is also called "Workbench."
SCS Project	A project database corresponding to a single SCS. In ProSafe-RS, engineering data are managed for each SCS project. Within an SCS project, the database consists of master database and work database, which are managed separately.
SCS project attribute	Attributes given to SCS projects for the testing of SCS. You can specify one of three attributes: default project, current project, and user-defined project. The project attribute determines whether the project can be downloaded to a target SCS, whether the project can be tested by SCS simulation, etc.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
SCS Project Properties	This is the title of the dialog box on SCS Manager that is used to define SCS properties such as the model name, domain number, and station number. When the system is integrated with CENTUM, the location of CENTUM project folder is also defined in this dialog box. See Workbench User's Guide for more information.
SCS security level	The numeric value which shows the degree of how the data in the SCS is protected against data setting access from external devices or by personnel. The security levels are 0, 1, or 2, and SCS usually runs at level 2, which is the highest level. Level 0 is called the offline level, and levels 1 and 2 are called the online level.
SCS simulation test	Testing with SCS Simulators. SCS simulator is a program to simulate SCS actions on a computer.
SCS taglist generation	The function to generate an SCS taglist, which is required for monitoring SCS from CENTUM HIS. SCS taglist generation is run by selecting the [SCS Taglist Import] command on System View of CENTUM. SCS taglist is a database that is defined based on the tag names assigned to function blocks and other elements of SCS.
SCS Test Function Window	A window which manages starting and quitting of SCS simulator. You can start this window from SCS Manager or System View of CENTUM.
SCSL2-S (SCSL2)	SCS which uses L1SC70S/L1SC70D as the CPU node.
SCSP1-S (SCSP1)	SCS which uses SSC50S/SSC50D as the CPU node.
SCSP2-S (SCSP2)	SCS which uses SSC60S/SSC60D as the CPU node.
SCSP3-S (SCSP3)	SCS that uses S2SC70S/S2SC70D as the CPU node.
SCSV1-S (SCSV1)	SCS which uses SSC10S/SSC10D as the CPU node.
SCSU1-S (SCSU1)	SCS which uses SSC57S/SSC57D as the CPU node.
Self document	A function of SENG which prints out the definitions of SCS projects in certain formats.
Self-diagnosis	The schema of SCS for detecting abnormality in hardware and software by itself. It is run periodically and if any abnormality is detected, a diagnostic information message and status information are generated. The diagnostic information messages are sent to SENG and CENTUM HIS. The status information can be referenced by the application logic.
Sequence of Event Recorder (SOER)	A function that records events detected by SCS so that the user can analyze them. The collected and saved event information can be shown on the SOE viewer of SENG or CENTUM HIS.
Serial communication module	The name of a module that supports Modbus communication protocol (RTU mode). SCS uses this module to perform subsystem communication or Modbus slave communication.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Stand-alone ProSafe-RS system	The ProSafe-RS system that is not integrated with the CENTUM system ,CI Server system, nor FAST/TOOLS system. The following cases apply to this system: • Stand-alone SCS configuration • When temporarily separated from the CENTUM system , CI Server system, or FAST/TOOLS system during engineering (including when the CENTUM system , CI Server system, or FAST/TOOLS system is finally integrated) • Including when connected to PRM or STARDOM
Stand-alone SCS configuration	A system configuration where an SCS which is connectable to Vnet/IP network runs alone without being connected on Vnet/IP network.
Standard model	A model of IT security settings set on SENG. The standard model is categorized into two types according to the management of computers on the Windows network: Windows domain type and stand-alone type.
Start output module operation	The operation to recover the outputs of a module that were shut off by the activation of the output shut-off switch. This operation is performed using the SCS maintenance support tool. After recovery, all the channels of the output module are in the output disable status, so the output enable operation is required to deliver outputs.
Signal category	Classification of AI/AO/DI/DO
Structured Text (ST)	A language defined in IEC 61131-3.
Subsystem communication	Communications performed between SCS and a subsystem. In this communication, SCS acts as the communication master and reads/writes data from/to the subsystem. Modbus protocol is supported in subsystem communication.
Subsystem communication module	Another name of serial communication module. This name is used when the serial communication module is used for subsystem communication.
System function block	Function blocks which indicate the status of SCS. System function blocks have a name beginning with "SYS_."
System View	The main window of the system generating functions of CENTUM. System View plays a central part in CENTUM engineering works.
Tag Name Builder	The builder used to define tag names for function blocks and variables for use in a system integrated with CENTUM. Annunciator messages are also defined on this builder. By defining tag names using this builder, their mapping blocks or elements are created.
Target test	Testing of created application on an actual SCS by using the test functions.
Test Project Creating Tool	The tool used to create projects for SCS simulation test.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Time synchronization method	Method of system time synchronization. For SCSV, V net time synchronization or IRIG-B time synchronization can be selected. For SCSP, only Vnet/IP time synchronization is used. • V net time synchronization: The V net time is set to the CPU modules and input modules of the SCS. • IRIG-B time synchronization: Time information is acquired via IRIG-B from the standard clock installed outside the system and set to the CPU modules and input modules of the SCS. • Vnet/IP time synchronization: The network time on Vnet/IP is set to the CPU modules and input modules of the SCS.
Trip signal file	A file on SCS that stores the SOE data of the event specified as the trip signal and the data of the events before and after that event. This file can be saved into SENG. The signals that can be specified as trip events are the signals of DI/DO modules and the signals of function blocks dedicated to SOE.
Universal type I/O module	General term for the modules that can switch signal category of I/O module channels by software setting
Unit for optical ESB bus repeater module	A unit which is connected to SCS and exclusively used for mounting ESB bus optical repeater modules.
User-defined function	Functions defined by the user. You can create user-defined functions by using Multi Language Editor.
User-defined function block	Function blocks defined by the user. You can create user-defined function blocks by using Multi Language Editor.
User-defined project	A project created using Test Project Creating Tool. This project is for SCS simulation tests and cannot be downloaded to actual SCS.
Vnet/IP device	The device that is connected with Vnet/IP. Vnet/IP interface card (model: VI702) and processor module (model: SCP451, SCP461, S2CP471, and L1CP471) are included.
V net bus repeater	The device used to extend the distance of V net bus coaxial cable.
V net router	The device used to connect a V net domain and a Vnet/IP domain. Engineering of V net router is done on the CENTUM system.
Version Control Tool	A function that manages the change history of SCS projects and assists the user with system updating tasks. By using the Version control tool, you can save the SCS project data at a certain point with a version number and restore the project data of a certain version.
Virtual domain link transmission	Virtual domain link transmission provides virtual domain capability to V net domain and Vnet/IP domain connected with V net router style S3 or above. SCS global switch communications are allowed between SCS and FCS in the virtual domain and these communications are called virtual domain link transmission.
Vnet/IP interface card	An interface card installed to a PC to allow it connecting to Vnet/IP network.

Continues on the next page

Table Appendix 1-1 Terminologies used in User's Manual (Table continued)

Terminology	Meaning
Vnet/IP open communication driver	A driver software on a PC necessary to perform open communications (Ethernet communications) on Vnet/IP network.
Watch Dog Timer (WDT)	A mechanism which allows a system to self-diagnose to check if it is running normally at a constant period. SCS also has a WDT.
Windows authentication mode	A user authentication mode to manage a ProSafe-RS user as a Windows user when using access control and operation history management functionality.
Wiring check adapter	An element used to detect faults in the wiring between discrete input modules and field devices. Two types of wiring check adapters are available: SCB100 for detecting disconnections and SCB110 for detecting short-circuits.
Work database	The results of engineering are first saved in a work database. A work database consists of source files containing definitions for the SCS and the SCS database generated by running a build of the source files.
Workbench	Another name of SCS Manager. Workbench User's Guide is the help file that explains the development environment of SCS application. You can read Workbench User's Guide while you perform engineering works in the development environment called up from SCS Manager. (However, Workbench User's Guide does not include explanations about the tools started from the launchers selected in the [Tools] menu of SCS Manager.)

Appendix 2. List of links

This section provides information and links to the operation that are required in using the ProSafe-RS software and hardware in each typical scene.

- To know the type of the SCS hardware
- To know the function of the SCS software
- To know what type of software can be used in SENG
- To know the functions and precautions when using SENG on the virtualization platform
- To know the function of the tool that are included in the SCS Maintenance Support Tool
- When wanting to know the operation in an emergency.
- To know the procedures and precautions of online change download
- To replace the ProSafe-RS equipment
- When wanting to know about connections with other systems.

Information on the types of SCS hardware

Information on the types of SCS hardware is as follows.

SEE ALSO

For more information about types of the safety control unit, refer to:

A5.1, “Safety control unit” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about types of input/output modules, refer to:

“■ I/O module types” in A5.3, “Restrictions on installation of hardware” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about configuration of the safety control unit, refer to:

B1., “Configuration of SCU” in Hardware User's Guide (IM 32P06C10-01EN)

For more information about configuration of the safety node unit, refer to:

B2., “Configuration of SNU” in Hardware User's Guide (IM 32P06C10-01EN)

For more information about configuration of the unit for mounting the optical ESB bus repeater module, refer to:

B3., “Configuration of unit for optical bus repeater module” in Hardware User's Guide (IM 32P06C10-01EN)

For more information about equipment configuring the FIO node, refer to:

B4., “FIO node devices” in Hardware User's Guide (IM 32P06C10-01EN)

For more information about equipment configuring the N-IO node, refer to:

B5., “N-IO node devices” in Hardware User's Guide (IM 32P06C10-01EN)

Information on the functions of SCS software

Information on the SCS software is as follows.

SEE ALSO

For more information about overview of SCS software configuration, refer to:

“■ Overview of SCS software configuration” on page A3-1

For more information about RAS function of SCS, refer to:

A3.2, “RAS (Reliability, Availability, Serviceability) functions of SCS” on page A3-10

For more information about scan period of SCS, refer to:

A7., “Performance and scan period in the SCS” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about I/O of SCS, refer to:

A6., “Inputs and outputs of SCS” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about Forcing function, refer to:

F8., “Forcing function” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about types of POU and the use thereof, refer to:

1., “Overview of POU” in POU Reference Manual (IM 32P03B20-01EN)

For more information about SCS link transmission, refer to:

A6.1, “Overview of the SCS link transmission” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about SCS global switch communication, refer to:

A6.5, “SCS global switch communication” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about Inter-SCS safety communication, refer to:

A7., “Inter-SCS safety communication” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about SOER, refer to:

A8., “SOER functions and how to use them” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about Subsystem communication, refer to:

D1., “Common items regarding subsystem communication functions” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about Safety subsystem communication, refer to:

E., “Safety subsystem communication” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about Modbus slave communication, refer to:

F1., “Common items regarding the Modbus slave communication function” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about DNP3 communication of SCSU1, refer to:

G., “DNP3 slave function” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about Gas flow rate calculation function of SCSU1, refer to:

B2., “Gas flow rate calculation function” in Integration with CI Server (IM 32P04D20-01EN)

Information on the functions and precautions when using SENG on the virtualization platform

Information regarding functions and precautions when using SENG on the virtualization platform is as follows.

SEE ALSO For more information about functions and precautions when using SENG on the virtualization platform, refer to:

A7., “Virtualization platform” on page A7-1

Information on the software that can be used on SENG

Information on the software that can be used on SENG is as follows.

SEE ALSO

For more information about AD Suite, refer to:

A., “Overview of Automation Design Suite” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about SCS Manager, refer to:

A10.2, “SCS Manager” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about SCS Project Properties dialog box, refer to:

C1.2.5, “SCS Project Properties dialog box” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about SCS Constants Builder, refer to:

C1.2.6, “SCS Constants Builder” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about Link Architecture View, refer to:

“■ Link Architecture View” in A1.2, “Windows used to create application logic” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about Multi-Language Editor, refer to:

“■ Multi-Language Editor” in A1.2, “Windows used to create application logic” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about overview of Safety Analyzers, refer to:

C5., “Testing with the Safety Analyzers” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about the method for engineering iDefine, refer to:

D5., “Engineering by using iDefine” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about tools used for engineering of SCS, refer to:

F., “Tools and functions used with engineering of ProSafe-RS” in Engineer's Reference Manual (IM 32P04B10-01EN)

■ Information on the functions of the SCS Maintenance Support Tool

Information on the functions of the SCS Maintenance Support Tool is as follows.

SEE ALSO

For more information about overview, refer to:

A6.1, “Relationships among functions of SCS Maintenance Support Tool” on page A6-2

For more information about security for the SCS Maintenance Support Tool, refer to:

B5., “Security of SCS Maintenance Support tool” on page B5-1

For more information about SCS Status Overview window, refer to:

H1.1, “SCS status overview” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about SCS State Management window, refer to:

H1.2, “SCS State Management window” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about Diagnostic Information window, refer to:

H5.1, “Diagnostic Information window” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about SCS report, refer to:

“■ SCS Report” in H2., “System reports” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about IOM Report, refer to:

H3., “Checking diagnostic information by using IOM Report” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about SOE Viewer, refer to:

I4.3, “SOE Viewer” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about Forced I/O viewer function, refer to:

I4.1, “Forced I/O Viewer function” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about other tools used for operation and maintenance, refer to:

I4., “Tools for operations and maintenance” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Information on the operation in an emergency.

Information on designing the operation in an emergency and the actual operation in an emergency is as follows.

SEE ALSO

For more information about items to consider when planning operation in an emergency, refer to:

G., “Emergency procedures” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about behavior upon occurrence of an error with SCS and means for recovery, refer to:

G2., “Operations and recovery procedures during the SCS error occurrence” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Information on procedures and precautions of online change download

Information on procedures and precautions of online change download is as follows.

SEE ALSO For more information about how to run an online change download, refer to:

E1.1, “Online change download” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about procedures for online change of an application, refer to:

E1.2, “Entire procedure of online change of application” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about online change downloadable items, refer to:

E1.3, “List of applicable items for online change” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about precautions when performing an online change of an application, refer to:

E1.5, “Precautions for online change” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about precautions when performing an online change download with the N-IO node, refer to:

E1.6, “Precautions for online change download of N-IO” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about online changes with subsystem communication, refer to:

E1.7, “Online change of subsystem communication modules” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Information on tasks for replacing ProSafe-RS equipment

Information on tasks for replacing ProSafe-RS equipment is as follows.

SEE ALSO For more information about precautions when replacing ProSafe-RS equipment, refer to:

I1.2, “Maintenance for ProSafe-RS equipment” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about precautions and procedures for performing hardware maintenance, refer to:

E., “Maintaining the SCS” in Hardware User's Guide (IM 32P06C10-01EN)

Information on connections with other systems

Information on connections with other systems is as follows.

SEE ALSO For more information about integration with CENTUM, refer to:

B., “CENTUM integration” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about integration with CI Server, refer to:

A., “Integration with CI Server function” in Integration with CI Server (IM 32P04D20-01EN)

For more information about connecting with ProSafe-SLS, refer to:

D4., “ProSafe-SLS communication (for ALR121)” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about connecting with other YOKOGAWA software, refer to:

D., “Connection with Other Products” in Installation Guide (IM 32P01C50-01EN)

Revision information

Title : ProSafe-RS User's Guide

Manual No. : IM 32P01B10-01EN

Dec. 2023/11th Edition/R4.10 or later

A1.1, A1.2, A7.3.1	Added descriptions of Windows Server 2022.
A1.1, A1.2	Deleted descriptions of Windows Server 2012 R2.
A1.2	Changed the version of .NET Framework.
A1.2	Updated software version descriptions in "● Software that can coexist with ProSafe-RS," "■ CENTUM integration system," "■ CI Server integration system," "■ FAST/TOOLS integration system," "■ Use of iDefine," "■ Use of PRM," "■ Use of Exaopc," and "■ Use of Exaquantum."

Jun. 2023/10th Edition/R4.09

A1.2	Updated software version descriptions in "● Software that can coexist with ProSafe-RS," "■ CENTUM integration system," "■ CI Server integration system," "■ FAST/TOOLS integration system," "■ Use of iDefine," "■ Use of PRM," "■ Use of Exaopc," and "■ Use of Exaquantum."

Nov. 2022/9th Edition/R4.08

A1.2	Added descriptions of Windows Server IoT 2019 Standard.
A1.2	Updated software version descriptions in "● Software that can coexist with ProSafe-RS," "■ CENTUM integration system," "■ CI Server integration system," "■ FAST/TOOLS integration system," "■ Use of iDefine," "■ Use of PRM," "■ Use of Exaopc," and "■ Use of Exaquantum."

Jan. 2022/8th Edition/R4.07

A1.1, A1.2, A7.3.1	Added descriptions of Windows Server 2019.
A1.2	Updated software version descriptions in "● Software that can coexist with ProSafe-RS," "■ CENTUM integration system," "■ CI Server integration system," "■ FAST/TOOLS integration system," "■ Use of iDefine," "■ Use of PRM," "■ Use of Exaopc," and "■ Use of Exaquantum."
A7.2.1	Added descriptions of replication.
A7.4.2	Updated descriptions of resources required for a virtual machine and precautions when connecting remote desktop.

Feb. 2021/7th Edition/R4.06

Introduction, A7.4.1, Appendix1, 2	Updated FAST/TOOLS to CI Server.
A	Added descriptions about ProSafe-RS Lite.
A1.1, A1.2	Deleted descriptions about unsupported OS and added descriptions about supported OS.
A1.2	Updated software version descriptions in "● Software that can coexist with ProSafe-RS," "■ CENTUM integration system," "■ FAST/TOOLS integration system," "■ Use of iDefine," "■ Use of PRM," "■ Use of Exaopc," and "■ Use of Exaquantum", added CI Server integration system.
A2	Added a system configuration of ProSafe-RS.

Appendix 1	Added CI Server, iDefine for ProSafe-RS, ProSafe-RS, ProSafe-RS Lite, ProSafe-SLS, and SCSL2-S (SCSL2) in the glossary.

Dec. 2019/6th Edition/R4.05

Introduction	Updated description of registered trademarks and trademarks
A1.1, A5, A5.1, A6.4.2, B1	Added description of Forced I/O Viewer function
A1.2	Updated software version descriptions in "● Software that can coexist with ProSafe-RS," "■ CENTUM integration system," "■ FAST/TOOLS integration system," "■ Use of iDefine," "■ Use of PRM," "■ Use of Exaopc," and "■ Use of Exaquantum."
Appendix 1	Added Forced I/O Viewer function, and stand-alone ProSafe-RS system in the glossary.

Aug. 2018/5th Edition/R4.04

Introduction	Updated description of registered trademarks of YOKOGAWA.
A1.1, A1.2	Added descriptions of Windows Server 2016.
A1.2	Updated descriptions of .NET Framework.
A1.2	Updated software version descriptions in "● Software that can coexist with ProSafe-RS," "■ CENTUM integration system," "■ FAST/TOOLS integration system," "■ Use of iDefine," "■ Use of PRM," "■ Use of Exaopc," and "■ Use of Exaquantum."
A6	Added new section on virtualization platform.

Oct. 2017/4th Edition/R4.03.10

A1.2	Changed version number and added version description in CENTUM integration system, FAST/TOOLS integration system, use of iDefine, use of PRM, use of Exaopc and use of Exaquantum.
A2, A2.3.1	Added Safety Subsystem communication related descriptions.
A2.3.1, A2.4.1	Added description about Fire and Gas communication module.
A3, A4, B1	Added Safety subsystem communication engineering related descriptions.
Appendix 1	Added Field network, Field wireless backbone network, Field wireless network, Field wireless system, Fire and gas communication, %WB, %WW, %XB, %XW and safety subsystem communication in the glossary.

May 2017/3rd Edition/R4.03

Introduction	Deleted Windows Vista from "■ Trademark Acknowledgments."
A1.1, A1.2	Added descriptions of Windows 10 and deleted descriptions of Windows Vista and Windows Server 2008.
A1.2	Changed software versions, descriptions of ProSafe-RS functions and CENTUM release number, descriptions of coexistence of ProSafe-RS and CENTUM on the same computer, descriptions of whether or not ProSafe and iDefine can coexist on the same computer, and descriptions of versions.

Oct. 2016/2nd Edition/R4.02

Entire manual	Changed the symbols that indicate warning and caution.
Introduction	Updated descriptions in "■ Safety, Protection, and Modification of the Product," "■ Symbols," and "■ Trademark Acknowledgments." Added a new term in "■ Full Names and Simplified Terms."
A1.2	Updated software version numbers in "● Supported OS," "● Software that can coexist with ProSafe-RS," "■ CENTUM integration system," "■ FAST/TOOLS integration system," "■ Use of PRM," and "■ Use of Exaopc."

A1.2, A3, B1	Added iDefine related descriptions.
Appendix 1	Added iDefine-config file, iDefine Test Manager, and ProSafe-RS I/O file to the glossary.

Dec. 2015/1st Edition/R4.01

Newly published

■ For Questions and More Information Online Query: A query form is available on the following URL for online query. http://www.yokogawa.com/iss
■ Written by Yokogawa Electric Corporation
■ Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Attachment 9.2 Engg Guide Vol-1
GS 33J60F20-01EN

User's
Manual

ProSafe-RS
ProSafe-RS Lite

Engineering Guide Vol. 1

IM 32P01C10-01EN

YOKOGAWA
Yokogawa Electric Corporation

IM 32P01C10-01EN
11th Edition

Introduction

This manual is the engineering guide of ProSafe-RS.

This document explains an overview of ProSafe-RS functions and the cautionary notes which needs to be considered for engineering, based on the basic flow of engineering such as design, manufacturing, operation and maintenance of a safety equipment system by using ProSafe-RS.

Please refer to the Engineering Guide Vol.2 for the steps and precautions to take for creating application logic using ProSafe-RS engineering.

See the Appendix in the ProSafe-RS User Guide for the terminology in the descriptions of ProSafe-RS.

Notes and precautions regarding SCSP1 described in this document also apply to SCSU1.

CI Server Integration also contains FAST/TOOLS Integration function. If FAST/TOOLS Integration is used, replace the term “CI Server” with “FAST/TOOLS” in the user’s manual.

If you are using the Field Commissioning Support Package, replace “FieldMate Validator” in the User's Manual with “Field Commissioning Support Package.”

If you are using YFGW520, replace the term “YFGW510” with “YFGW520” in the User’s Manual.

This document is composed of the following parts.

- Part A Specifications and functions that are needed to design applications
  This part describes the specifications and functions that are needed to design a ProSafe-RS application. It describes the control bus, system time synchronization, and the engineering specifications and functions with a focus on ProSafe-RS and Control Station.
- Part B Designing applications
  This part describes the main points of the design specifications of ProSafe-RS systems.
- Part C Basics of creating applications
  This part describes the common work flow, precautions and common procedures to create a ProSafe-RS application.
- Part D Procedures to create applications using the I/O list engineering method
  This part gives an overview of the procedures of the automated design organizer when using I/O list engineering and the procedures when using iDefine.
- Part E Changing applications
  This part describes the steps to change applications online, the function that can export the application data to external folder and import the exported external file.
- Part F Installation and start-up
  This part explains the installation of ProSafe-RS system, the connection to field devices, a procedure of start-up including tests, commissioning and precautions for the start-up.
- Part G Emergency procedures
  This part describes the actions to be taken in an emergency situation during plant operation, behavior of SCS at error occurrence, and recovery procedures.
- Part H Monitoring the status of SCS
  This part describes the management of the SCS status. It explains the method to view the SCS status registered in RS projects, the detailed status of the specified SCS, and the detailed status of I/O module by using the IOM Report. It also mentions how to verify the diagnostic information message that is generated in the SCS.
- Part I Maintenance
  This part explains cautionary points and steps to maintain ProSafe-RS devices (such as I/O modules) and field devices.
- Appendix

11th Edition : Dec. 2023 (YK)
All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

This part describes the setting items of nodes, modules and channels, RS original engineering, cautionary points and maintenance of ProSafe-RS prior to R4, and maintenance of sales discontinued products.

Safety Precautions for Use

Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Be sure to confirm the specifications and required settings of the devices that are used in combination with the Product by referring to the instruction manual or other documents of the devices.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:



Indicates that caution is required. This symbol for the Product indicates the possibility of dangers such as electric shock on personnel and equipment, and also indicates that the user must refer to the User’s Manuals for necessary actions. In the User’s Manuals, this symbol is used together with a word “CAUTION” or “WARNING” at the locations where precautions for avoiding dangers are described.

<French> Signale qu’il faut faire preuve de prudence. Ce symbole pour le produit signale la possibilité d’un danger pour le personnel et l’équipement comme un choc électrique, et signale également que l’utilisateur doit se référer au Manuel de l’utilisateur afin de prendre les mesures nécessaires. Dans le Manuel de l’utilisateur, ce symbole est utilisé conjointement avec la mention «CAUTION» ou «WARNING» aux endroits où sont décrites les précautions pour éviter les dangers.



Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.

<French> Signale qu'il faut faire preuve de prudence avec la surface brûlante. Les appareils sur lesquels est apposé ce symbole risquent de devenir brûlants. Tout contact physique ou matériel avec ces appareils risque de provoquer des brûlures ou des dommages.



Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.



Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.

~ Indicates an AC supply.

⎓ Indicates a DC supply.

| Indicates that a component such as a power supply switch is turned ON.

○ Indicates that a component such as a power supply switch is turned OFF.

Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

Warning and Disclaimer

- Except as specified in the warranty terms, YOKOGAWA shall not provide any warranty for the Product.
- YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Product.

Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the Software Product's merchantability or suitability for any particular purpose, except as specified in the warranty terms.
- Purchase the appropriate number of licenses of the Software Product according to the number of computers to be used.
- No copy of the Software Product may be made for any purpose other than backup; otherwise, it is deemed as an infringement of YOKOGAWA's Intellectual Property rights.
- Keep the software medium of the Software Product in a safe place.
- No reverse engineering, reverse compiling, reverse assembling, or converting the Software Product to human-readable format may be performed for the Software Product.
- No part of the Software Product may be transferred, converted, or sublet for use by any third-party, without prior written consent from YOKOGAWA.

Documentation Conventions

Symbols

The following symbols are used in the User's Manuals.

 WARNING	Indicates precautions to avoid a danger that may lead to death or severe injury.
 CAUTION	Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.
IMPORTANT	Indicates important information required to understand operations or functions.
TIP	Indicates additional information.
	Indicates referenced content. In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

Typographical Conventions

The following typographical conventions are used throughout the User's Manuals.

Commonly Used Conventions throughout the User's Manuals

- Δ Mark
  Indicates that a space must be entered between character strings.
  Example:

  ```
  .ALΔPIC010Δ-SC
  ```

- Character string enclosed by braces { }
  Indicates character strings that may be omitted.

  Example:

  ```
  .PRΔTAG{Δ.sheet name}
  ```

Conventions Used to Show Key or Button Operations

- Characters enclosed by brackets [ ]
  When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a button name in a window, or an item in a list box displayed in a window.

  Example:

  To alter the function, press the [ESC] key.

Conventions of a User-defined Folder

- User-defined folder name enclosed by parenthesis ( )
  User definable path is written in a pair of parentheses.

  Example:

  ```
  (RS Project Folder)\SCS0101
  ```

If the RS Project Folder is `C:\MYRSPJT`, the above path becomes `C:\MYRSPJTSCS0101`.

Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.
If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

Definitions of Node and Module Terms

In the User's Manuals, nodes and modules are referred to by using collective terms, another terms, or abbreviations based on the following definitions:

- Definitions of nodes
  - Node: A node is a collective term for an FIO node and an N-IO node.
  - FIO node: This is a collective term for a safety control unit, a safety node unit, and a unit for optical ESB bus repeater module.
  - CPU node: This is another term for a safety control unit. The abbreviation of safety control unit is SCU.
  - I/O node: This is another term for a safety node unit. The abbreviation of safety node unit is SNU.
  - N-IO node: This is a collective term for a node interface unit and an N-IO I/O unit. The abbreviation of node interface unit is NIU.
- Definitions of modules
  - I/O module: This is a collective term for an FIO I/O module and an N-IO I/O module.
  - FIO I/O module: This is a collective term for an analog I/O module and a digital I/O module for FIO, and a communication module.
  - N-IO I/O module: This is a collective term for the modules that can be mounted on an N-IO I/O unit.
  - AIO/DIO module: This is a collective term for an analog I/O module, a digital I/O module, and a universal type I/O module.
  - Analog I/O module: This is a collective term for an analog input module and an analog output module.
  - Digital I/O module: This is a collective term for a digital input module and a digital output module.
  - Universal type I/O module: This is a collective term for the I/O modules for which the channel signal category can be changed by software.

- Input module: This is a collective term for an analog input module, digital input module, and a universal type I/O module with defined input channels.
- Output module: This is a collective term for an analog output module, digital output module, and a universal type I/O module with defined output channels.
- Communication module: This is a collective term for a serial communication module, an Ethernet communication module, and a fire and gas communication module.

Full Names and Simplified Terms

In the User's Manuals, simplified terms listed in the following table are used.

Table Info-1 Full Names and Simplified Terms

Full Name	Simplified Term
Automation Design Suite	AD Suite
Automation Design Organizer	AD Organizer
Automation Design Server	AD Server
Automation Design project	AD project
Automation Design Master Database	ADMDB
Automation Design Suite Administration Tool	ADS Administration Tool
iDefine for ProSafe-RS	iDefine
Modification Package	ModPack
SCSV1-S (SCS supporting the SSC10S/SSC10D safety control units)	SCSV1
SCSP1-S (SCS supporting the SSC50S/SSC50D safety control units)	SCSP1
SCSP2-S (SCS supporting the SSC60S/SSC60D safety control units)	SCSP2
SCSP3-S (SCS supporting the S2SC70S/S2SC70D safety control units)	SCSP3
SCSL2-S (SCS supporting the L1SC70S/L1SC70D safety control units)	SCSL2
SCSU1-S (SCS supporting the SSC57S/SSC57D safety control units)	SCSU1

Copyright and Trademark Notices

All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, PRM, Exaopc, FieldMate Validator, and STARDOM are registered trademarks or trademarks of Yokogawa Electric Corporation.
- The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

Engineering Guide Vol. 1

IM 32P01C10-01EN 11th Edition

CONTENTS

PART-A Specifications and functions that are needed to design applications.....A-1

A1. Overview of Vnet/IP network.....A1-1
- A1.1 Vnet/IP network system configuration.....A1-2
- A1.2 Device Connections in a Vnet/IP Domain.....A1-4
- A1.3 Connection between Vnet/IP domains.....A1-6

A2. ProSafe-RS security.....A2-1
- A2.1 Overview of ProSafe-RS security.....A2-2
- A2.2 Security for project database.....A2-7
- A2.3 Security of SCS Maintenance Support tool.....A2-8
- A2.4 Access control and history management.....A2-11

A3. Time synchronization.....A3-1

A4. Overview of SCS software configuration.....A4-1

A5. SCS hardware.....A5-1
- A5.1 Safety control unit.....A5-2
- A5.2 SCS hardware configuration.....A5-4
- A5.3 Restrictions on installation of hardware.....A5-10

A6. Inputs and outputs of SCS.....A6-1
- A6.1 Flow of AIO/DIO data.....A6-2
- A6.2 I/O variable.....A6-4
- A6.3 High current output function.....A6-7

A7. Performance and scan period in the SCS.....A7-1
- A7.1 Definition of SCS scan period.....A7-2
- A7.2 Automatic extension function for scan period of the application logic execution function.....A7-5
- A7.3 Locking of internal variables and performance in SCSP3/SCSL2/SCSP2.....A7-10

A8. RAS (Reliability, Availability, Serviceability) functions of SCS.....A8-1
- A8.1 SCS operating mode.....A8-3
- A8.2 Security level of SCS.....A8-6
- A8.3 Operations at SCS startup.....A8-12

A8.4 Diagnostic information management....A8-14
A8.5 Diagnosis for hardware....A8-16
A8.6 Dual-redundancy in the SCS....A8-17
A8.6.1 Redundant configuration in SCS....A8-18
A8.6.2 CPU redundant status....A8-21
A8.7 NIU status and security....A8-24
A8.7.1 Status of the NIU maintenance port....A8-25
A8.7.2 Operation mode of the NIU....A8-26
A8.7.3 Shifting the Status of the NIU....A8-28
A9. Capacity of SCS applications....A9-1
A10. Outline of the safety system generation function....A10-1
A10.1 Engineering method by using the safety system generation function....A10-2
A10.2 SCS Manager....A10-3
A10.3 Safety application definition....A10-7
A10.4 CENTUM integration application definition....A10-12
A10.5 Defining applications that use communication modules....A10-14
A10.6 CI Server integration application definition....A10-16
A10.7 Engineering tools....A10-17

Engineering Guide Vol. 1

IM 32P01C10-01EN 11th Edition

CONTENTS

PART-B Designing applications..... B-1
B1. Key points of basic design..... B1-1
B2. Procedure for engineering..... B2-1
B3. Example of ProSafe-RS system configuration.....B3-1
B4. System reaction time.....B4-1

Engineering Guide Vol. 1

IM 32P01C10-01EN 11th Edition

CONTENTS

PART-C Basics of creating applications.....C-1

C1. Preparing the project.....C1-1

C1.1 Type of project.....C1-2

C1.1.1 AD project.....C1-4

C1.1.2 RS project.....C1-5

C1.1.3 SCS projects.....C1-6

C1.1.4 Library project.....C1-9

C1.2 Procedures for creating projects.....C1-10

C1.2.1 Connecting to AD projects.....C1-11

C1.2.2 Creating RS projects.....C1-12

C1.2.3 Registering RS projects in the AD project.....C1-13

C1.2.4 Creating SCS projects.....C1-15

C1.2.5 SCS Project Properties dialog box.....C1-18

C1.2.6 SCS Constants Builder.....C1-21

C2. Work flow of creating applications for each engineering method.....C2-1

C2.1 Work flow of I/O list engineering.....C2-2

C2.2 Work flow of I/O list engineering with iDefine.....C2-11

C2.2.1 System configuration when using iDefine.....C2-12

C2.2.2 Relationship between ProSafe-RS engineering functions and iDefine.....C2-13

C2.2.3 Engineering by using iDefine.....C2-17

C2.3 Work flow for RS original engineering.....C2-26

C3. Precautions when creating applications.....C3-1

C4. Procedures for generating a database.....C4-1

C5. Testing with the Safety Analyzers.....C5-1

C5.1 Integrity Analyzer.....C5-2

C5.1.1 Methods for checking analysis results.....C5-3

C5.1.2 Integrity Analyzer window structure.....C5-9

C5.1.3 Confirmation of analysis results by project tree.....C5-12

C5.2 Cross Reference Analyzer.....C5-19

C5.2.1 Methods for checking analysis results.....C5-20

C5.2.2 Cross Reference Analyzer window structure.....C5-27
C5.2.3 Confirmation of analysis results by Dependency tree.....C5-30
C5.2.4 Checking with Analysis report.....C5-40
C5.2.5 Precautions on Cross Reference Analyzer.....C5-46
C5.2.6 Comparison with the original project.....C5-49
C6. Simulation tests..... C6-1
C7. Offline download to the target SCS.....C7-1
C8. Output enable operation..... C8-1
C9. Target tests..... C9-1

Engineering Guide Vol. 1

IM 32P01C10-01EN 11th Edition

CONTENTS

PART-D Procedures to create applications using the I/O list engineering method..... D-1

D1. Engineering based on the safety I/O list.....D1-1

D1.1 Overview of I/O list engineering..... D1-2

D1.2 Creating a new safety I/O list..... D1-3

D1.3 Operating a safety I/O list.....D1-4

D1.4 Defining I/O information by using Safety I/O Editor..... D1-5

D1.4.1 Starting the Safety I/O Editor..... D1-6

D1.4.2 Importing the I/O information list.....D1-16

D1.4.3 Comparing and reflecting the I/O information before and after import D1-19

D1.4.4 Editing a safety I/O list..... D1-21

D1.4.5 Exporting the I/O information in the safety I/O list..... D1-23

D1.4.6 Purpose of user definition and changing user-defined name..... .....D1-25

D1.5 Using the safety I/O parameter profile..... D1-26

D1.5.1 Starting Safety I/O Parameter Profile Editor..... D1-27

D1.5.2 Checking out the safety I/O parameter profile..... D1-28

D1.5.3 Defining the safety I/O parameter profile..... D1-29

D1.5.4 Deleting the safety I/O parameter profile..... D1-31

D1.5.5 Saving and checking in the safety I/O parameter profile..... D1-32

D1.5.6 Assigning the safety I/O parameter profile to the I/O of the safety I/O list..... D1-33

D1.5.7 Reflecting the updated safety I/O parameter profile to the I/O of the safety I/O list..... D1-34

D1.5.8 Exporting the safety I/O parameter profile..... D1-36

D1.5.9 Importing the safety I/O parameter profile..... D1-37

D1.5.10 Behaviors when importing the safety I/O list with the safety I/O parameter profile assigned..... D1-39

D1.5.11 Precautions for importing and restoring SCS projects including safety I/O parameters..... D1-40

D1.6 Saving the safety I/O list and performing check-in.....D1-41

D2. Engineering based on the safety communication I/O list..... D2-1

D2.1 Creating a new safety communication I/O list.....D2-4

D2.2 Operating a safety communication I/O list..... D2-5
D2.3 Starting Safety Communication I/O Editor..... D2-6
D2.4 Entering I/O information in the signal definition list.....D2-17
D2.5 Converting I/O information into a data structure that can be communicated with subsystems.....D2-21
D2.5.1 Overview of definitions for communication with subsystems..... D2-22
D2.5.2 Deciding the data structure..... D2-24
D2.5.3 Defining program groups..... D2-25
D2.5.4 Defining communication group..... D2-26
D2.5.5 Fixing the element numbers of the communication I/O..... D2-27
D2.5.6 Procedure for creating and wiring communication I/O variables..... D2-28
D2.6 Importing I/O information into the safety communication I/O list..... D2-30
D2.7 Exporting the I/O information in the safety communication I/O list..... D2-33
D2.8 Saving and checking in the safety communication I/O list.....D2-34
D2.9 Engineering after changing the safety communication I/O list..... D2-35
D3. Input/output module configuration definition..... D3-1
D3.1 Overview of the node and I/O module creation.....D3-2
D3.2 Starting the IOM Definition Editor..... D3-3
D3.3 Displaying for each specified setting item..... D3-4
D3.4 Creating the node and I/O module.....D3-5
D3.5 Editing the setting items of the node and I/O module..... D3-10
D3.6 Deleting the node or I/O module.....D3-11
D3.7 Exporting information from IOM Definition Editor.....D3-12
D3.8 Importing information to IOM Definition Editor.....D3-13
D3.9 Saving the node and I/O module and performing check-in..... D3-14
D4. Overview of RS generation..... D4-1
D4.1 Reflection process.....D4-2
D4.2 Build process of the SCS project..... D4-3
D4.3 Generation Manager window configuration..... D4-4
D4.4 Operating procedure of RS generation.....D4-8
D4.5 Error messages in Generation Manager..... D4-11
D4.6 Engineering after changing the safety I/O list and safety communication I/O list..... D4-13
D5. Engineering by using iDefine..... D5-1
D5.1 Engineering steps when starting iDefine from AD Organizer.....D5-2
D5.1.1 Operations in AD Organizer.....D5-3
D5.1.2 Operations in iDefine..... D5-5
D5.1.3 Operations in RS Generation Manager..... D5-7
D5.2 Engineering steps when starting iDefine directly.....D5-8
D5.2.1 Exporting the ProSafe-RS I/O file from AD Organizer..... D5-9

D5.2.2 Operations in iDefine..... D5-10
D5.2.3 Import the iDefine-config file by using AD Organizer..... D5-11
D5.3 Precautions when performing engineering by using iDefine..... D5-13

Engineering Guide Vol. 1

IM 32P01C10-01EN 11th Edition

CONTENTS

PART-E Changing application..... E-1

E1. Online change of applications..... E1-1

E1.1 Online change download..... E1-2

E1.2 Entire procedure of online change of application..... E1-4

E1.3 List of applicable items for online change..... E1-12

E1.4 Online change of scan period of the application logic execution function. E1-18

E1.5 Precautions for online change..... E1-20

E1.6 Precautions for online change download of N-IO..... E1-30

E1.6.1 Procedure for online change download of signal category of channels..... E1-33

E1.7 Online change of subsystem communication modules..... E1-36

E2. Import/Export function..... E2-1

E2.1 Precautions concerning import/export..... E2-2

E2.2 Export/import using AD Organizer..... E2-5

E2.3 Importing and exporting data that is managed by SCS Manager..... E2-7

E3. Modification and reuse of SCS project database..... E3-1

E3.1 Data transfer procedure during expansions/remodeling in modifications where online change is possible..... E3-2

E3.2 Data transfer procedure during expansions/remodeling in modifications requiring offline download..... E3-6

E3.3 Data transfer procedure during SCS project regeneration..... E3-9

E3.4 Reusing SCS project data..... E3-17

Engineering Guide Vol. 1

IM 32P01C10-01EN 11th Edition

CONTENTS

PART-F Installation and start-up..... F-1
F1. Procedure of installation and start-up..... F1-1
F2. Preparation before installation and start-up of N-IO nodes..... F2-1
F2.1 Configuring the N-IO node interface unit..... F2-2
F2.1.1 Using the Node Number Setting Tool..... F2-3
F2.2 Testing by using FieldMate Validator..... F2-6
F3. Overview of procedures to construct/maintain a stand-alone SCS configuration system..... F3-1

Engineering Guide Vol. 1

IM 32P01C10-01EN 11th Edition

CONTENTS

PART-G Emergency procedures..... G-1

G1. Operation flow during the error occurrence..... G1-1

G2. Operations and recovery procedures during the SCS error occurrence..... G2-1

G2.1 Actions taken at fatal error occurrence and recovery procedure..... G2-3

G2.1.1 Operations and recovery procedures during the error occurrence in the entire SCS..... G2-4

G2.1.2 Actions taken at CPU module error occurrence and recovery procedure..... G2-5

G2.1.3 Behavior at abnormal calculation..... G2-7

G2.2 Actions taken at major error occurrence and recovery procedure..... G2-11

G2.2.1 Actions taken at input module error occurrence and recovery procedure..... G2-12

G2.2.2 Actions taken at input channel error occurrence and recovery procedure..... G2-13

G2.2.3 Actions taken at output module error occurrence and recovery procedure..... G2-15

G2.2.4 Actions taken at output channel error occurrence and recovery procedure..... G2-17

G2.2.5 Operations and recovery procedures during the error occurrence in the universal type I/O module..... G2-22

G2.2.6 Actions taken at errors between CPU and Input/Output module and recovery procedure..... G2-24

G2.2.7 Actions taken at error occurrence for optical ESB bus repeater devices..... G2-26

G2.2.8 Operations during hardware error occurrence related to N-IO..... G2-30

G2.2.9 Operations at fire and gas communication error occurrence and recovery procedure..... G2-32

G2.3 Actions taken at minor error occurrence and recovery procedure..... G2-35

Engineering Guide Vol. 1

IM 32P01C10-01EN 11th Edition

CONTENTS

PART-H Monitoring the SCS status.....H-1
H1. SCS status display.....H1-1
H1.1 SCS status overview.....H1-2
H1.2 SCS State Management window.....H1-6
H2. System reports.....H2-1
H3. Checking diagnostic information by using IOM Report.....H3-1
H3.1 IOM Report of AIO/DIO modules.....H3-2
H3.1.1 Display format for the IOM Report of FIO.....H3-3
H3.1.2 Display format for the IOM report of N-IO.....H3-6
H3.1.3 Code system for causes of errors in the IOM Report.....H3-12
H3.2 IOM Report of communication modules.....H3-19
H4. Displaying I/O channel status.....H4-1
H5. Displaying SCS diagnostic information.....H5-1
H5.1 Diagnostic Information window.....H5-2
H5.2 Diagnostic Information window.....H5-3
H6. Monitoring by diagnostic information message.....H6-1
H6.1 Notification of error level through diagnostic information messages.....H6-2
H6.2 Acknowledging and deleting diagnostic information messages.....H6-4
H6.3 Diagnostic information message help function.....H6-7
H6.4 Printing diagnostic information messages.....H6-9
H7. Vnet/IP bus status.....H7-1

Engineering Guide Vol. 1

IM 32P01C10-01EN 11th Edition

CONTENTS

PART-I Maintenance I-1

I1. Maintenance of devices I1-1

I1.1 Utilizing the forcing and override functions during maintenance I1-2

I1.1.1 Override I1-3

I1.1.2 Utilization of the forcing function in SCS maintenance I1-4

I1.2 Maintenance for ProSafe-RS equipment I1-9

I1.3 Maintenance of field devices I1-18

I1.4 Maintenance of field wireless system devices I1-19

I1.4.1 Changing the setting information of YFGW410 ..... I1-20

I1.4.2 Replacing YFGW410 ..... I1-21

I1.4.3 Replacing YFGW510 ..... I1-22

I1.4.4 Removing YFGW510 ..... I1-23

I1.4.5 Adding YFGW510 ..... I1-24

I1.4.6 Changing the setting information (F-Parameter, communication period) of GS01 ..... I1-25

I1.4.7 Replacing GS01 ..... I1-26

I1.4.8 Removing GS01 ..... I1-27

I1.4.9 Adding GS01 ..... I1-28

I2. Maintenance of the system I2-1

I2.1 Proof test I2-2

I2.2 Tests for improving the rate of operation I2-3

I3. Setting system time I3-1

I4. Tools for operations and maintenance I4-1

I4.1 Forced I/O Viewer function I4-2

I4.1.1 Operation environment of Forced I/O Viewer function I4-3

I4.1.2 Forced-I/O information I4-4

I4.1.3 Grouping and registering SCS I4-10

I4.1.4 Distributing a registration file and SCS projects I4-11

I4.1.5 Precautions for Forced I/O Viewer function I4-13

I4.1.6 Screen configuration of Forced I/O Viewer Setup Tool I4-14

I4.1.7 Operations in Forced I/O Viewer Setup Tool I4-24

I4.1.8 Screen configuration of Forced I/O Viewer I4-30

I4.1.9 Operations in Forced I/O Viewer..... I4-35
I4.2 Message Cache Tool..... I4-38
I4.2.1 Setting stations..... I4-42
I4.2.2 Setting Message Cache Service..... I4-43
I4.2.3 Displaying data acquisition status..... I4-44
I4.2.4 Displaying disk cache usage status..... I4-45
I4.2.5 Initialization of tripping information..... I4-48
I4.2.6 Saving disk cache..... I4-49
I4.3 SOE Viewer..... I4-50
I4.3.1 SOE Viewer window..... I4-51
I4.3.2 SOE Viewer configuration..... I4-59
I4.3.3 Event mode operation..... I4-68
I4.3.4 Trip mode operation..... I4-71
I4.3.5 Troubleshooting SOE Viewer..... I4-73
I4.4 Master database offline download..... I4-76
I4.5 NIU maintenance port setting tool..... I4-77
I4.6 IOM Download tool..... I4-80
I4.7 IOM Control Right Switching Tool..... I4-83
I5. Procedures and precautions for adding a station or domain..... I5-1
I6. Procedures and precautions for adding or replacing Vnet/IP devices. I6-1

Engineering Guide Vol. 1

IM 32P01C10-01EN 11th Edition

CONTENTS

Appendix

Appendix 1. Settings for node, module, and channel.....App.1-1

Appendix 1.1 Setting items for nodes..... App.1-2

Appendix 1.2 Settings for modules..... App.1-5

Appendix 1.3 Settings for channel items..... App.1-8

Appendix 1.3.1 Common display items for channels..... App.1-9

Appendix 1.3.2 Settings for the AI channel..... App.1-11

Appendix 1.3.3 Settings for the AO channel..... App.1-26

Appendix 1.3.4 Settings for the DI channel..... App.1-32

Appendix 1.3.5 Settings for the DO channel..... App.1-35

Appendix 2. RS original engineering.....App.2-1

Appendix 2.1 Operations on SCS projects that are not registered in the AD project..... App.2-2

Appendix 2.2 Definitions of inputs/outputs..... App.2-3

Appendix 2.2.1 I/O Wiring View.....App.2-5

Appendix 2.2.2 I/O Parameter Builder.....App.2-12

Appendix 3. Precautions related to main specification additions and modifications.....App.3-1

Appendix 3.1 The major changes in R1..... App.3-2

Appendix 3.2 The major changes in R2..... App.3-3

Appendix 3.3 The major changes in R3..... App.3-13

Appendix 3.4 Major changes in R4..... App.3-15

Appendix 4. Maintenance of sales discontinued products..... App.4-1

Appendix 4.1 Time synchronization of SCSV1..... App.4-2

Appendix 4.2 Inter-SCS safety communication in a V net domain..... App.4-7

Appendix 4.3 Precautions when engineering CENTUM systems for using BCV and CGW..... App.4-8

Appendix 4.4 System expansion with V net router connection..... App.4-9

A. Specifications and functions that are needed to design applications

This part describes the following specifications and functions that are needed to design a ProSafe-RS application:

- Vnet/IP network
- Security of ProSafe-RS
- Time synchronization
- SCS software configuration, hardware, I/O, performance and scan period, RAS, and application capacity
- Safety system generation function

Read this to understand the specifications and functions when engineering or doing the feasibility study prior to designing.

SEE ALSO

For more information about the engineering method differs for each engineering tool used guidelines for selecting an engineering method, refer to:

"■ Guidelines for selecting an engineering method" on page A10-2

A1. Overview of Vnet/IP network

Vnet/IP is a control communication network that is used in ProSafe-RS systems that conform to the IEEE802.3 standards. It is a highly reliable network built in dual-redundant configurations.

Vnet/IP supports 1 Gbps or 100 Mbps transmission speed.

A Vnet/IP network is built by using network devices such as Layer 2 switches and Layer 3 switches, and transmission media such as UTP (Unshield Twist Pair) cables and optical fiber cables.

Communication paths of control communication

A Vet/IP network is a redundant network for control communication. In Vnet/IP, redundant buses are configured with independent subnets of bus 1 and bus 2.

Control communication is the communication for transferring control data.

Normally, bus 1 is used for control communication. When bus 1 fails due to a communication error, control communication is continued on bus 2.

An Ethernet network apart from the Vnet/IP is used for file transfer and data communication except for control communication.

Connecting Ethernet devices

Ethernet devices that do not use control communication are connected to an Ethernet network that was installed separately from the Vnet/IP.

SEE ALSO For more information about the Vnet/IP- Upstream network used in CI Server integration, refer to:

A., “Integration with CI Server function” in Integration with CI Server (IM 32P04D20-01EN)

A1.1 Vnet/IP network system configuration

This section describes the system configuration and components of the Vnet/IP network.

Vnet/IP network system configuration

The following figure shows an example of the Vnet/IP network system configuration.

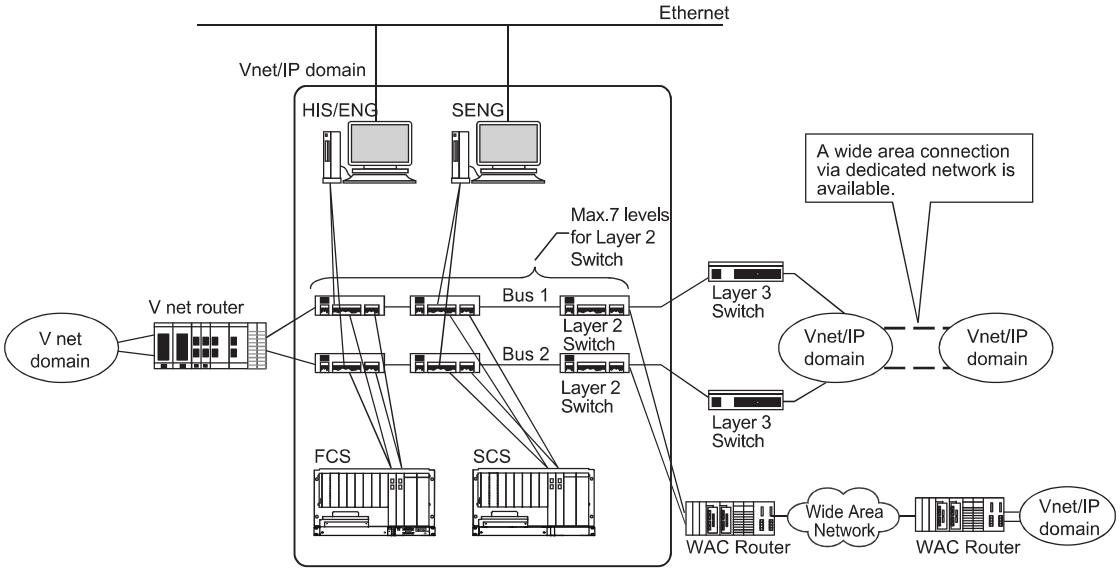


Figure A1.1-1 System components of a Vnet/IP network

SENG and HIS set up in the virtual machine on the virtualization platform are also connected to the Vnet/IP network.

SEE ALSO

For more information about system structure example on virtualization platform, refer to:

A7.2, “System configuration of virtualization platform” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

For more information about precautions related to Vnet/IP communication on the virtualization platform, refer to:

A7.4.1, “Precautions related to Vnet/IP communication on the virtualization platform” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

Components of Vnet/IP network

The components of the Vnet/IP network are as follows:

Vnet/IP station

A Vnet/IP device equipped station that is connected to a Vnet/IP network is referred to as a Vnet/IP station. A Vnet/IP station in a domain is connected to Layer 2 switches provided one for each bus. Vnet/IP stations are described below.

- Safety Engineering Station (SENG)
  SENG is a computer for ProSafe-RS engineering and maintenance. It is connected to a Vnet/IP network through a Vnet/IP interface card installed in the computer. The Vnet/IP interface card has two ports and each port is connected to a transmission cable for Vnet/IP to support redundant Vnet/IP buses.
- Safety Control Station (SCS)
  SCS is a station for ProSafe-RS safety control. The transmission speed of an SCS that is connected to Vnet/IP is 100 Mbps.

- V net router
  A V net router is a device dedicated for connecting a Vnet/IP domain with a V net domain. It performs the frame conversion and filtering between Vnet/IP and V net. The V net router is a station of CENTUM system.
- Wide Area Communication Router (WAC router)
  The wide area communication router is a hardware device dedicated for the communications between Vnet/IP domains distributed in remote areas through a wide area network. The wide area communication router is a device of CENTUM systems.
- HIS
  HIS (Human Interface Station) is an operation and monitoring station of CENTUM. The HIS is used for operation and monitoring of SCS. The CENTUM system builders are required for engineering and maintenance for the HIS and V net routers. The system builders can be installed on the HIS.

TIP

SENG and HIS set up in the virtual machine on the virtualization platform are referred to as a virtual Vnet/IP station. In order to connect the virtual Vnet/IP station to the Vnet/IP network, a software license for the Vnet/IP interface package is required.

SEE ALSO

For more information about the procedures and precautions when adding a Vnet/IP station, refer to:

"■ Procedures and precautions for adding a Vnet/IP station" on page I5-1

● Vnet/IP domain

A Vnet/IP domain consists of two independent subnets of bus 1 and bus 2. Each domain can have a maximum of 64 Vnet/IP stations (SENG, SCS, etc.).

If a safety system is integrated with a CENTUM system, the integrated system can have a maximum of 16 Vnet/IP and V net domains.

SEE ALSO

For more information about the procedures and precautions when adding a Vnet/IP domain, refer to:

"■ Procedures and precautions for adding a Vnet/IP domain" on page I5-2

● Layer 2 switch

Vnet/IP stations and general-purpose Ethernet communication devices in a domain are connected to Vnet/IP buses through the Layer 2 switches (L2SW). At least one L2SW is required for bus 1 and bus 2 respectively.

● Layer 3 switch

A layer 3 switch (L3SW) is used to connect between Vnet/IP domains on each bus.

A1.2 Device Connections in a Vnet/IP Domain

The devices in the Vnet/IP domain are connected in a star topology by using a 1-Gbps layer 2 switch as the hub. The connections among the layer 2 switches should be in a star topology or ring topology. A ring topology can be used with a CENTUM integration configuration only. It cannot be used with a configuration consisting of a ProSafe-RS system only, or a CI Server integration configuration.

Because the redundant Vnet/IP buses are separated as independent subnets of each bus, each bus should have its own layer 2 switch as the hub.

IMPORTANT

Multiple stations are connected to Layer 2 switches. It is strongly recommended to provide an uninterruptible power supply (UPS) for Layer 2 switches so that they will not stop due to power failure.

The following describes the impact when the Layer 2 switch power supply becomes faulty:

- A communication error will occur if Layer 2 switches for the buses stop due to power failure.
- For dual-redundant SCS, if the Layer 2 switches for both buses stop, the control will be switched to the standby CPU in rare cases, causing the dual-redundant SCS to operate in non-redundant mode.
- If a Layer 2 switch is restarted after momentary power failure, it takes several tens of seconds for the communications between stations to recover.

Specification when connecting devices in a Vnet/IP domain

The specification when connecting devices in a Vnet/IP domain is as follows:

- Number of Vnet/IP stations connected (Vnet/IP stations including V net routers) : Max. 64 Stations
- Distance between Vnet/IP stations : Max. 40 km
- Distance between Layer 2 switch and station : Max. 100 m (when UTP cable is used)
- Connection distance between Layer 2 switches: : Max. 5 km (when optical fiber cable is used)
- Levels of Layer 2 switches: : Max. 7 levels

TIP

- For the redundant stations such as the SCS and Vnet router, the respective CPU module and the Layer 2 switch at the control side and the standby side are connected by a UTP cable. The number of connected Vnet/IP stations is counted as one unit.

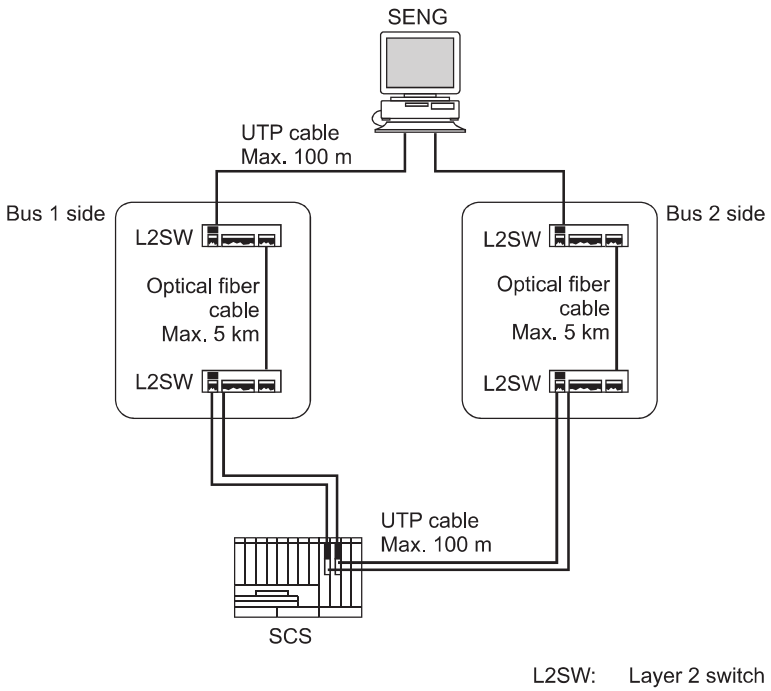


Figure A1.2-1 Example of connections in a Vnet/IP domain

IMPORTANT

When connecting layer 2 switches with a star topology, do not connect in such a way that multiple communication paths exist between any two stations. Otherwise, normal communication is not performed.

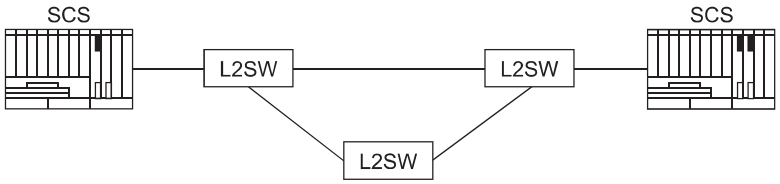


Figure A1.2-2 Example of an incorrect connection

Communication between SENG and SCS

The engineering and maintenance of SCS are performed via Vnet/IP from SENG.

You can perform safety communication between SENG and the SCS of Vnet/IP domains.

The communicable network range is the same as the range in which Inter-SCS safety communication can be performed.

You must connect one or more SENGs to the Vnet/IP network that allows communications with the SCS.

Communication between HIS/FCS and SCS

It is possible to communicate with an SCS in a V net domain or a Vnet/IP domain from an HIS/FCS. The communicable network range is the same as for executing Inter-SCS safety communication.

This communication has no impact on safety functions executed in SCS.

A1.3 Connection between Vnet/IP domains

1-Gbps layer 3 switches are used for connections among the Vnet/IP domains. For a redundantly configured Vnet/IP network, each bus should have a layer 3 switch for the connection of the domains. By using a leased line as the transmission path, the domains can be connected through the wide area networks.

However, connection between Vnet/IP domains is not supported in a ProSafe-RS only system.

IMPORTANT

It is strongly recommended to provide an uninterruptible power supply (UPS) to protect Layer 3 switches so that the Layer 3 switches do not stop upon power failure.

TIP

Wide area communication routers can also be used to connect Vnet/IP domains through a wide area network.

Specifications when connecting Vnet/IP domains

The specification of connection between Vnet/IP domains is as follows:

- Multi-level connection of Vnet/IP domains: Max. 15 levels (16 Layers) of Layer 3 Switches
- Transmission delay between any domains: Less than 80 ms

IMPORTANT

Do not connect in such a way that multiple communication paths exist between any two domains. Otherwise, normal communication is not performed. However, with a CENTUM integration configuration, it is possible to configure the connections among the layer 3 switches connecting adjacent domains in a ring topology.

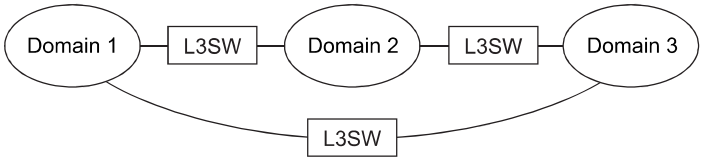


Figure A1.3-1 Example of incorrect connection

Connection between Vnet/IP domains

There are three types of connections between Vnet/IP domains: bi-directional, hierarchical and bridge connections. It is possible to configure a network coexisting these three types of connections. Set the connection types in Domain Properties for each domain using CENTUM engineering builders. The connection type may be selected in accordance with the upper and lower relationships that should be set between connected domains. Decide on the connection type after investigating whether or not message reception, SCS TCP communication or time synchronization is required between connected domains.

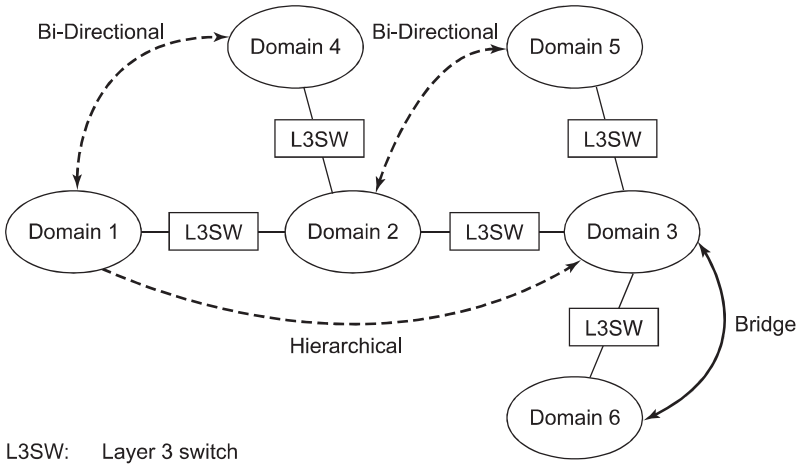


Figure A1.3-2 Domain connection types in Vnet/IP

Setting of TCP/IP communication relay processing

When the system consists of multiple Vnet/IP domains, you must configure the [FCS TCP] setting, which is a domain property setting of a CENTUM system builder. Setting it to ON allows TCP/IP broadcast frames to be relayed in both directions. This function enables the TCP/IP communication between SENG and SCS to be performed across domains.

Bi-directional connection

This connection type does not differentiate the upper and lower relationships between Vnet/IP domains. This type of connection can be established by setting the domain to receive HIS messages, FCS messages and FCS TCP communication frames from other domains. Moreover, when the domain is set to receive FCS messages, it can also receive SCS messages (such as system alarm messages). If the domain is set to receive FCS TCP frames, it can also receive the SCS TCP communication frames. By the default settings on the Domain Properties dialog box, the domain is set to receive all the transmissions.

Hierarchical connection

This connection type differentiates the upper and lower relationships between Vnet/IP domains. This type of connection can be established by setting a lower domain not to receive HIS messages, FCS messages and FCS TCP communication frames from upper domains; but all the stations in the upper domains can receive HIS messages, FCS messages, and FCS TCP communication frames from the lower domain. Moreover, when the domain is set to receive FCS messages, it can also receive SCS messages (such as system alarm messages). If the domain is set to receive FCS TCP frames, it can also receive the SCS TCP communication frames.

Bridge connection

This connection configuration emphasizes the independence among the Vnet/IP domains. In this configuration, the domain properties are configured such that the domains do not receive messages from each other. If time synchronization among the domains is not required, 0 is set in the time group.

IMPORTANT

- If the SCS exists in a Vnet/IP domains that are different from SENG, you need to configure such that the FCS TCP communication is receivable in both domains in order to engineer and maintain the SCS by using SENG.
- When performing inter-SCS safety communication between different Vnet/IP domains, you need to configure such that the FCS TCP communication is receivable in both domains.
- If an SCS that performs inter-SCS safety communication exists in the Vnet domain, you need to configure such that the FCS TCP communication is receivable in both domains. In this case, you need to configure the Vnet router, bus converter (BCV), and communication gateway (CGW) in such a way that the FCS TCP communication is receivable.

TIP

- Even if you select any of these communication configurations, you can access the SCS function block and variables from the CENTUM station across domains by using the tag name.
- You can also set the domain properties so that the domain receives only one type among HIS messages, FCS messages, and FCS TCP communication frames.

System expansion with WAC routers

WAC routers can be used to expand the system by connecting two or more Vnet/IP domains in remote sites using a wide-area network.

You can engineer WAC router by using the System Builders of CENTUM VP. You cannot engineer WAC routers by using the SENG.

Therefore, if you plan to add WAC routers to the system that consists of only SENG and SCS, and connect the system to a wide-area network, the System Builders of CENTUM VP are required.

Moreover, when connecting SCS with wide-area network through WAC routers, install an SENG in each Vnet/IP domain that are connected by WAC routers. Engineering operations such as offline download to SCS must be performed from the SENG that is connected to each Vnet/IP domain. Similarly, install an AD server for each Vnet/IP domain.

The following figure shows an example of system expansion using WAC routers.

The illustrated SENG includes AD Organizer.

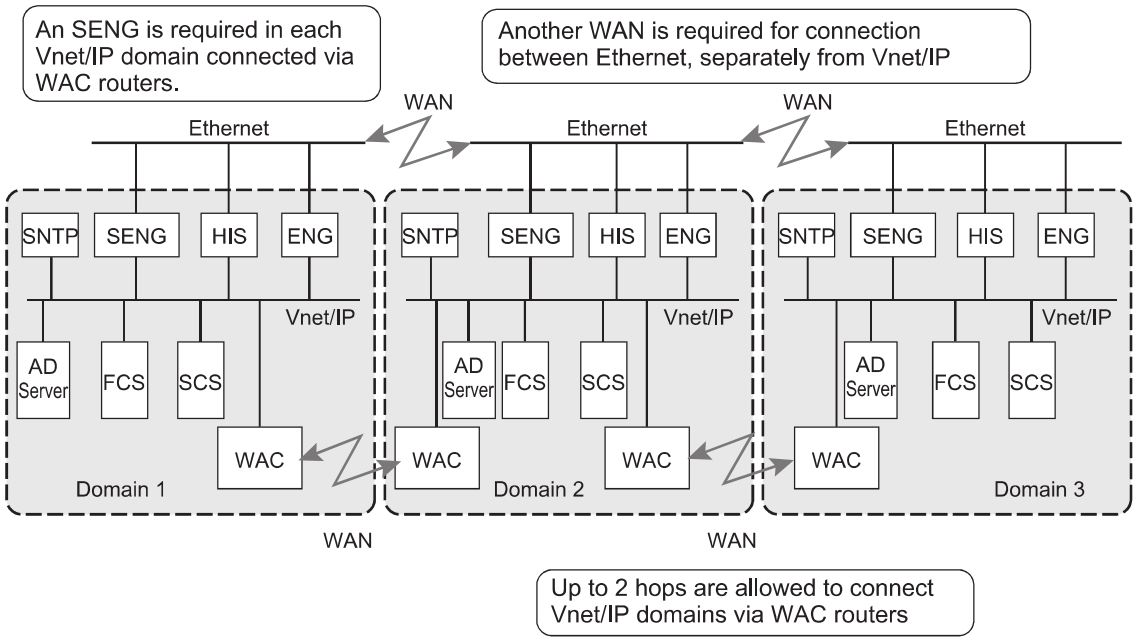


Figure A1.3-3 Example of system expansion with WAC routers

SEE ALSO

For more information about how to configure the WAC router with CENTUM VP R6, refer to:

8, "Wide Area Communication Router" in Communication Devices Reference (IM 33J20B10-01EN)

For more information about how to configure the WAC router with CENTUM VP R5, refer to:

8, "Wide Area Communication Router" in Communication Devices Reference (IM 33K03M10-50E)

Precautions when engineering CENTUM VP systems for using WAC router

A WAC router is engineered on the CENTUM VP side. When connecting the WAC router to ProSafe-RS, be careful of the following points.

Priority control of the Inter-SCS safety communication

A WAC router has the function to give priority to the inter-SCS safety communication, if the communication traffic between Vnet/IP domains exceeds the limit of bandwidth specified in the builder. When performing inter-SCS safety communication through WAC routers, be sure to set WAC routers to enable this function.

Network connection through a wide area network

Connection between Vnet/IP domains can be established through a wide area network for communicating with remote Vnet/IP domains. This type of connection can be established when integrated with CENTUM.

IMPORTANT

If you intend to connect Vnet/IP domains through a wide area network without using wide area communication routers, the following conditions have to be met.

- The transmission delay between any two Vnet/IP domains must be less than 80 ms.
- If inter-SCS safety communications are performed between domains connected through a wide area network, the recommended bandwidth of the wide area network is 100 Mbps or faster.

A2. ProSafe-RS security

ProSafe-RS has the following security functions to prevent access to the system by unauthorized users and devices, and unintended changes caused by operation mistakes made by users.

- Security for the project database
  You can configure the SENG function so that the user is required to enter a password when changing the project data with SCS Manager. (Recommended)
- Security for access to SCS
  You can limit access to SCS from the outside based on the SCS security level. The user is required to enter a password when changing the SCS security level. (Mandatory)
- Security for the SCS Maintenance Support Tool
  On SENG, you can limit writing to SCS with the SCS Maintenance Support Tool by setting a password. (Recommended)
- Access control and operation history management
  Access control and operation history management can be performed on projects that are saved in the AD Server. You can also use the Access control and operation history management package.
- Countermeasures against threats to IT security
  ProSafe-RS security threats include attacks via the network, direct attacks by executing actions on an SENG, and analysis of important data carried out by stealing an SENG. The security features are designed to take measures against these types of security breaches.

This section provides an overview of the ProSafe-RS security function, and the main procedures for setting passwords and implementing security relating to unauthorized access and protection against unintended operations.

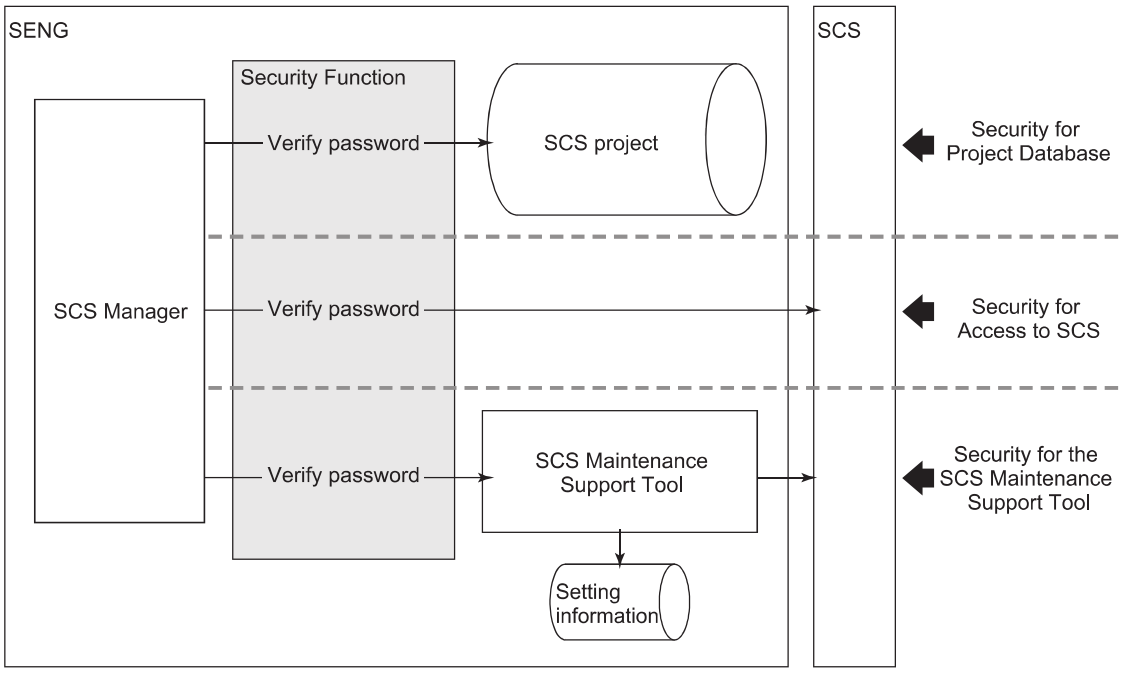


Figure A2-1 Password-based security functions

A2.1 Overview of ProSafe-RS security

The figure below illustrates the security management of SCS and SENG in ProSafe-RS.

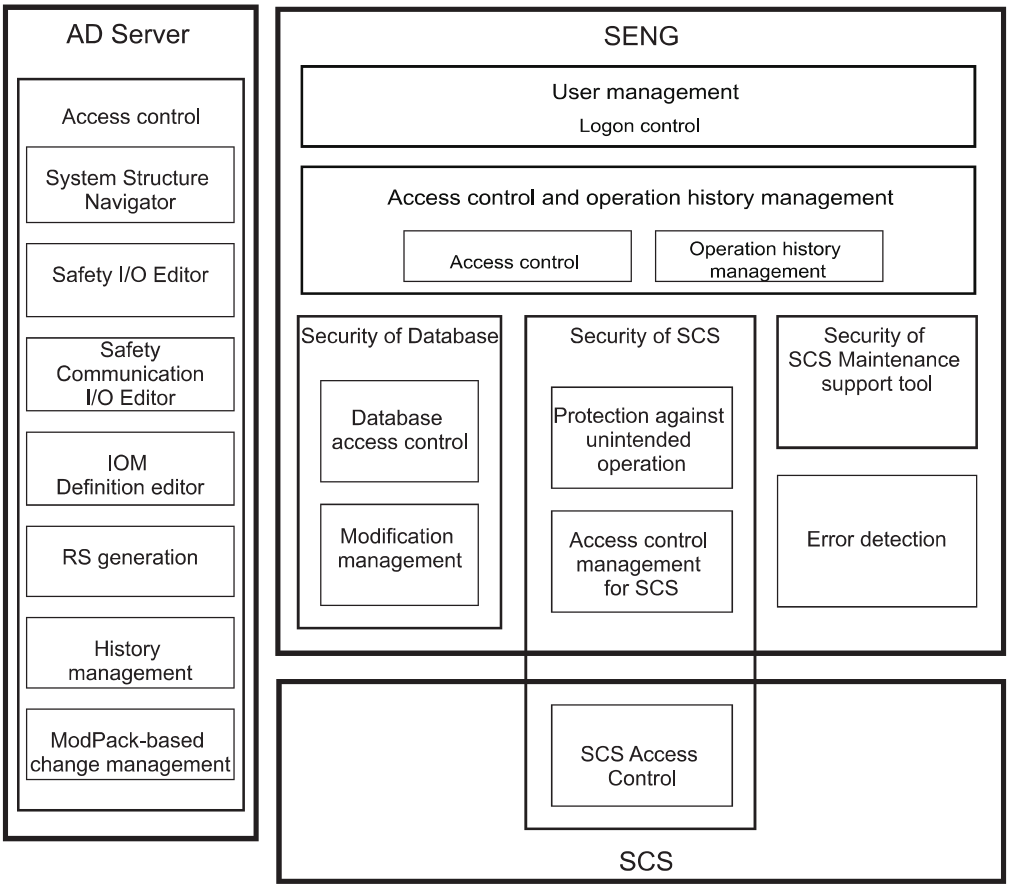


Figure A2.1-1 Overview of security management

IT security

This section describes the requirements for IT security.

For SENG, Windows OS is used as a platform. Therefore, it is necessary to prevent, detect, and recover from computer viruses and attacks from the external through the network. For example, there are countermeasure such as network access control using firewall and system backup.

In the CENTUM Integration Structure, it is necessary to consider comprehensive IT security including ProSafe-RS system and CENTUM system.

You can harden the security of the PC designated as a SENG terminal to enhance the ProSafe-RS IT security (PC hardening). This section describes the details regarding PC hardening and the setting guidelines.

TIP

When integrating ProSafe-RS with CENTUM VP, configure the security settings during installation of ProSafe-RS and installation of CENTUM VP, respectively.

When integrating ProSafe-RS with CS 3000, select Legacy model in IT security tool.

Configure the IT security of the computer that has iDefine installed by referring to iDefine Security Manual (PR03076-MAN-981_01).

If your security model is a legacy model, anyone will be able to start iDefine Test Manager.

If your security model is a standard or strengthened model, any user that belongs to the PSF_ENGINEER or PSF_ENGINEER_LCL group will be able to start iDefine Test Manager.

SEE ALSO

For more information about security configurable on the PC, refer to:

2., “Security Models” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

An example of registering a user to the user account

IT security enhancement for a PC can protect the ProSafe-RS system from the illegal access by any user other than the user of ProSafe-RS user groups. For protecting the ProSafe-RS system from the accidental mistaken accesses by the users of ProSafe-RS groups, the ProSafe-RS Security features should be used. By combining IT security enhancement for a PC and ProSafe-RS Security, you can fortify security of ProSafe-RS.

The typical examples of registering a ProSafe-RS user to the user groups are shown as follows:

(A) ProSafe-RS Engineer (Integrated with CENTUM VP)

ProSafe-RS Engineer user should be assigned to both PSF_ENGINEER group of ProSafe-RS and CTM_ENGINEER group of CENTUM VP.

(B) ProSafe-RS Engineer (Not Integrated with CENTUM VP)

ProSafe-RS Engineer user should be assigned only to the PSF_ENGINEER group.

(C) Maintenance and service persons

The user who requires the role for upgrading SENG software to newer versions, maintaining or changing the hardware components such as I/O modules should be assigned only to the PSF_MAINTENANCE group.

(D) Network and System Administrator (User who is responsible for network maintenance)

This user is considered as the administrative user of Windows environment in SENG. This user needs to be assigned only to the PSF_MAINTENANCE group.

(E) User account for emergency attention (For domain or parallel management in standard model)

When ProSafe-RS system is running in an Windows domain environment, if the domain controller encounters an abnormality, no one can logon to the SENG with the domain account. You need to prepare the user accounts who are assigned to the PSF_MAINTENANCE_LCL group for an emergency attention. If the domain controller encounters an abnormality, user can logon to the SENG with this user account, then maintain and operate ProSafe-RS.

Though the users in the above groups are all granted with the Write permission to all the Project folders, in the cases of (C) and (D), the Write permission is not required. An engineer should define a password by using the security feature of the project database and keep the password as secret to the users whom you do not grant the Write permission so as to protect the project database. Moreover, ProSafe-RS provides security features for accessing the SCS and for Maintenance Support Tool. These security features can be utilized in accordance with the role of the users so as to protect the database and SCS from the accidental operation mistakes.

Database security management

The database has the following security functions.

Access control of the SCS project database

It is possible to set a password for the database used in an SCS project; so that only users who know the password are allowed to make changes to the database. It is also possible to set whether or not to allow users who do not know the password to refer to the database.

Security for AD projects

The following security functions are available for AD projects:

- Management of users who are permitted to access AD projects
- Access control of AD project data

Modification management

This function manages the changes made to SCS projects. It has the following functions:

- Backup
  SCS projects are registered and managed in AD Server.
- Version management
  This function manages the history of changes made to SCS projects.
- Master database management
  SENG always maintains the backup SCS project that keeps the same SCS database with the one running on the SCS.
- Saving modification files
  When you use the Access Control and Operation History Management Package, the changes made to the project database downloaded to the SCS are saved.

Security management of SCS

The SCS has the following security functions.

SEE ALSO For more information about security of SCS, refer to:

B3., “Security of SCS” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

Prevention of SCS operation mistakes made by users

When a user attempts to perform the following operations on the SCS, the user is prompted to confirm the execution of the operation in order to prevent operational mistakes.

- Offline download
- Online change download
- Master database offline download
- IOM download
- I/O lock
- SCS security level change

Access control to SCS

- Access control based on the security level

Access from outside to SCS is controlled by SCS security levels. Password must be set for changing the SCS security levels (to Level 1 or Level 0). The SCS security level can only be operated using the SCS security level operation function, by users who know the password.

- Access control for each user
  When the Access Control and Operation History Management Package is applied, you can control operations on SCS for each user.

Security management of SCS Maintenance Support Tool

In SCS Maintenance Support Tool, write access to SCS is controlled by setting a password. If the Access Control and Operation History Management Package is used, operations of the SCS Maintenance Support Tool can be controlled for each user.

SEE ALSO For more information about how to set a password for SCS Maintenance Support Tool, refer to:

"■ How to enter SCS Maintenance Support tool password" on page A2-10

SCS Status Overview window, Diagnostic Information window, Setup Tool

The SCS Status Overview window, Diagnostic Information window and Setup Tool are protected by passwords. Each of these functions is launched as read-only unless the correct password is specified.

In the case of the SCS Status Overview window, the password is checked when calling this window from SCS Manager. The Diagnostic Information window and Setup Tool inherit the password of the SCS Status Overview window when they are launched.

When the Access Control and Operation History Management Package is applied, enter the name and password of the engineer.

Message Cache Tool

Message Cache Tool is protected by a password. It is launched as read-only unless the correct password is specified.

SOE Viewer

No password is set up for SOE Viewer because no writing operations to an SCS are performed on SOE Viewer.

Forced I/O Viewer and Forced I/O Viewer Setup Tool

Forced I/O Viewer and Forced I/O Viewer Setup Tool do not perform password authentication at startup.

Access control of AD server

You can control access to individual files and functions of an AD project for each user. You can also set access rights to the files and folders in AD Server according to the role of the user.

System Structure Navigator

You can set the rights to register, unregister, back up, and restore RS projects, edit RS project comments, and delete SCS.

Safety I/O Editor

You can set the rights to create and delete safety I/O lists and assign safety I/O.

- **Safety Communication I/O Editor**

  You can set the rights to create and delete safety communication I/O lists and assign safety communication I/O.

- **IOM Definition Editor**

  You can set the rights to create and delete nodes and I/O modules.

- **RS generation**

  You can set the rights to run RS generation.

- **History management**

  You can set the rights to set and delete labels.

- **ModPack change management**

  You can set the rights to perform operations for each ModPack operation category.

A2.2 Security for project database

This section describes security for project databases.

Setting a password for project databases

You can assign a password to a database to prevent unauthorized users from making changes to the database in SCS projects. Users without entering the password can be given permission for read only operation.

Passwords can be specified for the following.

- For each SCS Project
- For each POU

The reading and writing right for the whole project and the access right for each POU can be controlled using the security function of the SCS project and the security function of each POU.

Set a different password for each SCS Project.

If higher level of security is required, set a password for each important POUs.

You need to set different passwords for each SCS project. These passwords should be different from the one for the SCS security level.

Database files in RS projects should not be changed from tools other than the ProSafe-RS software.

A2.3 Security of SCS Maintenance Support tool

SCS Maintenance Support Tool has a security by setting a password to be entered when starting related windows. A password is set for each SENG.

This section describes how to set passwords for the SCS Maintenance Support Tool.

The password described in this section is not applicable if the Access Control and Operation History Management Package is used. Instead, the user enters the password that is set for each user in the Access Control and Operation History Management Package when starting the SCS Maintenance Support Tool.

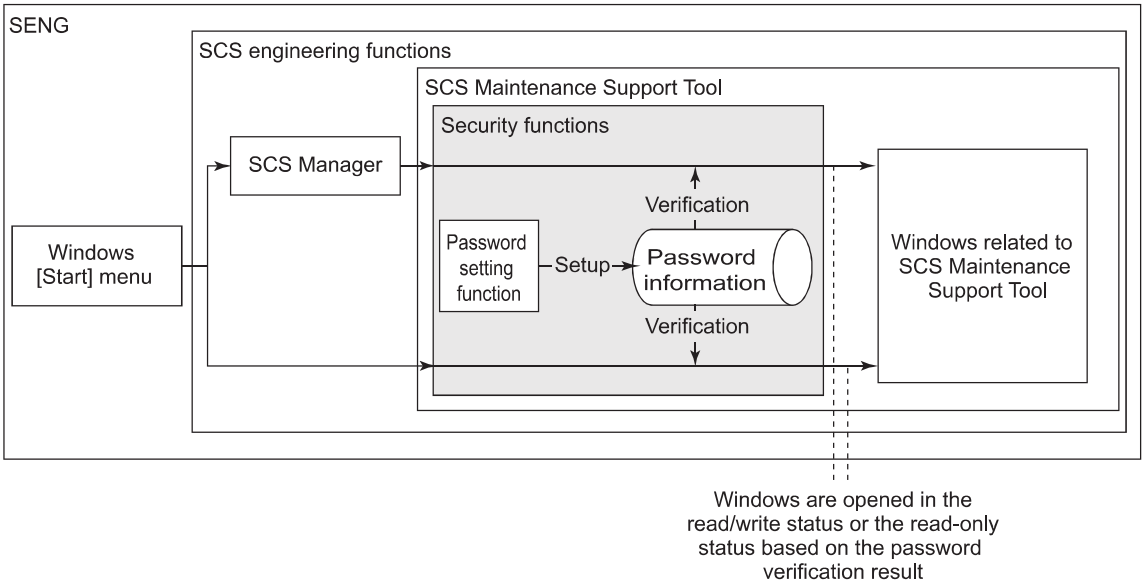


Figure A2.3-1 Security functions of Maintenance Support tool

TIP

No security is set in order to use SOE Viewer as it only displays information.

Setting a password for the SCS Maintenance Support Tool

The SCS Maintenance Support Tool requires a password entry every time you start a window to ensure the security of the SCS access. Password needs to be set for each SENG.

Each tool in the SCS Maintenance Support Tool can be operated for security by entering a password at the start of each tool. When the password entry is cancelled, the tools' operations are disabled for security and the window is in the read-only mode.

The following table shows whether tools can be operated or not when the password is entered and when password entry is cancelled.

Table A2.3-1 Operation of SCS Maintenance Support tool

Tool	Operations provided security	Inputting a password	Without inputting a password
SCS State Management Window	IOM Download	Enabling operation	Read Only
	Output Enable Operation	Enabling operation	Read Only
	Output Module Start Operation	Enabling operation	Read Only
	Setting Time	Enabling operation	Read Only

Continues on the next page

Table A2.3-1 Operation of SCS Maintenance Support tool (Table continued)

Tool	Operations provided security	Inputting a password	Without inputting a password
Diagnostic Information Window	Confirmation and Deletion of Diagnostic information	Enabling operation	Read Only
Setup Tool	Setting and change of display font, color and operating methods for confirming or deleting messages	Enabling operation	Read Only
SOE Viewer	Display of events of SCS and generation of report	Enabling operation	Enabling operation
Message Cache Tool	Setting of message collection, initialization of TRIP information in SCS and storage and deletion of cache data.	Enabling operation	Read Only

How to set and change a password for SCS Maintenance Support tool

The Change Maintenance Support Password dialog box is used to specify or change the password that the user must enter when starting the SCS Maintenance Support Tool.
To use SCS Maintenance Support Tool, make sure to set the password first.

TIP

No password is set automatically after installing SENG. Make sure to set a password at this stage.

1. Open the window related to SCS Maintenance Support Tool from SCS Manager or [Start] menu of Windows.
   When the window requiring a password is opened, the Input Maintenance Support Password dialog box appears.

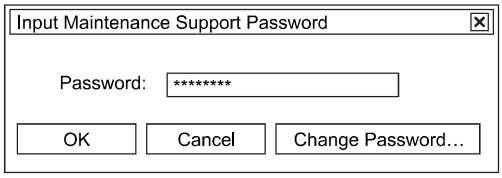


Figure A2.3-2 Input Maintenance Support Password dialog box

2. Click the [Change Password] button.
   The Change Maintenance Support Password dialog box appears.

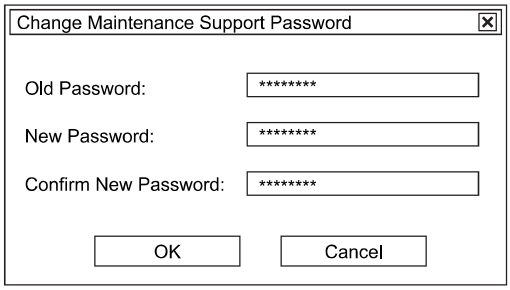


Figure A2.3-3 Change Maintenance Support Password dialog box

3. Enter the current password in the [Old Password:] field. Enter a new password in the [New Password:] field, and once again in the [Confirm New Password:] field.
   The passwords you have entered appear as a series of asterisks (*).

4. Click [OK].
   The password is set.

Specification for passwords

- A password is a maximum 16 of single-byte alphanumeric characters and following symbols including a space character. The password is case-sensitive.
  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~
- Set a password for each SENG-installed PC.
- There is no password when SENG is installed for the first time.
- Set a password when starting the SCS Maintenance Support Tool for the first time.

How to enter SCS Maintenance Support tool password

To start SCS Maintenance Support Tool, the correct password must be entered.
Once you enter the correct password, you are allowed to perform writing and customization operations using SCS Maintenance Support Tool.

IMPORTANT

If you fail to enter the correct password, SCS Maintenance Support Tool is started in the read-only status.

1. Open the window related to SCS Maintenance Support Tool from SCS Manager or [Start] menu of Windows.
   When the window requiring a password is opened, the Input Maintenance Support Password dialog box appears.

   If the current window is called from another window of SCS Maintenance Support Tool, the Input Maintenance Support Password dialog box does not appear, because the security is inherited.

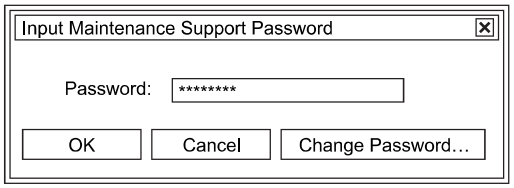


Figure A2.3-4 Input Maintenance Support Password dialog box

2. Enter a password in [Password:] text box.
   All characters you enter are displayed as asterisks (*).
3. Click the [OK] button.
   If you enter the correct password, the window is opened in the read/write status.

   Click the [Cancel] button to start the window related to SCS Maintenance Support Tool in the read-only status.

   Click the [Change Password] button to display the Change Maintenance Support Password dialog box.

A2.4 Access control and history management

When using the Access Control and Operation History Management Package, the functions that can be used by a user are restricted based on the access rights for that user.

SEE ALSO For more information about the Access Control and Operation History Management Package, refer to:

E., “Access Control/Operation History Management functions” in Engineer's Reference Manual (IM 32P04B10-01EN)

User management

The package has a function that enables management of the users who work with SCS Manager and the SCS Maintenance Support Tool. In AD Suite, you can set access rights to the targets of operation for each user role. The user management function is used to register and delete engineers and manage the passwords of engineers. It also keeps records of the operations that were performed by each user.

Access control

The access control function enables you to check engineers who operate the SENG, restrict login or operations on the SENG, and control authorization of engineering operations.

In AD Suite, you can define access rights to files and folders on the AD Server and various functions for all users who perform engineering and maintenance of ProSafe-RS.

Operation history management

This function enables to keep a log of the operations performed by an engineer on the SENG and save the changed project information when a download to an SCS is performed.

In AD Suite, operation history management is available for the following editors and features:

- Safety I/O Editor, Safety Communication I/O Editor, and IOM Definition Editor of AD Organizer
- SCS Manager, builders, and tools including the SCS Maintenance Support Tool
- RS Generation Manager

The change history on all builders and editors is saved on the AD Server and can be viewed in the history window of AD Organizer.

A3. Time synchronization

SCS is capable of synchronizing the time among SCSs, SCS and DI modules to make the event log accurate.

Time synchronization method

SCS for Vnet/IP: Vnet/IP time synchronization is the only option.

Table A3-1 Time synchronization methods

Type	Target SCS	Description
Vnet/IP time synchronization	For Vnet/IP	The system time of SCSs that are connected on Vnet/IP is synchronized with the Vnet/IP network time. If an SNTP server is installed, it is possible to achieve highly accurate time synchronization with the absolute time. The time synchronization status can be checked in the SCS State Management window of the SCS Maintenance Support Tool on SENG, or in the SCS Status Display view on HIS. In Vnet/IP time synchronization, all the stations in one time group that are connected with control bus have the same time data.

Vnet/IP time synchronization method configuration

The following describes the configuration for Vnet/IP time synchronization method.

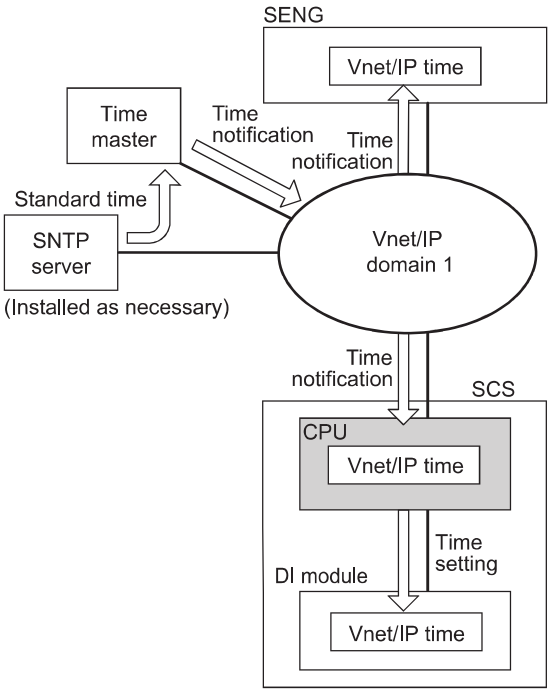


Figure A3-1 Synchronization with Vnet/IP time

- The SCS system time is synchronized with the Vnet/IP network time. When using the synchronization with Vnet/IP time, all stations in the same time group on the Vnet/IP network have the same time information as the clock master. If an SNTP server is installed, the SCS system time is synchronized with the standard time of the SNTP server.
- If the SCS system time is synchronized with the SNTP server time, any time change setting from the SENG or HIS is ignored.
- If the SNTP server is shut down or the SNTP server is not synchronized with the standard time, the SCS system time is automatically synchronized with the clock master of the

same time group (synchronized with internal clock). Accuracy with the standard time drops, but time accuracy between stations is maintained.

Time broadcast to DI modules

The CPU broadcasts the time to DI modules mounted in the station every second.

Selection of Time synchronization method

You can set this method by using the SCS Constants Builder.

For an SCS that is connected to Vnet/IP, the Vnet/IP time synchronization method is automatically selected as the time synchronization method.

Precautions when changing the time in Vnet/IP time synchronization

- If the Vnet/IP time synchronizes with the SNTP server, time setting from SENG or HIS is ignored.
- Changing the Vnet/IP time may cause the SOE generation order to be reversed. Be sure to take the timing to set the time and the difference of the time into consideration when setting the V net time.

IMPORTANT

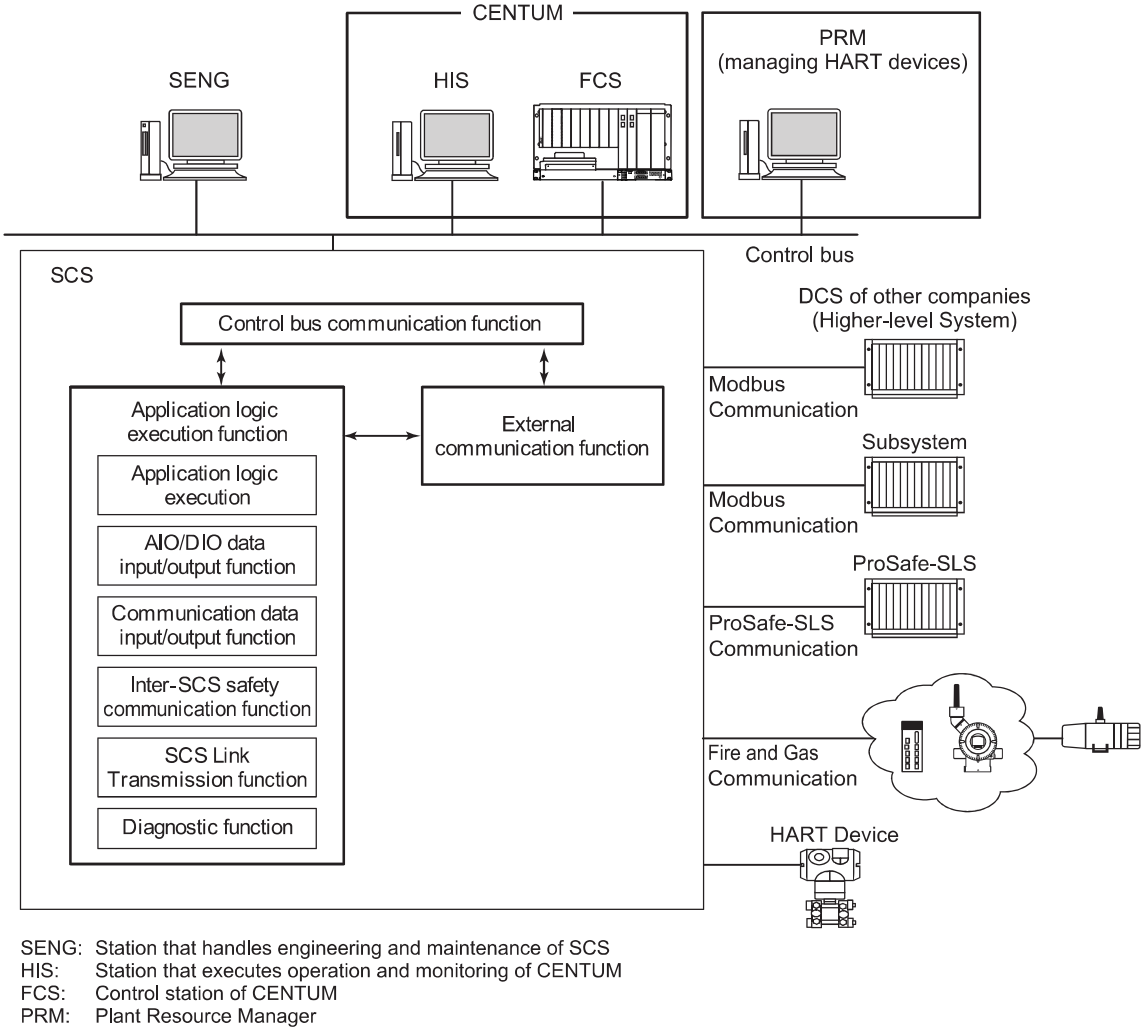
Do not change the Vnet/IP time from more than one SENG or HIS concurrently. It may cause the following errors:

- Self-diagnosis function detects a clock error on the running non-redundant SCS and a system alarm is raised.
- Self-diagnosis function detects a clock error on one of the running redundant SCS and the control right is switched to the standby CPU module.

As a rule, time changes from an HIS/SENG should be made when both buses in the Vnet/IP network are in a normal state. If you change the time from an HIS/SENG during a network failure, there may be stations on which the time does not change immediately, depending on which area of the network has failed and the circumstances of the failure.

A4. Overview of SCS software configuration

SCS is equipped with an application logic execution function for detecting dangerous situations and executing control to prevent or mitigate such situations and an external connection function inclusive of functions for integration with CENTUM which is the production control system of Yokogawa Electric. Note that these functions exchange data with a station on the control bus via a control bus communication function which serves as an interface. In particular, when data is being written into the application logic execution function, the memory inside the SCS is protected with various functions for ensuring safety with such as security levels.



SENG: Station that handles engineering and maintenance of SCS
HIS: Station that executes operation and monitoring of CENTUM
FCS: Control station of CENTUM
PRM: Plant Resource Manager

Figure A4-1 Overview of SCS function configuration

Application logic execution function

This function monitors the safety condition of the plant and makes the process shift to the safety state on detecting any hazards. It mainly performs the following processing.

- Receiving Analog Input (AI)/Digital Input (DI) data from the field
- Execution of user-defined application logic
- Sending Analog Output (AO)/Digital Output (DO) data to the field
- Inter-SCS safety communication

- SCS link transmission
- Communication data I/O (subsystem communication function, safety subsystem communication function)
- Self-diagnosis

Application logic

An SCS executes application logic written in the IEC 61131-3 program language. The application logic is defined by the user using Multi Language Editor and downloaded to the SCS.

An SCS supports the following three languages of IEC 61131-3:

- Function Block Diagram (FBD)
- Ladder Diagram (LD)
- Structured Text (ST)

TIP

The application logic execution function explained here is not simply a name for a function that handles execution of the application logic; rather, it is a generic name for all the functions explained above, including the actual execution of the application logic. In this manual, this term is used in the following explanation as well.

SEE ALSO

For more information about Function Block Diagram (FBD), Ladder Diagram (LD), refer to:

1., “Overview of POU” in POU Reference Manual (IM 32P03B20-01EN)

For more information about Structured Text (ST), refer to:

2., “Structured text” in POU Reference Manual (IM 32P03B20-01EN)

External communication function

This is a function for exchanging information with external systems connected to an SCS and it does not influence the application logic execution function. Main operations are as follows:

- Diagnostic information collection function
- SOER function
- CENTUM Integration Function
- CI Server integration function (SCSP3, SCSP2, SCSP1, and SCSU1)
- Modbus slave communication function
- PRM-supported HART On-demand Communication
- DNP3 communication function (SCSU1 only)

PRM-supported HART on-demand communication

On-demand communication with a HART device is implemented by PRM issuing a HART command, and then receiving a response from the HART device via the SCS. Analog Input/Output modules with HART function serve as communication relays. Specifically, they receive HART communication frames from PRM and send them directly to HART devices, while receiving HART communication frames from HART devices and returning them directly to PRM.

A5. SCS hardware

This section describes the hardware configuration in the SCS, and the important points to determine the configuration.

A5.1 Safety control unit

The following types of safety control units are available:

Table A5.1-1 Types of safety control unit

Model	Name	Safety control unit fan
S2SC70D-S	Duplexed Safety Control Unit (for N-IO/FIO, Rack Mountable Type, Standard Type)	No
S2SC70D-F	Duplexed Safety Control Unit (for N-IO/FIO, Rack Mountable type, Wide Range Temperature Type)	Yes
S2SC70S-S	Safety Control Unit (for N-IO/FIO, Rack Mountable Type, Standard Type)	No
S2SC70S-F	Safety Control Unit (for N-IO/FIO, Rack Mountable Type, Wide Range Temperature Type)	Yes
L1SC70D-S	SIL2, Duplexed Safety Control Unit (for Vnet/IP and FIO, Rack Mountable Type, Standard Type)	No
L1SC70D-F	SIL2, Duplexed Safety Control Unit (for Vnet/IP and FIO, Rack Mountable Type, Wide Range Temperature Type)	Yes
L1SC70S-S	SIL2, Safety Control Unit (for Vnet/IP and FIO, Rack Mountable Type, Standard Type)	No
L1SC70S-F	SIL2, Safety Control Unit (for Vnet/IP and FIO, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC60D-S	Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)	No
SSC60D-F	Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC60S-S	Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)	No
SSC60S-F	Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC57D-S	Duplexed Safety Control Unit (for Vnet/IP-Upstream, Rack Mountable Type, Standard Type)	No
SSC57D-F	Duplexed Safety Control Unit (for Vnet/IP-Upstream, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC57S-S	Safety Control Unit (for Vnet/IP-Upstream, Rack Mountable Type, Standard Type)	No
SSC57S-F	Safety Control Unit (for Vnet/IP-Upstream, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC50D-S	Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)	No
SSC50D-F	Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC50S-S	Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)	No
SSC50S-F	Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC10D-S	Duplexed Safety Control Unit (for Vnet, Rack Mountable Type, Standard Type)	No
SSC10D-F	Duplexed Safety Control Unit (for Vnet, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC10S-S	Safety Control Unit (for Vnet, Rack Mountable Type, Standard Type)	No
SSC10S-F	Safety Control Unit (for Vnet, Rack Mountable Type, Wide Range Temperature Type)	Yes

Combination of the safety control unit and CPU module

The following shows the applicable combinations of safety control unit models and CPU modules.

Table A5.1-2 Applicable combinations of safety control unit models and CPU modules

Safety control unit model	CPU module
S2SC70S/S2SC70D	SCP461 (Style 2), and S2CP471 (*1) (*2)
L1SC70S/L1SC70D	L1CP471
SSC60S/SSC60D	SCP461 (*3), and S2CP471 (*1) (*2)
SSC57S/SSC57D	SCP451
SSC50S/SSC50D	SCP451
SSC10S/SSC10D	SCP401

*1: Supported in the SCS system program of ProSafe-RS R4.05.00 or later.
*2: When the CPU module is made redundant, SCP461 and S2CP471 cannot be mixed.
*3: Style 1 and style 2 can be used. When the CPU module is made redundant, the style of SCP461 can be mixed.

Definition of SCS station types

Define a station type matching the hardware in the SCS Project Properties window called from SCS Manager. If a CPU module not supported by the defined station type is installed on the control side of SCS, a warning is displayed at offline download. The CPU module will not start even if offline download is executed ignoring the warning. If a correct CPU module is installed on the control side but a CPU module different from the definition is installed on the standby side, the CPU module on the standby side will not start.

A5.2 SCS hardware configuration

This section describes the hardware configurations for SCSs that support SIL 3 and SIL 2.

SCS hardware configuration that supports SIL 3

If the safety control unit is S2SC70D or S2SC70S (SCSP3), these three following methods are available to connect the I/O node to the SCSP3:

- N-IO nodes only connection
- Safety node units only connection
- Combined connection of N-IO nodes and safety node units

If the safety control unit is SSC60D or SSC60S (SCSP2), only the safety node unit can be connected.

The following table shows the main hardware names used in SCS that supports SIL 3.

Table A5.2-1 Main hardware names used in SCS that supports SIL 3

Name	Description	Note
SCU	Safety control unit	SSC60D/SSC60S (*1) and S2SC70D/ S2SC70S
SNU	Safety node unit	SNB10D
PSM	Power supply module	SPW481, SPW482, and SPW484. Always redundant.
CPU	Processor module (CPU module)	SCP461 (SSC60 only), SCP461 S2, and S2CP471
SEC401/ SEC402	ESB bus coupler module	Used when SNU and N-IO nodes are used. Installed in slots 7 and 8 of SCU. Always redundant.
SSB401	ESB bus interface module	Always redundant
SNT401/ SNT411	Optical ESB Bus Repeater Master Module	Always redundant
SNT501/ SNT511	Optical ESB Bus Repeater Slave Module	Always redundant
S2EN402/ S2EN404	N-ESB bus coupler module	Used when N-IO node is used. Installed in SCU. Always redundant.
FIO	FIO I/O module	Analog I/O module that supports SIL 3, digital I/O module that supports SIL 3, and communication module
N-IO node	Node for installing N-IO	Configured with node interface unit and N-IO I/O unit.
PSU	Power supply unit for N-IO	S2PW503 and S2PW504. Always redundant.
S2EN501	N-ESB bus module	Used when N-IO node is used. Installed in N-IO node. Always redundant.
N-IO	N-IO I/O module	Universal type I/O module
ESB bus	Bus to connect SCU and SNU	-
N-ESB bus	Bus to connect SCU and N-IO node	-
Optical ESB bus	Bus to connect SCU, SNU, and N-IO node	-

*1: N-IO node is not connectable.

N-IO node only connection

The following configuration are used when connecting only the N-IO nodes to the safety control unit.

When connecting the safety control unit and N-IO nodes by using the N-ESB bus, the S2EN402/S2EN404 is mounted to the safety control unit, and S2EN501 to the N-IO node. When connecting the safety control unit and N-IO node by using the optical ESB bus, the SEC401/SEC402 is mounted to the safety control unit, and S2EN501 to the N-IO node.

The connection between N-IO nodes must be connected with the N-ESB bus or the optical ESB bus.

The following figure shows an example of configuration with N-IO nodes-only connection.

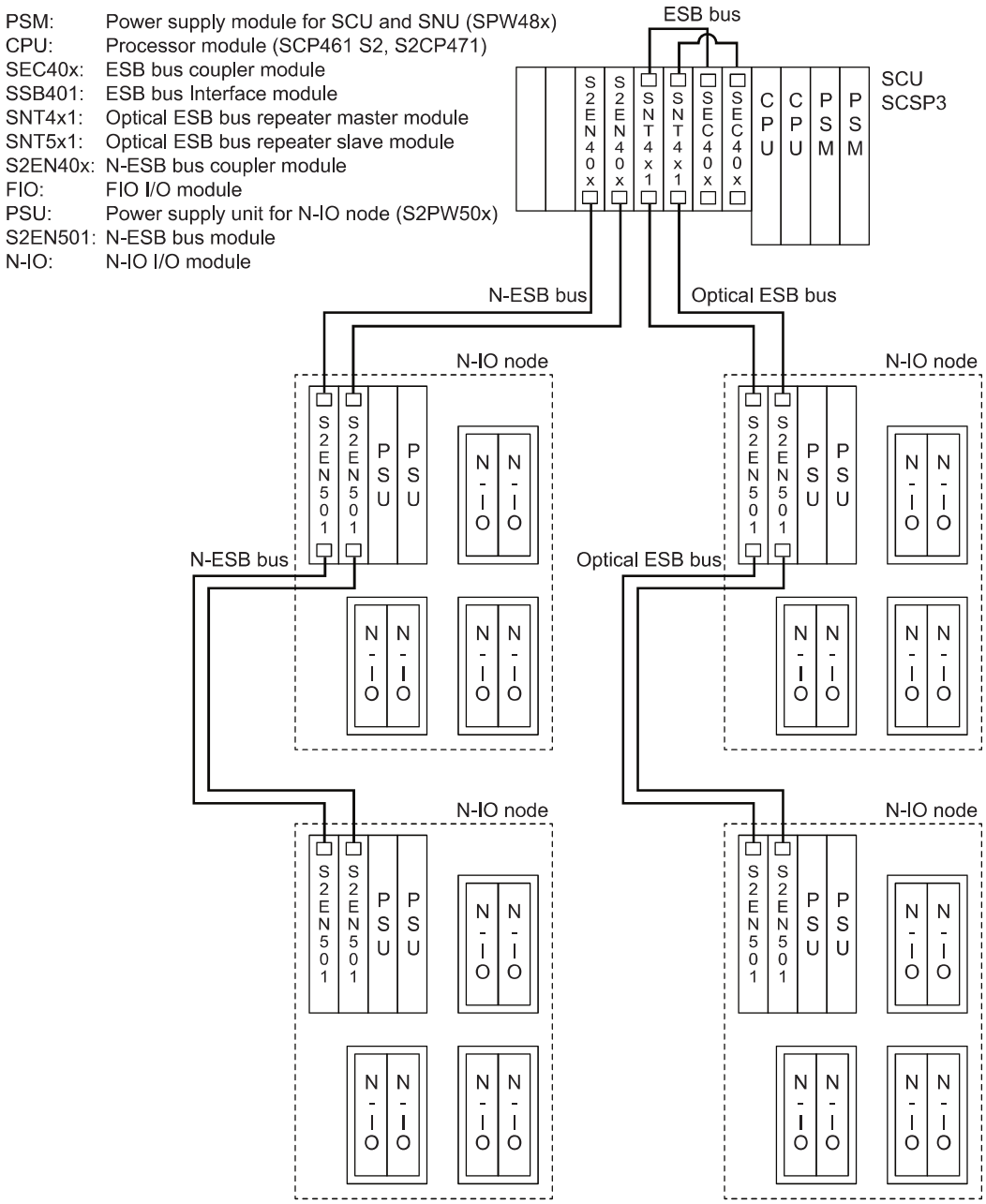


Figure A5.2-1 Configuration example of an N-IO node-only connection

Safety node unit only connection

The following configuration are used when connecting only the safety node units to the safety control unit.

When connecting the safety control unit and safety node unit by using the ESB bus, the SEC401/SEC402 is mounted to the safety control unit, and SSB401 to the safety node unit. When connecting the safety control unit and safety node unit by using the optical ESB bus, the SEC401/SEC402 and SNT401/SNT411 is mounted to the safety control unit, and SNT501/SNT511 and SSB401 to the safety node unit.

The connection between the safety node units must be connected with an ESB bus, or an optical ESB bus through SNT401/SNT411 and SNT501/SNT511.

The following figure shows a configuration example of a safety node units-only connection.

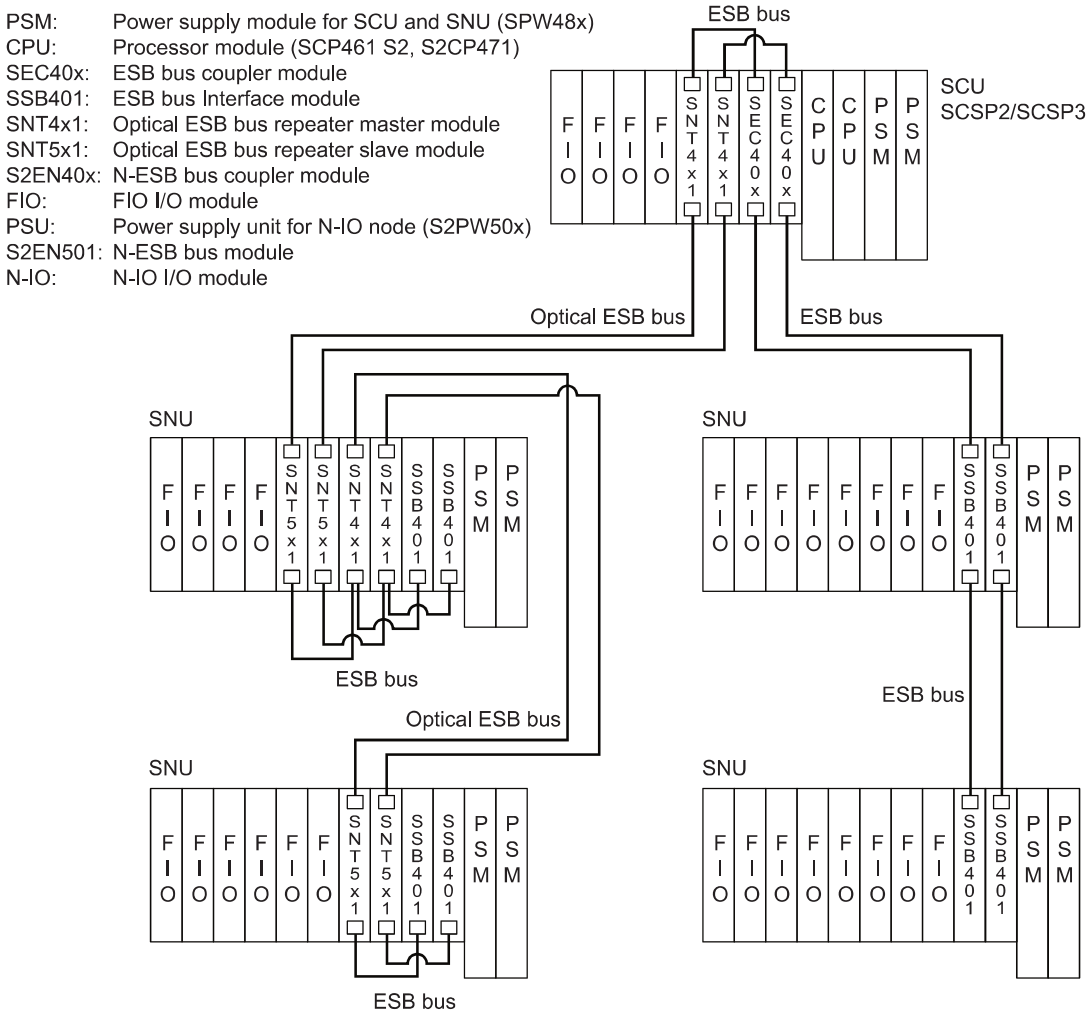


Figure A5.2-2 Configuration example of a safety node units-only connection

Combined connection of N-IO node and safety node unit

N-IO nodes and safety node units can be connected to a single safety control unit. To use both nodes together, you can connect the N-IO node and safety node unit, or separate them.

- Connecting N-IO nodes and safety node units together
  When connecting the safety control unit together with the safety node units and N-IO nodes, connect with the following configuration.

When connecting the safety control unit and N-IO node using the optical ESB bus, the SEC401/SEC402 and SNT401/SNT411 are mounted to the safety control unit, and S2EN501 to the N-IO node.

N-IO node and safety node unit are connected through an optical ESB bus. SNT501/ SNT511 and SSB401 are installed to the safety node unit.

The following figure shows a configuration example of an N-IO node and safety node unit connection.

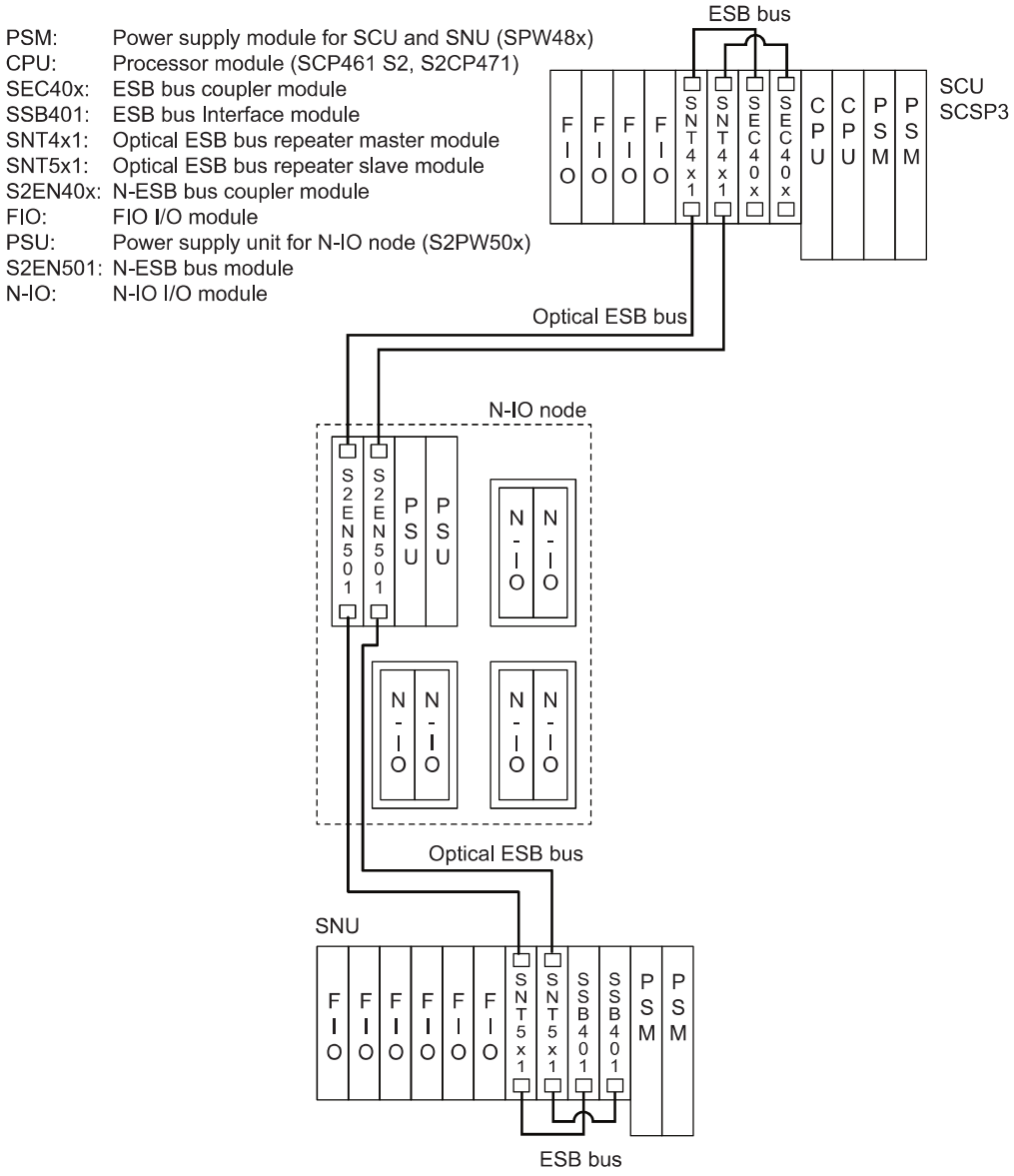


Figure A5.2-3 Configuration example of an N-IO node and safety node unit connection

- Separating N-IO nodes and safety node units, and connecting them together
  When N-IO nodes and safety node units are separated from each other, and they are connected with the safety control unit, the N-IO nodes-only connection and the safety node units-only connection are combined.

  The following figure shows a configuration example when N-IO node and safety node unit are separated and connected together.

PSM: Power supply module for SCU and SNU (SPW48x)
CPU: Processor module (SCP461 S2, S2CP471)
SEC40x: ESB bus coupler module
SSB401: ESB bus Interface module
SNT4x1: Optical ESB bus repeater master module
SNT5x1: Optical ESB bus repeater slave module
S2EN40x: N-ESB bus coupler module
FIO: FIO I/O module
PSU: Power supply unit for N-IO node (S2PW50x)
S2EN501: N-ESB bus module
N-IO: N-IO I/O module

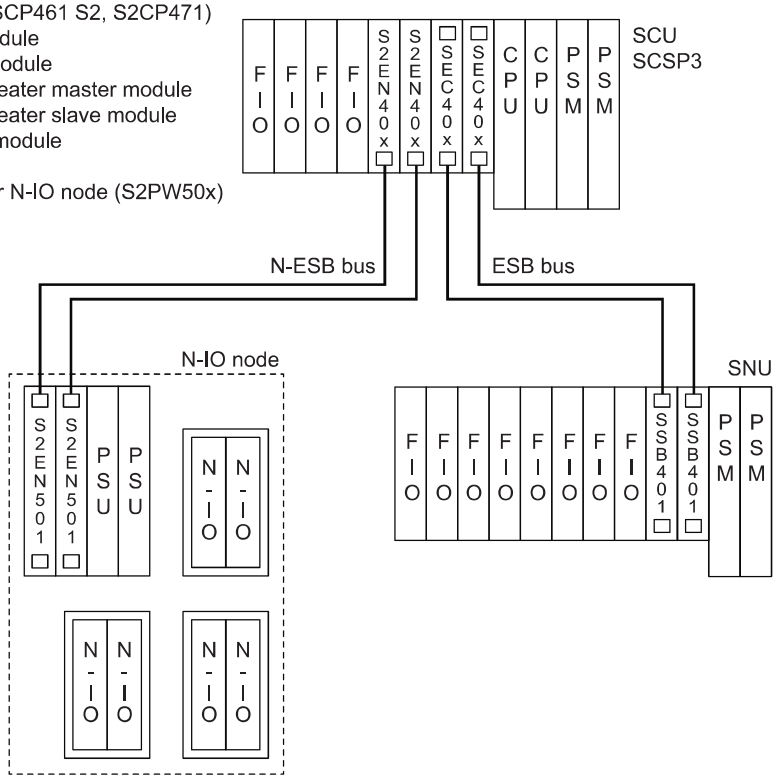


Figure A5.2-4 Configuration example when N-IO node and safety node unit are separated and connected together

SCS hardware configuration that supports SIL 2

If the safety control unit is L1SC70D or L1SC70S (SCSL2), only the safety node unit can be connected.

The following table shows the main hardware names used in SCS that supports SIL 2.

Table A5.2-2 Main hardware names used in SCS that supports SIL 2

Name	Description	Note
SCU	Safety control unit	L1SC70D/L1SC70S
SNU	Safety node unit	L1NB10D
PSM	Power supply module	L1PW481, L1PW482, and L1PW484. Always redundant.
CPU	Processor module (CPU module)	L1CP471
L1EC401/ L1EC402	ESB bus coupler module	Used when SNU is used. Installed in slots 7 and 8 of SCU. Always redundant.
L1SB401	ESB bus interface module	Always redundant
L1NT401/ L1NT411	Optical ESB Bus Repeater Master Module	Always redundant
L1NT501/ L1NT511	Optical ESB Bus Repeater Slave Module	Always redundant
FIO	FIO I/O module	Analog I/O module that supports SIL 2, digital I/O module that supports SIL 2, and communication module
ESB bus	Bus to connect SCU and SNU	-

Continues on the next page

Table A5.2-2 Main hardware names used in SCS that supports SIL 2 (Table continued)

Name	Description	Note
Optical ESB bus	Bus to connect SCU and SNU	-

Safety node unit only connection

The following configuration is used when connecting only the safety node units to the safety control unit.

When connecting the safety control unit and safety node unit by using the ESB bus, the L1EC401/L1EC402 is mounted to the safety control unit, and L1SB401 to the safety node unit. When connecting the safety control unit and safety node unit by using the optical ESB bus, the L1EC401/L1EC402 and L1NT401/L1NT411 are mounted to the safety control unit, and L1NT501/L1NT511 and L1SB401 to the safety node unit.

The connection between the safety node units must be connected with an ESB bus, or an optical ESB bus through L1NT401/L1NT411 and L1NT501/L1NT511.

The following figure shows a configuration example of a safety node units-only connection.

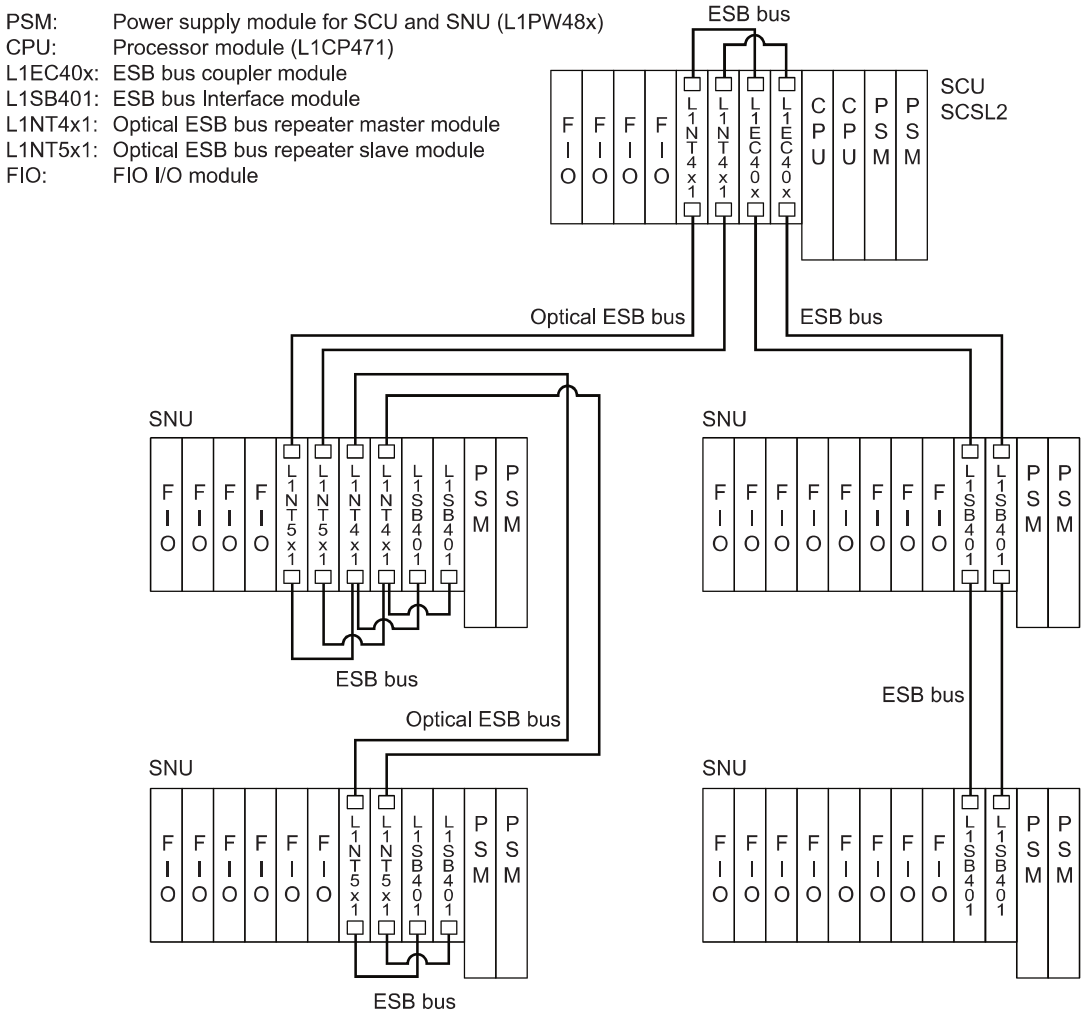


Figure A5.2-5 Configuration example of a safety node units-only connection

A5.3 Restrictions on installation of hardware

There are the following restrictions on the installation of hardware on the SCS.

- To connect a safety node unit in an SCS that supports SIL 3, you need to install SEC401 in slots 7 and 8 of the safety control unit. If you want to connect 10 or more safety node units with SCSP3 or SCSP2, install SEC402 instead. If I/O expansion is not required, you can install I/O modules in slots 7 and 8.
- To connect a safety node unit in an SCS that supports SIL 2, you need to install L1EC401 in slots 7 and 8 of the safety control unit. If you want to connect 10 or more safety node units with SCSL2, install L1EC402 instead. If I/O expansion is not required, you can install I/O modules in slots 7 and 8.
- When installing redundant I/O modules in a safety node unit, you can install the modules in pairs into slots 1 and 2, slots 3 and 4, slots 5 and 6, or slots 7 and 8.
- Up to 8 fire and gas communication modules (S2LP131) can be installed per SCS. S2LP131 can be used for SCSP3.
- For subsystem communication, a maximum of four (up to two pairs in redundant configuration) serial communication modules (ALR111, ALR121) and Ethernet communication modules (ALE111) can be installed per SCS.
- For Modbus slave communication, a total maximum of two modules among serial communication modules (ALR111, ALR121) and Ethernet communication module (ALE111) can be installed.
- In SCSU1, up to two ALE111 modules can be installed for communication as a DNP3 slave.
- A total maximum of eight serial communication modules (ALR111, ALR121) and Ethernet communication modules (ALE111) can be installed per SCS of type SCSU1, and a total maximum of six per SCS of other types of SCS.
- You cannot install the serial communication modules (ALR111, ALR121) and the Ethernet communication module (ALE111) for Modbus slave communication in the safety node unit that is located beyond 5 km by using the optical ESB bus repeater module.

SEE ALSO

For more information about implementation restrictions of the N-IO I/O module, refer to:

ProSafe-RS Outline of I/O Modules (for N-IO) (GS 32P06F10-01EN)

For more information about installation restrictions of the FIO I/O module, refer to:

ProSafe-RS Outline of I/O Modules (for FIO) (GS 32P06K60-01EN)

For more information about implementation restrictions of I/O modules that support SIL 2, refer to:

ProSafe-RS Lite Outline of I/O Modules (GS 32P56K60-01EN)

For more information about operating temperature of the safety control unit, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

For more information about operating temperature of the safety control unit that supports SIL 2, refer to:

ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

I/O module types

The available types of I/O modules include analog I/O module (AIO: Analog Input/Analog Output), digital I/O module (DIO: Digital Input/Digital Output), and a universal type I/O module where the signal category for channels can be changed by software. In addition, communication modules are available for communications with external devices.

TIP If the SCS project was created by SENG of the software release number that does not support the module you want to use, you cannot use that I/O module in the SCS project. To use the I/O module, you must create a new SCS project on the SENG of the software release number that supports the module and perform offline download to the SCS.

Analog I/O modules

Analog input/output modules are used to input/output analog signals that indicate electrical current, voltage, etc. There are analog input/output modules for SCSs that support SIL 3 and those that support SIL 2.

The following table shows the types (models) of analog input/output modules for SCS that supports SIL 3.

Table A5.3-1 Specifications of analog input/output modules for SCS that supports SIL 3

Classification	Type	Description	Number of channels	Redundancy
Analog input	SAI143	4 to 20 mA, module isolation	16	Allowed
	SAV144	1 to 10 V, module isolation	16	Allowed
	SAT145	Thermocouple/mV, isolated channels	16	Allowed
	SAR145	Resistance temperature detector, isolated channels	16	Allowed
Analog output	SAI533	4 to 20 mA, module isolation	8	Allowed

The following table shows the types (models) of analog input/output modules for SCS that supports SIL 2.

Table A5.3-2 Specifications of analog input/output modules for SCS that supports SIL 2

Classification	Type	Description	Number of channels	Redundancy
Analog input	L1AI143	4 to 20 mA, module isolation	16	Allowed
	L1AV144	1 to 10 V, module isolation	16	Allowed
	L1AT145	Thermocouple/mV, isolated channels	16	Allowed
	L1AR145	Resistance temperature detector, isolated channels	16	Allowed
Analog output	L1AI533	4 to 20 mA, module isolation	8	Allowed

- SAI143/L1AI143
  An analog input module for electrical current. Modules whose suffix code is SAI143-H/L1AI143-H support HART communication and are indicated as SAI143H/L1AI143H in the SCS State Management Window on the SENG or the SCS Status Display view on the HIS. SAI143-H can be used with software release number of R1.02.00 or later.
- SAV144/L1AV144
  An analog input module for electrical voltage.
- SAT145/L1AT145
  An analog input module for thermocouple (TC)/mV. SAT145 can be used with software release number of R3.01.00 or later.
- SAR145/L1AR145
  An analog input module for the resistance temperature detector (RTD). SAR145 can be used with software release number of R3.01.00 or later.
- SAI533/L1AI533

An analog output module for electrical current. SAI533 can be used with software release number of R1.02.00 or later. It is indicated as SAI533H/L1AI533H in the SCS State Management Window on the SENG or the SCS Status Display view on the HIS. This module supports HART communication.

Digital I/O modules

Digital input/output modules are used to input/output processes that use discrete on/off signals. There are digital input/output modules for SCSs that support SIL 3 and those that support SIL 2.

The following table shows the types (models) of digital input/output modules for SCS that supports SIL 3.

Table A5.3-3 Specifications of digital input/output modules for SCS that supports SIL 3

Classification	Type	Description	Number of channels	Redundancy
Digital input	SDV144	24 V DC, module isolation	16	Possible
Digital output	SDV521	24 V DC, module isolation	4	Possible
	SDV531	24 V DC, module isolation	8	Possible
	SDV53A	48 V DC, module isolation	8	Possible
	SDV541	24 V DC, module isolation	16	Possible
	SDV526	100 to 120 V AC, module isolation	4	Possible

The following table shows the types (models) of digital input/output modules for SCS that supports SIL 2.

Table A5.3-4 Specifications of digital input/output modules for SCS that supports SIL 2

Classification	Type	Description	Number of channels	Redundancy
Digital input	L1DV144	24 V DC, module isolation	16	Possible
Digital output	L1DV521	24 V DC, module isolation	4	Possible
	L1DV531	24 V DC, module isolation	8	Possible
	L1DV53A	48 V DC, module isolation	8	Possible
	L1DV541	24 V DC, module isolation	16	Possible
	L1DV526	100 to 120 V AC, module isolation	4	Possible

- SDV144/L1DV144
  A digital input module. This module provides SOER (Sequence of Events Recorder) function.
- SDV521/L1DV521
  This module is for 4-channel digital output.
- SDV531/L1DV531
  This module is for 8-channel digital output. There are two types of SDV531: SDV531-S, which is the standard type, and SDV531-L, which supports long distances. L1DV531 has only L1DV531-L which supports long distances.
- SDV53A/L1DV53A
  This module is for 8-channel 48 V DC digital output.
- SDV541/L1DV541
  This module is for 16-channel digital output.

- SDV526/L1DV526
  This module is for 4-channel 100 to 120 V AC digital output.

TIP

- Short circuits between channels cannot be detected in SDV526/L1DV526. In addition, the following faults cannot be detected while the output is OFF:
  - Short circuits in output wiring
  - Output overload (faults in field devices that cause short circuits or overcurrent when the module's output is set to ON)
- Satisfy either of the following conditions when creating an application logic that repeatedly outputs ON and OFF with SDV526/L1DV526:
  - The signal value is maintained for at least 1 s with each ON signal.
  - The signal value is maintained for at least 1 s with each OFF signal.

  These are conditions required in order to detect wiring errors and internal failures and correctly notify diagnosis information. There are no restrictions for cases involving the output of single-shot pulses.

Universal type I/O module

The signal category of the universal type I/O module can be switched by software. The universal type I/O module can only be used with SCSP3.

The following table shows the types (models) of the universal type I/O module.

Table A5.3-5 Universal type I/O module specifications

Model	Name	Description	Number of channels	Redundancy
S2MMM843	Analog digital I/O module	16 channel, module Isolation Analog I/O (AI/AO): 4 to 20 mA, HART compatible Digital I/O (DI/DO): 24V DC You can switch the signal category to AI, AO, DI, or DO for each channel. To use analog output (AO), it is 8 channels for every I/O module. For digital output (DO), a high current output function that combines two or three consecutive channels is supported. 1.3 A, 2.0 A	16	Allowed
S2MDV843	Digital I/O Module	16 channel, module Isolation Digital I/O (DI/DO): 24V DC You can switch the signal category to DI or DO for each channel. For digital output (DO), a high current output function that combines two or three consecutive channels is supported. 1.3 A, 2.0 A	16	Allowed

TIP

Satisfy either of the following conditions when creating an application logic which repeatedly outputs ON and OFF with the DO of S2MMM843 or S2MDV843:

- The signal value is maintained for at least 0.5 s with each ON signal.
- The signal value is maintained for at least 2 s with each OFF signal.

However, there are no restrictions for cases involving the output of single-shot pulses.

Failure detection may not be available in cases when ON/OFF signals are continuously modified in cycles which never satisfy either one of the conditions.

Example of a case where failure detection will be unavailable: An application logic which repeatedly outputs an ON signal for 0.3 s and an OFF signal for 0.3 s

Examples of cases where failure detection will be available:

- An application logic which repeatedly outputs an ON signal for 0.5 s and an OFF signal for 0.5 s
- An application logic which repeatedly outputs an ON signal for 0.3 s and an OFF signal for 2 s

The DO of S2MMM843 and S2MDV843 performs a diagnosis of short circuits and disconnected wiring upon the output of a signal. However, a certain amount of time is required from when the output has changed to when the diagnosis result is refreshed.

- When the signal has changed from OFF to ON, a maximum of 0.5 s is required from when the output has changed to when the diagnosis result is refreshed.
- When the signal has changed from ON to OFF, a maximum of 2 s is required from when the output has changed to when the diagnosis result is refreshed.

When a change of output is repeated in a shorter interval than the time required to refresh the diagnosis results, a state where the diagnosis results are not updated will continue. Refrain from creating such application.

Serial communication modules

Serial communication modules are used to implement Modbus slave communication, where an SCS acting as a Modbus slave communicates with an external device acting as the Modbus master, and are also used to implement subsystem communication, where an SCS communicates with a subsystem. Serial communication modules can be used with SCSs that support both SIL 3 and SIL 2.

- ALR111: Serial communication module (RS-232C)
  It is an interference-free communication module with an RS-232C interface.
- ALR121: Serial communication module (RS-422/RS-485)
  It is an interference-free communication module with an RS-422 or RS-485 interface.

Take note on the following cautions when using the serial communication modules:

- You need to prepare separate modules for Modbus slave communication and subsystem communication.
- When used for Modbus slave communication, serial communication modules cannot have a redundant configuration. If redundancy is required, use two serial communication modules and provide redundancy using a user application.
- Serial communication modules can be configured as redundant modules if used for subsystem communication.
- In a safety control station, the serial communication module for Modbus slave communication cannot be implemented in the safety node unit that is installed at a distance longer than 5 km by using an optical ESB bus repeater module.
- A redundant configuration cannot be used if ALR121 is used for the ProSafe-SLS communication function.

Ethernet communication module

The Ethernet communication module is used to establish the Modbus slave communication that connects the external device of the Modbus master with the SCS of the Modbus slave, and the subsystem communication that connects the SCS with the subsystem. It is also used for the DNP3 communication in SCSU1. Ethernet communication modules can be used with both SCSs that support each of SIL 3 and SIL 2.

- ALE111: Ethernet communication module
  It is an interference-free communication module with a 10BASE-T interface.

Take note on the following cautions when using the Ethernet communication module:

- When used for Modbus slave communication, the Ethernet communication modules cannot have redundant configuration. If redundancy is required, you need to use two Ethernet communication modules and provide redundancy through user application.
- The modules can be configured as redundant modules if used for subsystem communication.
- For DNP3 slave function, the redundant configuration cannot be set by using two modules.
- When the CPU node of SCS is SSC10D or SSC10S, do not define ALE111.
- The Ethernet communication module used for Modbus slave communication or DNP3 communication cannot be installed in the FIO node that is located beyond 5 km by using the optical ESB bus repeater module.

Fire and gas communication module

The fire and gas communication module can be used for fire and gas communication to connect to gas detectors. The fire and gas communication module can only be used with SCSP3.

- S2LP131: Fire and gas communication module
  A communication module with a 100BASE-TX interface.

Take note on the following cautions when using a fire and gas communication module:

- The modules cannot have a redundant configuration.

Installation using devices related to optical ESB bus repeater

In SCS, I/O nodes and N-IO nodes are connected via the ESB bus that is the I/O bus of the SCS. When nodes are to be located at remote places, the ESB bus can be extended by using optical ESB bus repeater modules and fiber-optic cables via the ESB bus coupler module.

Optical ESB bus repeater modules are used by installing them on CPU node, I/O nodes, and nodes for optical ESB bus repeater modules.

Related hardware

There are related hardware devices for SCSs that support SIL 3 and those that support SIL 2.

The following table shows the optical ESB bus repeater modules for SCS that supports SIL 3.

Table A5.3-6 Optical ESB bus repeater modules for SCS that supports SIL 3

Model	Name	Description
SNT401/ SNT411	Optical ESB Bus Repeater Master Module	Master module for extending ESB bus with fiber-optic cable(s). SNT411 supports extending of the long distance.
SNT501/ SNT511	Optical ESB Bus Repeater Slave Module	Slave module for extending ESB bus with fiber-optic cable(s). SNT511 supports extending of the long distance.

The following table shows the optical ESB bus repeater modules for SCS that supports SIL 2.

Table A5.3-7 Optical ESB bus repeater modules for SCS that supports SIL 2

Model	Name	Description
L1NT401/ L1NT411	Optical ESB Bus Repeater Master Module	Master module for extending ESB bus with fiber-optic cable(s). L1NT411 supports extending of the long distance.
L1NT501/ L1NT511	Optical ESB Bus Repeater Slave Module	Slave module for extending ESB bus with fiber-optic cable(s). L1NT511 supports extending of the long distance.

The following table shows the related devices when using optical ESB bus repeater modules for SCS that supports SIL 3.

Table A5.3-8 Related devices when using optical ESB bus repeater modules for SCS that supports SIL 3

Model	Name	Description
SEC402/ SEC401	ESB bus coupler module	Module installed in the CPU node and for communication with the I/O node and N-IO node. SEC402 has two ports for ESB bus. Upper and Lower. SEC401 has one port for ESB bus.
SSB401	ESB bus interface module	Module installed in the I/O node and for communication with the ESB bus coupler module
S2EN501	N-ESB bus module	Module that is installed in the N-IO node. Using this module, N-IO nodes can be connected with fiber-optic cable(s)
SNT10D	Unit for Optical ESB Bus Repeater Module	Node dedicated for mounting optical ESB bus repeater modules. The power supply modules are duplicated.

The following table shows the related devices when using optical ESB bus repeater modules for SCS that supports SIL 2.

Table A5.3-9 Related devices when using optical ESB bus repeater modules for SCS that supports SIL 2

Model	Name	Description
L1EC402/ L1EC401	ESB bus coupler module	Module installed in the CPU node and for communication with the I/O node. L1EC402 has two ports for ESB bus. Upper and Lower. L1EC401 has one port for ESB bus.
L1SB401	ESB bus interface module	Module installed in the I/O node and for communication with the ESB bus coupler module
L1NT10D	Unit for Optical ESB Bus Repeater Module	Node dedicated for mounting optical ESB bus repeater modules. The power supply modules are duplicated.

- When connecting FIO nodes in an SCS that supports SIL 3, use SNT401 and SNT501 or SNT411 and SNT511 in pairs. SNT411 and SNT511 cannot be mounted on SCSV1.
- When connecting FIO nodes in an SCS that supports SIL 2, use L1NT401 and L1NT501 or L1NT411 and L1NT511 in pairs.
- The ESB bus coupler module, ESB bus interface module, N-ESB bus module, and optical ESB bus repeater module must be used in redundant configuration. The fiber-optic cable is also used in redundant configuration. It is recommended that the two cables in a pair be the same length.
- The following table shows the optical attenuation required for the optical ESB bus repeater module when the optical transmission distance is 5 to 50 km. If the conditions are not met, use an attenuator to ensure that the conditions are met.

Table A5.3-10 Optical attenuation required for the optical ESB bus repeater module

Module to be used	Required attenuation
SNT411 and SNT511 of Style S2 and above S2EN501 L1NT411, L1NT511	3 dB or more
SNT411 and SNT511 of Style S1	1 dB or more

SEE ALSO

For more information about the specifications and installation restrictions of hardware used in relation to the optical ESB bus repeater, refer to:

Safety Instrumented System ProSafe-RS System Specifications (for Vnet/IP) (GS 32P01B10-01EN)

For more information about specifications, implementation restrictions, etc., of related hardware for optical ESB bus repeaters that support SIL 2, refer to:

Safety Instrumented System ProSafe-RS Lite System Specifications (GS 32P51B10-01EN)

Node types and installable slots

The following table shows the slot numbers where the optical ESB bus repeater module can be installed for each installation node type.

Table A5.3-11 Optical ESB bus repeater module and installable slots

Node type	Slot number
CPU node	1 to 6
I/O node	1 to 8 (*1)
Unit for Optical ESB Bus Repeater Module	1 to 10

*1: An I/O node is a node for installing an I/O module. Therefore, it is not possible to install only the optical ESB bus repeater modules in the I/O node without installing the I/O module.

The optical ESB bus repeater module has Mounting unit setting switch 1. Change the settings according to the node type that will be installed. The following table shows the required settings for each installation node type.

Table A5.3-12 Switch setting of the optical ESB bus repeater module according to the node type to be installed

Node type	Mounting unit setting switch 1 (*1)	The impact when it was not set definitely
CPU node and I/O node	Is set to 1.	If it is set to 0, an error in one of the power-supply modules of the nodes will be notified as a failure of the one-side optical ESB bus repeater module.
Unit for Optical ESB Bus Repeater Module	Is set to 0.	If it is set to 1, one-sided error of the power-supply modules of the Unit for optical ESB bus repeater module will not be notified.

*1: The default setting of Mounting unit setting switch 1 is 0. This setting status can be checked by the display of the status display lamp (NODE 1) on the front of the module. Only the number 1 is the LED lamp. When the Mounting unit setting switch 1 is set to 1, the number 1 is turned on in green.

Maximum number of nodes that can be connected according to ESB bus coupler module type

The maximum number of I/O nodes that can be connected excluding CPU nodes is shown for each ESB bus coupler module type. For the connection specifications of the SCSP3 node interface unit, refer to the General Specifications.

For SCS that supports SIL 3

- When using SEC402
  SCSP3/SCSP2: 13 I/O nodes

- When using SEC401
  9 I/O nodes

For SCS that supports SIL 2

- When using L1EC402
  13 I/O nodes
- When using L1EC401
  9 I/O nodes

ESB bus extendable distance for each optical ESB bus repeater device

The transmission distance of ESB bus can be extended by using the optical ESB bus repeater device. The following table shows the extendable transmission distance for each device. Refer to the General Specifications for the extendable distance for each N-IO node connection method not mentioned here.

Table A5.3-13 ESB bus extendable distance for each optical ESB bus repeater device

Devices to be used		Extendable distance
ESB bus coupler module (electric signal)	SEC402, L1EC402	Upper: 10 m, Lower: 10 m
	SEC401, L1EC401	10 m
Optical ESB bus repeater module	Combination of SNT401 and SNT501, or combination of L1NT401 and L1NT501	5 km
	Combination of SNT411 and SNT511, or combination of L1NT411 and L1NT511	5 to 50 km
N-ESB bus module (for N-IO)	Between SNT411 and S2EN501 Between S2EN501 and SNT511	5 to 50 km

SEE ALSO For more information about connection specifications of N-IO node, refer to:

Model S2NN30D Node Interface Unit (for N-IO) (GS 32P06F20-01EN)

Maximum extension distance of fiber-optic cable

The total extension distance of the fiber-optic cable between the CPU node and the final node is called "Maximum extension distance of fiber-optic cable." The maximum extension distance of fiber-optic cable is 50 km (however, it is 5 km for SCSV1).

I/O nodes and N-IO nodes can be connected in chain or in star by using the optical ESB bus repeater device. Connection methods can be mixed.

One set of optical ESB bus repeater master module and optical ESB bus repeater slave module is counted as 1 layer, and up to 2 layers can be connected. If N-IO nodes are connected with fiber-optic cable(s), they can be connected up to 16 layers. However, if the system has N-ESB buses or I/O nodes, up to 2 layers can be connected.

The selection of optical ESB bus repeater modules or the distances between nodes can be combined freely as long as it is within the maximum optical fiber cable extension distance. The examples are as follows. Modules in brackets indicate devices for SCS that supports SIL 2.

- It shall be 10 km by connecting the distance between SNT401 and SNT501 (L1NT401 and L1NT501) up to 2 layers with 5 km each.
- It shall be 50 km in total by using SNT401/SNT501 (L1NT401/L1NT501) for the first layer (5 km), and SNT411/SNT511 (L1NT411/L1NT511) for the second layer (45 km).

Wiring examples using optical ESB bus repeater devices

The following figures show wiring examples using optical ESB bus repeater devices, divided by type of node to be connected.

- FIO node only connection example

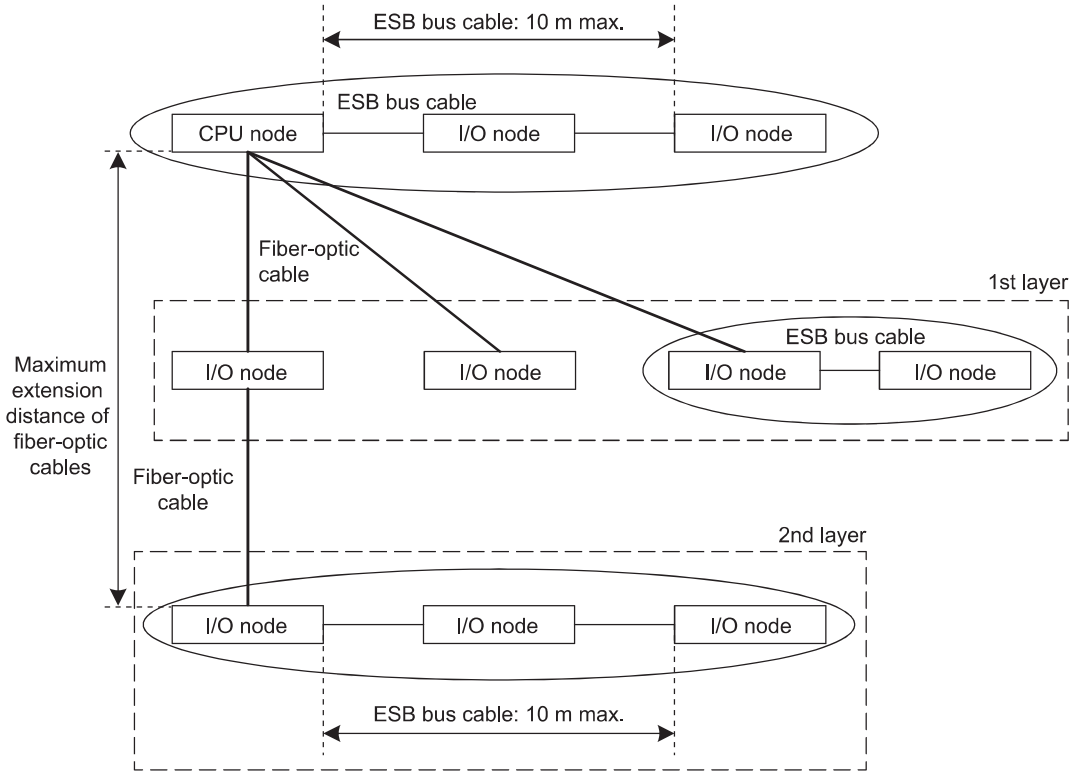


Figure A5.3-1 Overview of the optical ESB bus repeater connection function with FIO

- N-IO node only connection example

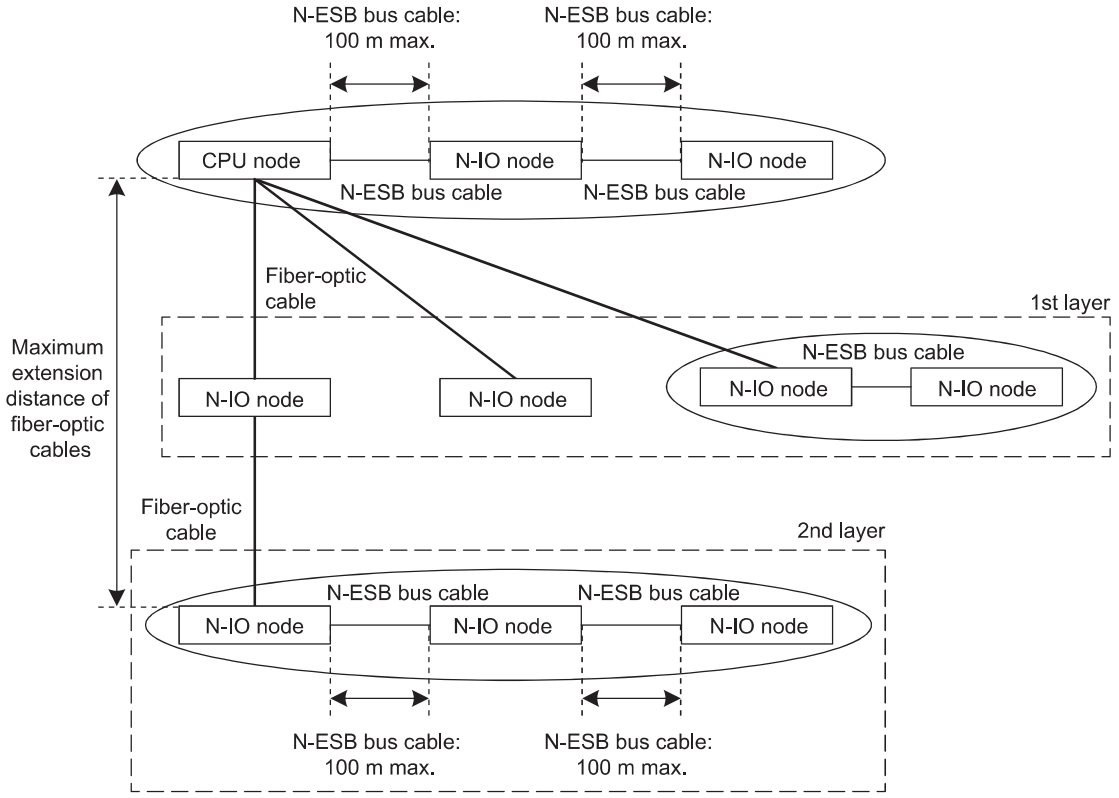


Figure A5.3-2 Overview of the optical ESB bus repeater connection function with N-IO

- FIO node and N-IO node mixture connection example

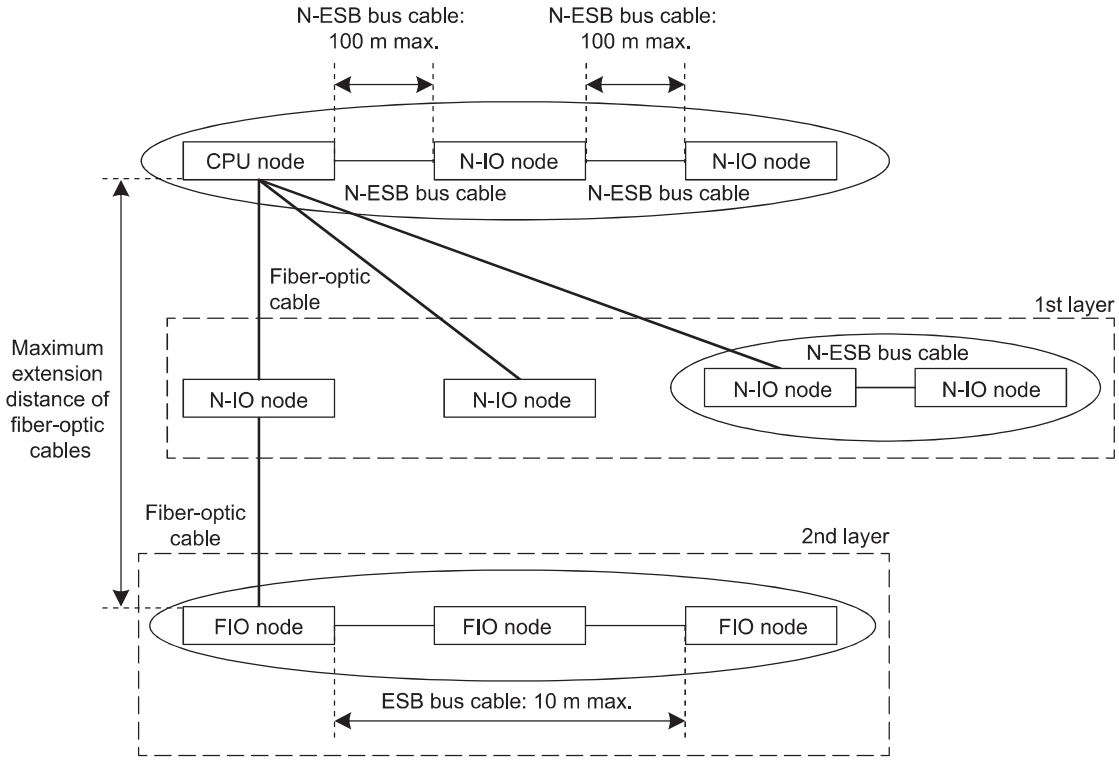


Figure A5.3-3 Overview of the optical ESB bus repeater connection function with N-IO+FIO

Related builder definition items

When connecting nodes via the optical ESB bus repeater module, definitions in the builders are required. If they are not defined properly, the following problems may occur.

- The data of the I/O module installed in the nodes is not updated correctly.
- SOE data is not updated correctly.
- The time required for communication module startup (ALR111, ALR121, or ALE111) becomes longer.
- In the station that supports Modbus slave communication or DNP3 communication, this communication cannot be performed correctly.

The following describes the definitions required for each SCS type and the specific impact of the SCS type if it is not defined.

- SCSP3/SCSL2/SCSP2
  Perform the following definition.
  - For I/O list engineering

Table A5.3-14 Builder definition (I/O list engineering) required when using optical ESB bus repeater module

Builder to be defined	Target	Definition
Node definition of IOM Definition Editor of AD Suite	Perform it for all connected I/O nodes that are extended through the optical ESB bus repeater modules. In SCSP3, perform it for all N-IO nodes that are connected with fiber-optic cable(s).	Set Optical ESB Bus Repeater-Extends Node Bus to Yes.
		Specify the ESB bus distance from the CPU node to the relevant node in Optical ESB Bus Repeater - Extends To.

  - For RS original engineering

Table A5.3-15 Builder definition (RS original engineering) required when using optical ESB bus repeater module

Builder to be defined	Target	Definition
I/O Parameter Builder	Perform it for all connected I/O nodes that are extended through the optical ESB bus repeater modules.	Set Extends Node Bus to Yes.
		Specify the ESB bus distance from the CPU node to the relevant node in Extends To.

  For the undefined node, communication errors may occur to the node. If this error occurs, the output modules may output the Output value at fault.

- SCSP1/SCSU1
  Perform the following definition.

Table A5.3-16 Builder definition required when using optical ESB bus repeater module

Builder to be defined	Definition
SCS Constants Builder	Set Optical ESB Bus Repeater to Yes.
	Specify the correct “Maximum extension distance of fiber-optic cable” in Maximum Extension Distance.
Use the Resource Properties dialog box. If the node extension distance exceeds 25 km and HART communication is performed periodically, the scan period must be changed.	Cycle Timing must be set to 100 ms or longer.

  - For I/O list engineering

Table A5.3-17 Builder definition (I/O list engineering) required when using optical ESB bus repeater module

Builder to be defined	Target	Definition
Node definition of IOM Definition Editor of AD Suite	Perform it for all connected I/O nodes that are extended through the optical ESB bus repeater modules.	Set Optical ESB Bus Repeater-Extends Node Bus to Yes.
		Specify the ESB bus distance from the CPU node to the relevant node in Optical ESB Bus Repeater - Extends To.

- For RS original engineering

Table A5.3-18 Builder definition (RS original engineering) required when using optical ESB bus repeater module

Builder to be defined	Target	Definition
I/O Parameter Builder	Perform it for all connected I/O nodes that are extended through the optical ESB bus repeater modules.	Set Extends Node Bus to Yes.
		Specify the ESB bus distance from the CPU node to the relevant node in Extends To.

In the undefined nodes, the system behaves as if the corresponding I/O node is located at the Maximum extension distance of fiber-optic cable. Although I/O modules function correctly, the CPU load fluctuation may become large if abnormalities occur. By performing definition, the CPU load fluctuation can be reduced at the time of abnormality.

- SCSV1
  Perform the following definition.

Table A5.3-19 Builder definition required when using optical ESB bus repeater module

Builder to be defined	Definition
SCS Constants Builder	Set Optical ESB Bus Repeater to Yes.
	Specify the correct “Maximum extension distance of fiber-optic cable” in Maximum Extension Distance.

Influence of ESB bus extension by optical ESB bus repeater devices

When the ESB bus is extended and installed by using optical ESB bus repeater, there is influence as follows: However, both the demand reaction time and fault reaction time are the same as those when I/O nodes are connected with non-optic ESB bus cables.

- The number of I/O modules and the amount of applications need to be adjusted according to the SCS load.
- The time required for IOM download becomes longer.
- ALR111, ALR121, or ALE111 for Modbus slave communication cannot be mounted on I/O nodes located at a distance of 5 km or further.
- For SCSP1/SCSU1 or SCSV1, the load on the CPU modules increases according to the maximum extension distance of fiber-optic cable.
- The time accuracies of SOE data (discrete inputs) vary according to the maximum extension distance of the optical fiber cable (except SCSV1). The following table shows influence.

Table A5.3-20 Time accuracies of SOE data (discrete inputs)

Maximum extension distance of fiber-optic cable	Time accuracies
Extension within 25 km	±2 ms
Extension from 25 km to 50 km	±3 ms

- When using a barrier for Digital Input, the delay time of the barrier will be added to the time precision.

SEE ALSO For more information about delay time of barrier, refer to:

Specifications and manual of barrier for Digital Input being used

A6. Inputs and outputs of SCS

This section describes the flow and processing of Analog I/O data and Digital I/O data (AIO/DIO data), and I/O variables in the SCS.

A6.1 Flow of AIO/DIO data

The following figure illustrates the flow of AIO/DIO data in an SCS.

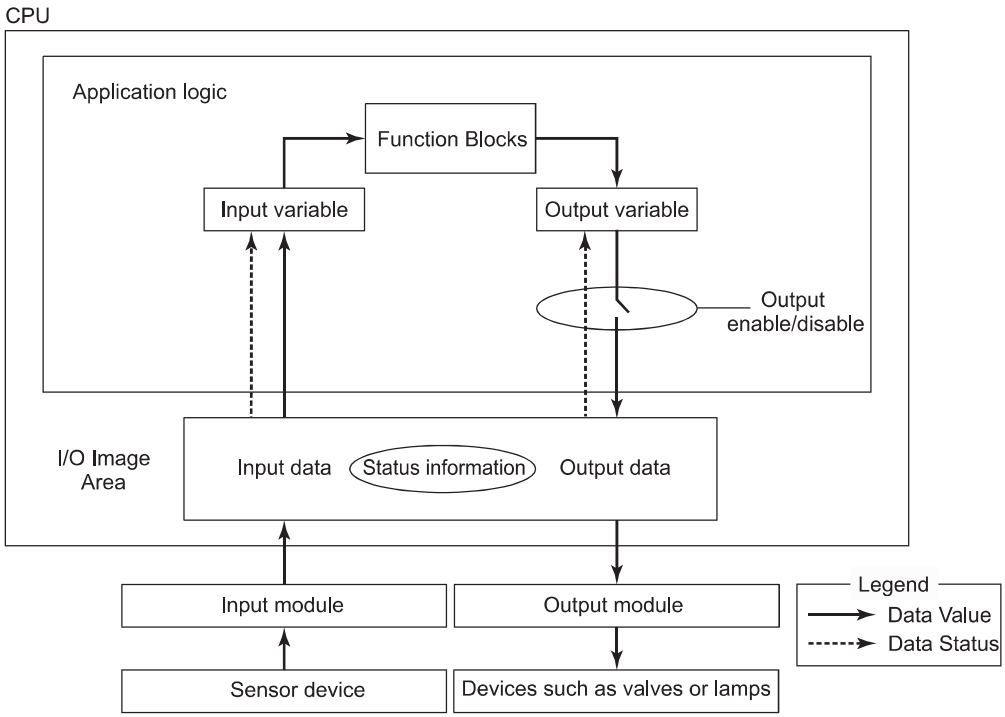


Figure A6.1-1 Flow of AIO/DIO data

1. Data sent from sensor devices or other sources is read from each channel of a connected input module.
2. The CPU copies the data stored in the input module to the I/O image area at the start of scanning. At this point, the data value and data status are determined based on the information from the input module. If the input data is erroneous, the data status is set to "BAD" and the data value is set to the "Input value at error occurrence" specified in an I/O parameter by the user.

TIP

The following I/O parameters are used for "Input value at error occurrence", which is used when input data is erroneous.

- [Input Processing at Fault] of AI and DI modules
- [Input Processing at Transmitter Fault] of an AI module

This manual uses the term "input value at error occurrence" in the following explanation as a generic term.

3. The CPU stores the input data in the I/O image area in the input variables of the application logic. It also updates the data status of the output variables.
4. The application logic references the data value and data status from the input variables and monitors the process conditions and input device status.
5. The result of the application logic processing is stored in the output variables and then sent to the output module via the I/O image area.
6. The output module outputs the data to devices such as valves or lamps connected to each of the channels.

Data value at AIO/DIO module dual-redundant configuration

If dual-redundant input modules are used, the input values from the active module are stored in the input variables. If dual-redundant output modules are used, the data values of the output variables are set to both active and standby modules, but the data is output to the field from only the active module. In the case of SDV526/L1DV526, the data values are output to the field from both modules.

Conversion of analog input data

Analog data of either 4 to 20 mA or 1 to 5 V/ 1 to 10 V is converted to normalized data of 0 to 100% in the CPU process data input processing and stored in the input variables.

All data that requires normalization, such as measurements from differential pressure transmitters, is automatically processed in the process data input processing in this way. Subsequent conversion from normalized data to data using engineering units can be performed freely in the application logic. Analog data of either thermocouple or resistance temperature detector is converted to the data (physical quantity or normalized data) specified in the input signal conversion for each channel and stored in the input variables.

Flow of analog output data

Data of 0 to 100% set in IO_REAL type output variables from the application logic are converted to electrical current of 4 to 20 mA by each output module and output.

Output enable and output disable

Output channels of an SCS can be in the Output Enable and Output Disable states. The Output Enable and Output Disable states are managed by each channel; the output states of all the output channels of an SCS do not always match.

- Output Enable is a status where the output values from the application logic are output from the output module as is.
- Output Disable is a status where the output values from the application logic are not output from the output module.

Output enable operation

Output enable operation means connecting outputs from the application logic to the output channels. If you perform the output enable operation from the I/O Channels Status dialog box of SCS Maintenance Support Tool on the SENG, all modules are placed in the Output Enable status simultaneously (not individually). Once the output enable operation is performed, all output channels are in the Output Enable status and output values of the application logic are output from the output channels. Channels that continue to generate errors remain in the Output Disable status. The following processing is also performed in the output enable operation implemented immediately after an SCS is started:

- Start sending data in inter-SCS safety communication
- Start SCS Link Transmission
- Start outputting data in subsystem communication

A6.2 I/O variable

This section explains the I/O variables, and their data value and the data status.

What are I/O variables?

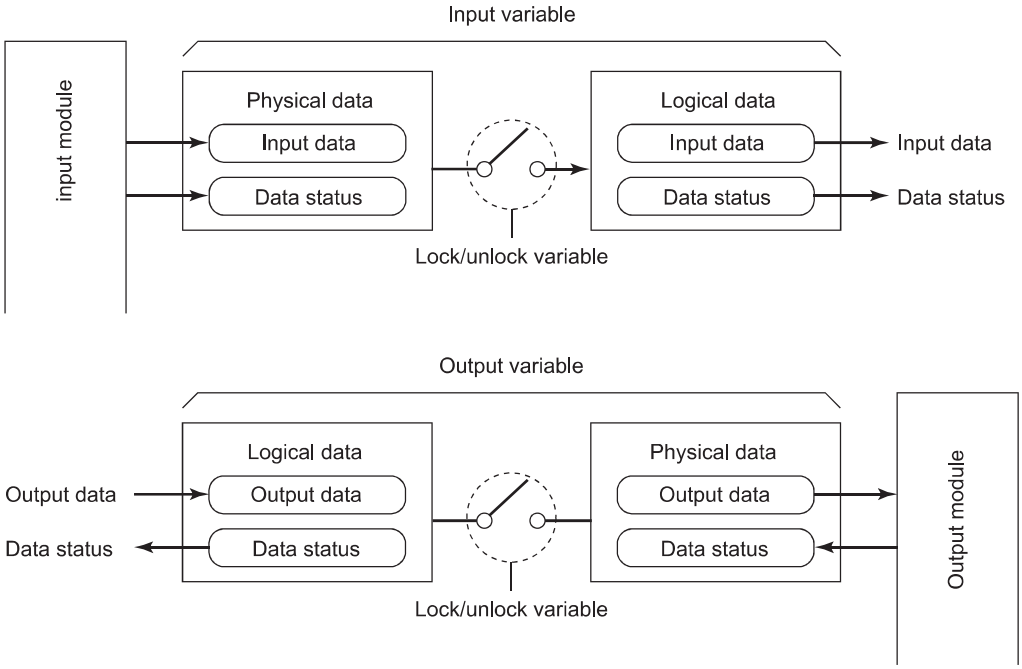


Figure A6.2-1 Input variable and output variable

The variables carrying the input values or output values of input/output modules are called I/O variables. There are two types of I/O variables: input variables and output variables. I/O variables contain two types of data, logical data and physical data. When I/O variables are defined, both logical data and physical data are automatically created.

Table A6.2-1 Input variable and output variable

Type	Data	Description
Input variable	Physical data	Data set from the I/O image area.
	Logical data	Data viewed by the application logic. (*1)
Output variable	Physical data	Data set in the I/O image. (*2)
	Logical data	Data set by the application logic.

*1: If the input data is erroneous, the input value at error specified by the user in advance is set.
*2: This is the value set to the output module.

The application logic can basically handle logical data only. In the normal status, the same data is stored in the logical data and physical data; the user does not need to be aware of the difference between these two types of data. Note, however, that physical data needs to be referenced from the SCS Manager window when locking I/O variables via the forcing function, or if both data are not connected due to input/output module failures, etc.

Both the logical data and physical data are composed of data value and data status. In order to handle data value and data status, I/O variables provide IO_BOOL type for handling BOOL-type data and IO_REAL type for handling real number-type data, which can be used according to the data type of the data value.

The data value and data status can be referenced using the application logic. Use the syntax "I/O variable name.v" and "I/O variable name.status" in order to read only the data value or the data status from an I/O variable, respectively.

Data status of I/O variables

The data status of I/O variables is expressed as a BOOL value.

Table A6.2-2 Data status that can be referenced by user applications

BOOL value	Status	Meaning
TRUE	GOOD	Status where no error has occurred in input/output modules. In the case of an input variable, this means the data value is from the field.
FALSE	BAD	This indicates that a normal data value cannot be obtained from or a value cannot be set to the I/O module due to failure of the module. In the case of an input variable, the data stored is the input value at error occurrence that is specified in an I/O parameter.

I/O variable condition and data value/data status

Timing at which data status is created

The data status of the I/O variables is created based on the I/O status information. If the I/O variables are not locked, the data statuses of the physical data and the logical data are the same. If the I/O variables are locked, only the data status of the physical data is updated.

In the case of an output variable, the update timing and transmission direction are different for the data value and the data status. Moreover, in the Output Disable status, the data values of the physical data and the logical data are different but the data status matches.

Lock/unlock status of I/O variables, Output Enable/Output Disable status and data value/data status in each status can be summarized as shown in the following tables.

Data value and data status of input variables

Table A6.2-3 Data value and data status of input variables

Status	Physical data	Logical data
Unlocked status (at normal input)	The data value takes the input value from an input module. The data status is GOOD.	The data value matches with that of the physical data. The data status matches with that of the physical data.
Unlocked status (at erroneous input)	The data value takes the input value from an input module. The previous value is maintained if there is no response. The data status is BAD.	The data value becomes the input value at error occurrence that is defined in an I/O parameter. The data status matches with that of the physical data.
Locked status	Same as for unlocked status for both the data value and data status	The data value and data status immediately before locking are retained. They can be changed from the SCS Manager.

Data value and data status of output variables

Table A6.2-4 Data value and data status of output variables

Status		Physical data	Logical data
Unlocked Status	Output Enabled	The data value matches with that of the logical data. The status of the output module is reflected in the data status at each interval.	The data value is set to the result of the application logic processing. The data status matches with that of the physical data.
	Output Disabled	The data value becomes the fail-safe value that is defined in an I/O parameter. The status of the output module is reflected in the data status at each interval.	

Continues on the next page

Table A6.2-4 Data value and data status of output variables (Table continued)

Status		Physical data	Logical data
Locked status	Output Enabled	The data retains the value immediately before locking and the value can be changed from the SCS Manager. The status of the output module is reflected in the data status at each interval.	The data value is set to the result of the application logic processing. The data status is retained immediately before locking and the status can be changed from the SCS Manager.
	Output Disabled	The data value retains the previous value. However, the fail-safe value is set by the CPU when the output is disabled. (The value can be changed from the SCS Manager.) The status of the output module is reflected in the data status at each interval.	

Logical data and physical data of analog output

The relationship of logical data and physical data of analog output is shown below. Analog output processing consists of discrete output operation, plus limiter processing and tight-shut/full-open processing.

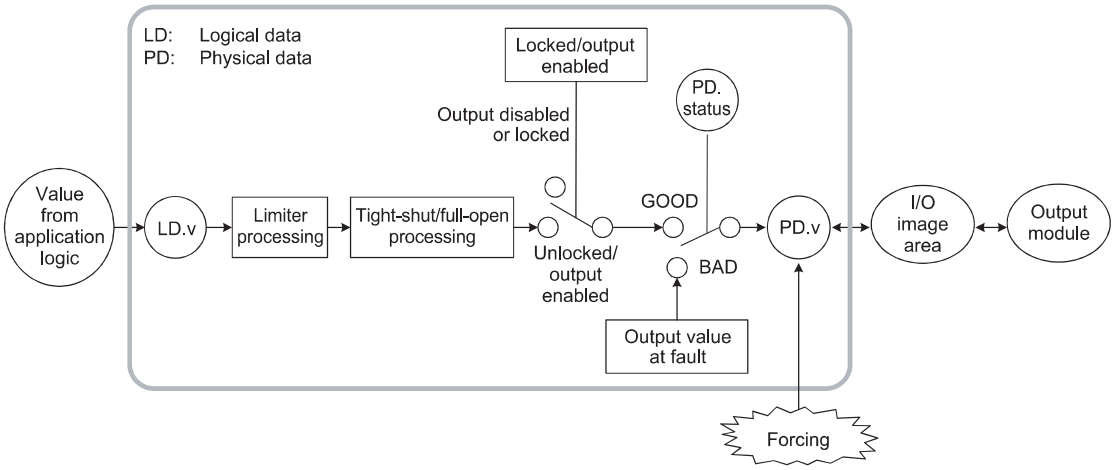


Figure A6.2-2 Flow of logical data and physical data of analog output

The following processing is performed until the logical data is output as physical data from the analog output module.

- Output is limited to a range of -17.19 to 118.75 [%].
- If tight-shut/full-open is specified, the tight-shut value is set when the logical data is 0.0 or below, or the full-open value is set when the data is 100.0 or above.
- If output is disabled or locked, the last physical data value is retained.
- If an error occurs, the Output value at fault is set or the last value is retained in accordance with the Output processing at fault.

Data status at AIO/DIO module dual-redundant configuration

In the case of dual-redundant input modules, the data status of each input variable is determined based on the I/O status information of the active input module. The same rule applies to dual-redundant output modules as well.

A6.3 High current output function

This high current output function combines consecutive DO channels of an N-IO I/O module, and supplies a large current to the connected devices. This function is used to connect to devices such as beacon and sounder.

You need to determine the number of channels to be used according to the current that is required by a connected device.

- Connecting to a device that requires a current of 1.3A: Use two consecutive channels
- Connecting to a device that requires a current of 2.0A: Use three consecutive channels

Combined channels can be categorized as primary channel and non-primary channel.

- Primary channel: The channel to which I/O variable can be assigned among the combined channels. This is the lowest number channel among the selected channels.
- Non-primary channel: The channel to which I/O variable cannot be assigned among the combined channels.

If an error occurs in the combined channels, it is notified as error in primary channels.

For example, if the channels are set to be combined on engineering, and if the combined channels are insufficient or their numbers are misplaced, it is notified as error due to open circuit in the primary channel. In this case, the output that is set in engineering becomes fail-safe value for both primary and non-primary channels in the same manner as in the output channel error. In addition, the primary channel will be in output disable status.

You need to specify the primary channel when you execute output enable operation and forcing function for the combined channels. A non-primary channel is handled in the same way as a channel that is not being used.

You can check the position of the faulty channel in the IOM Report.

IMPORTANT

The high current output function cannot be used when using an intrinsically safe barrier.

A7. Performance and scan period in the SCS

There are two types of scan periods of SCS, the scan period of the application logic execution function and the scan period of the external communication function. The scan period of the application logic execution function can be changed online.

SCS has the automatic extension function for the scan period of the application logic execution function. This function automatically extends the scan period of the application logic execution function when the load on SCS becomes high. Use the SCS Constants Builder to specify whether or not to use this function.

A7.1 Definition of SCS scan period

This section describes the definition of the SCS Scan period and how to define it.

Scan periods in SCS

The periodic processing for SCS falls into two types: Application Logic Execution Function and External Communication Function. They are executed at their respective scan periods.

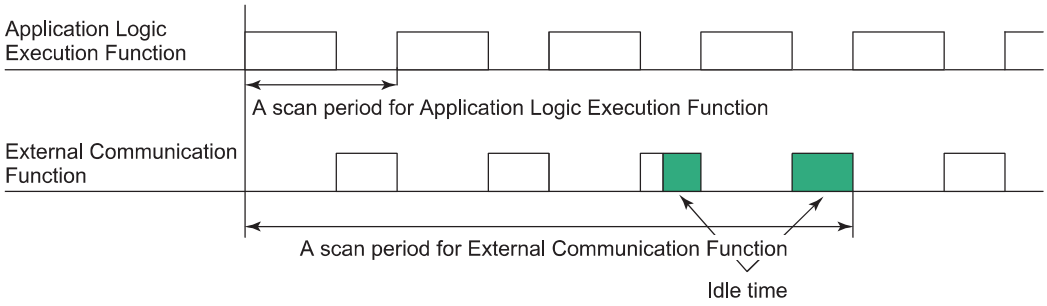


Figure A7.1-1 Scan periods of SCS

The Application Logic Execution Function is the function having a top priority among SCS functions.

The External Communication Function is executed in a part where the Application Logic Execution Function is not executed in the CPU processing period. If the External Communication Function finishes its processing before a scan period ends, the remaining time becomes the idle time on CPU.

Processing of the Application logic execution function

The Application Logic Execution Function is executed in the order presented as follows.

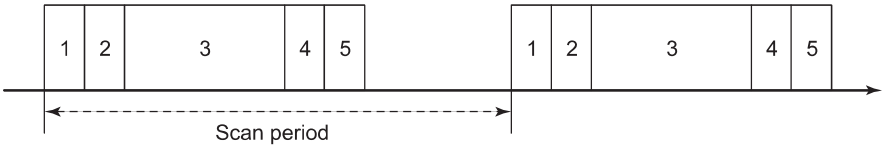


Figure A7.1-2 Processing of the Application logic execution function

Table A7.1-1 Processing of the Application logic execution function

Order	Processing Name	Description
1	Input AI/DI data, Self-diagnosis	Collects AI/DI data from input modules, and generates data values and data status. Stores the generated data in the input variables. Generates status of output modules and the self-diagnostics are also executed at the same time.
2	Receive data from other SCS	Receives the data from other SCSs, and stores them to the variables. (Applicable to inter-SCS safety communication and SCS link transmission)
3	Execute Application Logic	Executes application logic in FBD and LD.
4	Transmit Data to other SCS	Transmits data to other SCSs. (Applicable to inter-SCS safety communication and SCS link transmission)
5	Output AO/DO data, Self-diagnosis	Collects the data from output variables, and writes the data to the output modules. The self-diagnostic processing is executed at this timing.

The processing time of the Application Logic Execution Function may be prolonged by about 20% at maximum because of the increase in the CPU load caused by communication for tag data access or some other processing.

Processing of the external communication function

The External communication function is a general name for functions of communicating information of SCS with external systems. CENTUM Integration Function and Modbus Slave Communication Function are included in it.

Specification of scan period of the application logic execution function

The scan period of the application logic execution function is specified on the Link Architecture View of SCS Manager. From [Edit] > [Properties], Call the Resource Properties dialog box, enable the "Trigger cycles" check box in the "Settings" tab, and specify the value in "Cycle timing."

- The scan period can be specified in the range from 50 ms to 1000 ms in increments of 10 ms.
- The specified scan period can be changed online. (*1)

*1: Supported in the SCS of SCS system program R2.03 or later.

SEE ALSO For more information about Link Architecture View, refer to:

"Run-time Settings" in "Editing resource Properties" in "Link Architecture view" in "Workbench" in the Workbench User's Guide

Specification of scan period of the external communication function

The scan period of the external communication function is specified in the SCS Constants Builder. Specify the value in [Scan Period for External System] in the [Communication] tab.

- Either 1 second or 2 seconds can be specified.
- The default value is 1 second.
- Offline download is required to change the specified scan period.

Watching scan run time

While the SCS system program runs successfully, the Watch Dog Timer (WDT) is periodically reset. The WDT is for self-diagnosing the cyclic operations.

Confirmation of CPU processing time and consideration of idle time

CPU processing time

The actual processing time of the Application Logic Execution Function can be checked on the SCS State Management window of SENG or Status Display View of HIS. It can also be referred with the application logic by using the SYS_SCAN system function block.

Application execution time is the period of time required for processing the application logic within a scan period. Instantaneous value (%) in each scan calculated by 10 ms resolution is displayed.

CPU idle time is the period of time when the CPU has no task including the External Communication Function. Idle time per 60 seconds is displayed.

These displayed times tend to fluctuate depending on the communication load since the CPU of SCS processes the communication with SENG and communication requests from DCS.

Consideration of CPU idle time

You must confirm the above-mentioned Application Logic Execution time and CPU idle time when creating, adding, or changing an application logic for the SCS. The appropriate CPU idle time is necessary to ensure the external communication, the online change, etc.

You can take the following measures when the CPU idle time is insufficient.

- Reduce application logic.
- Lengthen the scan period.
- Divide application logic into two SCS.

Influence on application logics according to the increase of communication load

Processes on communication with SENG (online monitoring, I/O lock window operation, etc.) and communication request from DCS are done by the CPU of SCS so that they consume its idle time. Upon the increase of the frequency of such communication requests, SCS restricts the communication requests to accept to a certain amount. Thus those communications may be delayed.

Therefore when there is no communication, securing the idle time of the CPU to be more than 30 % is recommended to keep the influence on the communication to minimum upon the temporary increase of the communication load.

Influence when the execution load of the application logic is large

Even if the time taken for the processing of application logic execution occupies large portion of the SCS scan period and therefore CPU idle time is steadily less than 30%, the application logic can still be executed when there are no communications with SENG (online monitoring, I/O lock window operation, etc.) nor with DCS. However, if the communication load increases this situation, the following phenomenon will be observed.

- When the idle time is not sufficient
  - Updating the data displayed on HIS window, communication with SENG and FCS may be delayed.
  - Process alarms and annunciator alarm may be delayed.
  - Modbus slave communication may become an error.

  As the idle time lessens, the above phenomenon will become more obvious.
- When there is hardly any idle time and the application logic execution time is equal to scan period
  - Updating the data displayed on HIS window, communication with SENG and FCS may be stopped.
  - Sending process alarms and annunciator messages may be stopped.
  - Modbus slave communication may become an error.
- When there is no idle time and the application logic execution time is steadily longer than scan period
  - Inter-SCS safety communication will not be performed properly and timeout errors may be detected on the receiving side. Such phenomenon does not occur in SCS link transmission safety communication because the communication mechanism is different.

A7.2 Automatic extension function for scan period of the application logic execution function

In such a case as when the SCS has to perform very large amount of communication to access tag data, the processing time of the Application Logic Execution Function may be prolonged. If the amount of application is large and there is insufficient idle time before the next scan period starts, the SCS does not have sufficient time for the processing of communication on the control bus and for the External Communication Function that is done during the intervals between executions of the Application Logic Execution Function.

In such conditions, some functions such as the CENTUM integration function are affected. If high-load conditions continue steadily, inter-SCS safety communication may also be affected.

To avoid such adverse effects, you need to design the application logic so as to ensure the recommended CPU idle time given in the Engineering Guide.

If you anticipate that the SCS cannot maintain sufficient CPU idle time because of underestimating the amount of application logic at initial engineering or the modification of the SCS project, you can specify the use of the automatic scan period extension function in order to avoid the adverse effects (*1)

*1: Supported in the SCS of SCS system program R2.03 or later.

IMPORTANT

The purpose of this function is to temporarily avoid occurrences of erroneous conditions in SCS. SCS cannot maintain the assumed process safety time if the automatic scan period extension function is executed. Thus, take permanent measures such as reducing the amount of application logic in order to lower the CPU load on the SCS.

It is possible to check if the scan period has been automatically extended on the SENG or Status Display view of HIS as well as via diagnostic information messages. It is also possible to create application logic for confirming the state of scan period extension.

Automatic scan period extension function

The purpose of this function is to extend the scan period of the application logic automatically in order to prevent communication functions, such as inter-SCS safety communication, from stopping when the execution of application logic takes longer than the scan period defined in the SENG as a result of online changes of application software that contains engineering mistakes for example. This function can be enabled or disabled on the SCS Constants Builder. It is disabled by default.

IMPORTANT

If a demand occurs while scan period is extended, it can affect safety because, for example, the reaction time may become longer than the process safety time. You need to judge carefully whether or not to enable the automatic scan period extension, taking the process safety time into consideration. If the scan period is extended while the automatic scan period extension is enabled, promptly take countermeasures such as reducing the amount of application logic by online change.

Overview of automatic extension of scan period

If the processing of the Application logic Execution Function is prolonged and almost occupies the whole scan period of the Application logic Execution Function defined in SCS Manager, the SCS cannot perform the processing for the communication on the control bus and for the External Communication Function that is done during the intervals between executions of the Application Logic Execution Function.

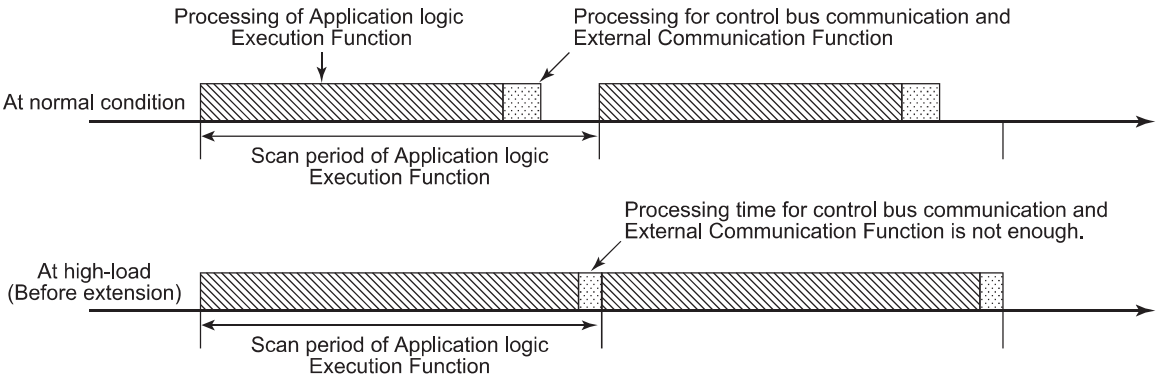


Figure A7.2-1 Example of the case when the scan period is automatically extended

The automatic scan period extension function automatically extends the scan period of the Application logic Execution Function when high-load conditions occur and ensures sufficient time for the processing of communication on the control bus and for the External Communication Function that is done during the intervals between executions of the application logic.

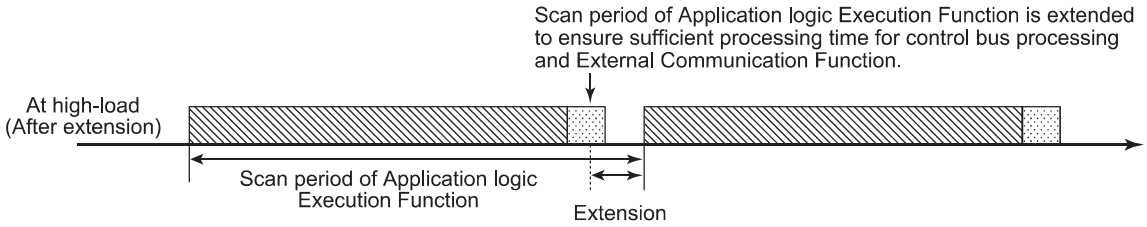


Figure A7.2-2 State in which the scan period is automatically extended

By using the automatic scan period extension function, the time for the communication processing related to the following features are ensured.

- Inter-SCS safety communication
- Integration with CENTUM
- Communication with SENG
- Diagnostic information message, process alarm notification

Conditions of starting scan period extension

When both of the following conditions are satisfied in a state at once, it is defined as a high load status.

- The total time to execute the application logic execution function and to process inter-SCS safety communications exceeds 80% of the original scan period of the application logic execution function.
- The CPU idle time becomes 0.

In this case, you can estimate the processing time for inter-SCS safety communication with the following formula:

```
Processing time for inter-SCS safety communication = (Number of consumer groups +
 Number of producer groups) x T [ms]
```

The values of T are as shown in the following table according to the configuration of the CPU module.

Table A7.2-1 Values of T

CPU module	T
SCP401/SCP451 (Dual-redundant)	5.0
SCP401/SCP451 (Single)	2.5
SCP461/S2CP471/L1CP471 (Dual-redundant)	3.0
SCP461/S2CP471/L1CP471 (Single)	1.5

If this high load status continues for 1 second or longer, the scan period of the application logic execution function is automatically extended.

The new scan time is obtained by adding 20% of the original scan period of the application logic execution function to the actual measurement of the application execution time at that time.

Influence until activation of scan period extension

The following situations may occur before the automatic scan period extension period is activated after the SCS is placed under high load status.

- Stopping of CENTUM integration data update
- Delay of diagnostic information message notification
- Stopping of forcing data update
- Stopping of status display in the SCS State Management window

Upper limit of scan period extension

The upper limit of scan period extension is 200% of the original scan period of the application logic execution function. Note that the extended scan period will never exceed the upper limit value of 1 second.

Cancellation of scan period extension

If both high load conditions explained in item "Conditions of Starting Scan Period Extension" are removed, the scan period becomes shorter by each scan in decrements of 20% of the original scan period of the application logic execution function. Note that the scan period will never become shorter than the scan period of the application logic execution function defined in SCS Manager.

Notification of execution/cancellation of automatic scan period extension

- If the automatic scan period extension function is activated on the SCS, it is notified via the diagnostic information message (No. 4143). The cancellation of extension is notified via the diagnostic information message of automatic scan period extension cancellation (No. 4144).
- If automatic scan period extension is continuously activated for a certain period of time or longer, the diagnostic information message indicating the start of the automatic scan period extension function is notified to give warning again. The re-warning interval is 10 minutes by default.

The interval of re-warning can be changed using the SYS_SCANEXT system function block.

- The system function block (SYS_SCANEXT) can be used to determine whether the automatic scan period extension function is being executed via application logic. (*1)
- If the scan period of the application logic execution function is changed via online change download while the scan period is being automatically extended, the scan period extension status is cancelled after the completion of the online change download and the diagnostic information message on cancellation of scan period automatic extension is notified. However, if the high CPU load continues even after the scan period is changed and if the conditions for automatic scan period extension are met, the scan period is extended automatically.
- The SCS State Management window of SENG and the Status Display view of HIS (*2) display both the scan period of the application logic execution function defined in SCS Manager and the actual scan period of the application logic execution function of SCS.

*1: The SYS_SCANEXT system function block can be used in new SCS databases created by SENG of R2.03.00 or later.
*2: Supported in CENTUM VP R4.02 or later.

SEE ALSO For more information about SYS_SCANEXT, refer to:

11.27, “SYS_SCANEXT (scan period extension indicator)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about Diagnostic information messages, refer to:

Message Number 4143 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)

Precautions when using Automatic scan period extension function

The fact that the SCS is running with an automatically extended scan period is important safety information. In projects where no HIS is connected, it is necessary to use the SYS_SCANEXT function block to notify the user that the SCS is running with an automatically extended scan period.

Influence of automatic extension of scan period

Automatic extension of the scan period has the following influence.

Influence on process safety time

Since the reaction time is determined based on the scan period of the application logic execution function, the time also becomes longer accordingly if the scan period is extended.

SEE ALSO For more information about precautions upon engineering related to automatic extension of scan period, refer to:

A7., “Performance and scan period in the SCS” on page A7-1

Influence on test functions

The automatic scan period extension function does not operate in SCS simulation tests and logic simulation tests.

Influence on Function Blocks

- SYS_SCAN function block
  The current scan period of the application logic execution function of SCS is output to the output parameter SCAN of the SYS_SCAN function Block.
- Function blocks handling time

There is no influence of changes in scan period on the operations of function blocks handling time. Those function blocks operate according to the actual time even if the scan period is changed.

- Function blocks handling execution count
  In the case of function blocks whose output is determined by the number of calls, the number of outputs within the unit time decreases if the scan period is extended.

  Targets: CTU, CTD, CTUD, FILTER, FILTER_S

A7.3 Locking of internal variables and performance in SCSP3/SCSL2/SCSP2

It is important to note that the application runtime becomes longer (i.e., the CPU load increases) if any internal variable is locked in SCSP3/SCSL2/SCSP2. You should lock internal variables for engineering and maintenance purposes only.

You must investigate whether there is a need to use the automatic extension function for scan period of the application logic execution function as a countermeasure to prevent high CPU load.

SEE ALSO For more information about automatic extension of the scan period of the application logic execution function, refer to:

A7.2, “Automatic extension function for scan period of the application logic execution function” on page A7-5

Internal variables that affect performance

Internal variables whose lock status affects the performance are those defined in the Dictionary. I/O variables and the variables that are locked in the Communication I/O Lock window, SCS Link Transmission Lock window and Inter-SCS Communication Lock window do not affect the performance.

Locking of internal variables

- In SCSP3/SCSL2/SCSP2, you can lock internal variables only when [Extend Scan Period Automatically] is set to [Yes], and [Locking of Internal Variables] is set to [Enable] in the SCS Constants Builder. If you need to lock internal variables, you need to set [Extend Scan Period Automatically] to [Yes], change [Locking of Internal Variables] to [Enable], and download to the SCS. Once the required lock operations are complete, you need to set these specifications back to the original settings and download to the SCS. Note that the locking of internal variables can be canceled regardless of these specifications.
- When the SCS security level is at Level 0, internal variables can be locked only if [Extend Scan Period Automatically] is set to [Yes], and [Locking of Internal Variables] is set to [Enable]. However, at Level 0, the application run time may get extended not only when the internal variables are locked, but also when the break point function of the application debugging function is used. If you use the break point function once, the application execution time does not return to the original length even if you cancel all break points.
- The locked internal variables can be checked with the diagnostic information messages of SENG or system alarm messages of HIS.

CPU load due to locking of internal variables

- If you lock internal variables when the CPU idle time is small, the execution time of the CPU may exceed the specified scan period. In such cases, the automatic scan period extension function may be activated in order to extend the scan period so that external communication processing and similar are not affected.
- Even if you lock one internal variable, the CPU load increases by 20% to 30% compared to the status where no internal variables are locked.(The rate of CPU load increase depends on the application)
- If you unlock all internal variables, the application execution time automatically returns to the original value before the internal variables are locked.
- It is recommended to set [Locking of internal variable] to [Disable] on the SCS Constants Builder while the SCS is running in normal operation. This is because there is a risk of

locking internal variables without considering the increase of CPU load if [Locking of Internal Variable] is set to [Enable].

A8. RAS (Reliability, Availability, Serviceability) functions of SCS

This section explains functions related to reliability, availability and serviceability of the SCS (hereinafter referred to as RAS in this manual). Moreover, it is a function that implements safety. The function includes the ability to shift to a safe state in a fast and reliable manner when an error occurs in the plant or system.

The RAS functions of the SCS are as follows:

- Operating mode
- Security level
- Diagnostic management function, diagnostic information messages
- Operation during start, and operation during error
- Dual redundancy

SEE ALSO For more information about SCS status monitoring functions, refer to:

H., “Monitoring the SCS status” on page H-1

For more information about Operations and recovery procedures during the SCS error occurrence, refer to:

G2., “Operations and recovery procedures during the SCS error occurrence” on page G2-1

Positioning of RAS function

RAS stands for Reliability, Availability and Serviceability, and is an important index when evaluating the system performance. Reliability means robustness against error occurrence, availability means shortness of downtime and serviceability means ease of repair at failure.

Functional relation of software

The RAS function diagnoses whether hardware and software are running normally and handles maintenance of them if any errors are detected. Since this function is able to shut the system down and change the SCS status as required, it is one of the most essential SCS functions.

Relationship with other hardware

The RAS function collects hardware error information concerning the I/O modules and other components in the station. The RAS function organizes hardware error information and executes pre-defined safety operations accordingly, such as shutting down. Error information is sent to the SENG and HIS as diagnostic information messages. The SCS saves diagnostic information generated internally. And the information can be referenced from SENG. You can delete saved diagnostic information messages from SENG.

The figure below shows how the RAS function of the SCS is positioned.

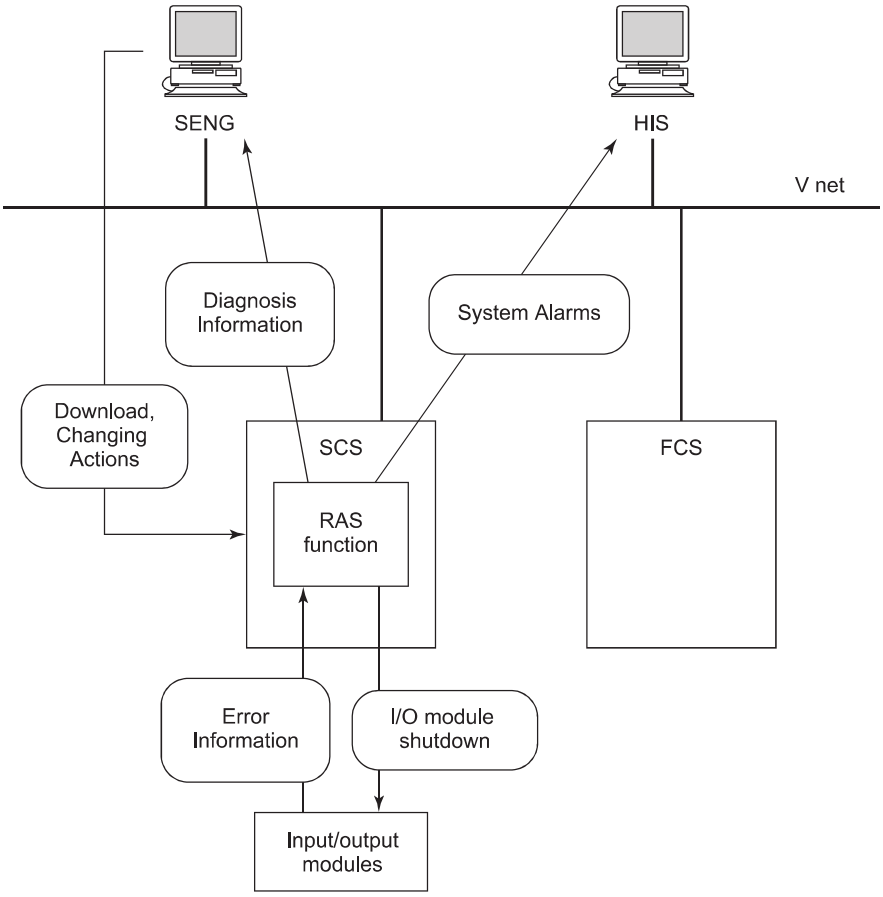


Figure A8-1 Positioning of RAS function

A8.1 SCS operating mode

The operating mode indicates the operation status of an SCS. Operations of the functions that are implemented by the system program of the SCS are determined by the operating mode. The operating mode is outlined as follows:

- The operating mode indicates the overall operating status of SCS, not the status of individual output modules.
- The operating mode indicates the status of a single SCS, regardless of whether the CPU configuration of the SCS is single or dual-redundant.
- For an SCS with dual-redundant CPU, the operating mode remains the same before and after a control right switchover of the CPU.

There are five SCS operating modes: Stop mode, Loading mode, Initial mode, Waiting mode, and Running mode

The following figure shows the transitions between operating modes. Note that it is possible to shift to the Stop mode from all other modes, but the arrows indicating these shifts are omitted for the sake of clarity.

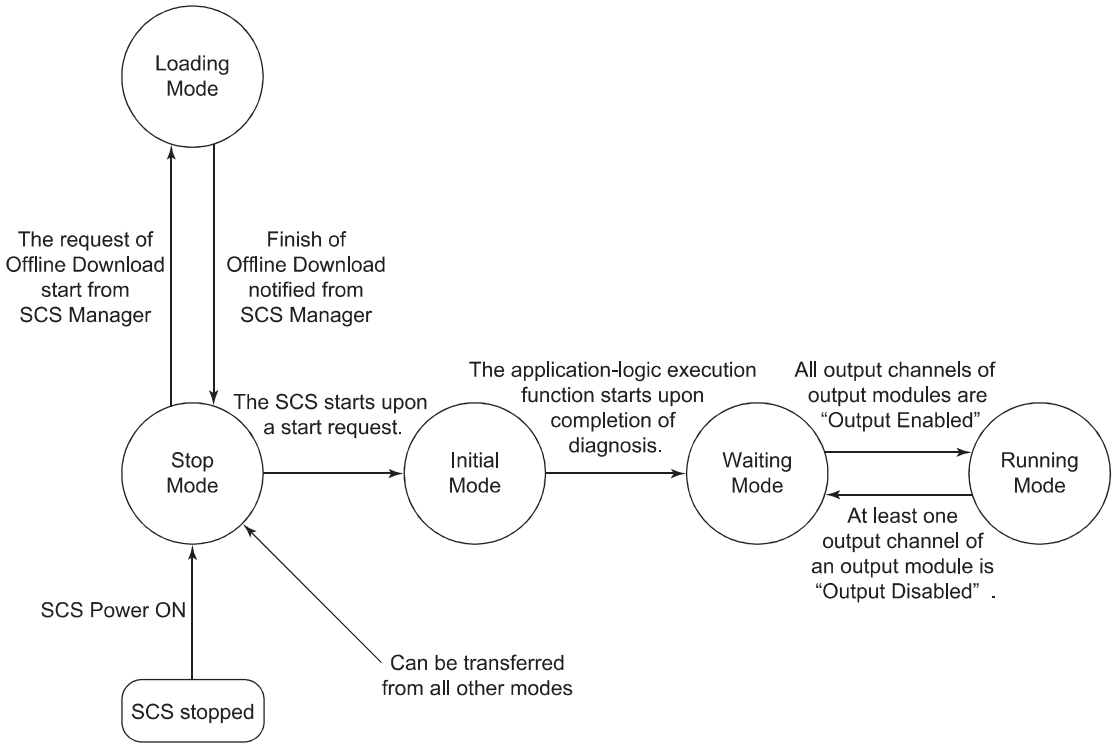


Figure A8.1-1 Transitions between operating modes

Stop mode (stopped status)

This is the initial state of the SCS.

Loading mode (during offline download)

In this mode, program and database are being downloaded from the SCS Manager to the SCS.

Initial mode (initializing status)

In this mode, the SCS is initializing databases, processing the diagnostic at startup, and starting the I/O modules as follows:

- Input modules
  If started successfully, input values are set to applicable input variables. If the startup of any module has failed, an error is recognized for the module.
- Output modules
  The outputs of all channels remain disabled after the startup is completed, so that the output values from the application logic will not be sent to the field immediately.
- Subsystem communication modules
  Receives only the input from subsystems while having an output that is invalid.
- Fire and gas communication modules
  If the startup process is successfully completed, fire and gas communication modules receive only the input from subsystems. If the startup process ends in an error, the SCS handles the fire and gas communication modules as erroneous.

Waiting mode (waiting for output enable request)

Application logic is periodically executed on each scan period. However, the output channel will not output the application logic value if the status is set to "Output Disable". The waiting mode status can be checked in the SCS State Management window and the LED display of the CPU module.

When "Output enable operation" is performed, the outputs on the normal channels of output modules are enabled. If you execute the "Output enable operation" just after starting up the SCS, the SCS also enables the output of inter-SCS safety communication, SCS link transmission and subsystem communication.

TIP

- Failure on the output channel should be removed, then perform "Output enable operation".
- Even when the channel is set to "Output Disabled", if the physical data is rewritten using the forcing function, the output value from the output channel changes.

SEE ALSO

For more information about the output enable operation, refer to:

C8., “Output enable operation” on page C8-1

For more information about relationship between forcing function and I/O variable data value/data status, refer to:

“■ I/O variable condition and data value/data status” on page A6-5

Running mode (controlling status)

This mode indicates that the SCS is running normally. All output channels of output modules are outputting the output values from the application logic. The Running mode status can be checked with the SCS State Management Window and LED display of the CPU module.

Output status monitoring

All output channels of output modules are monitored. If any of the channels becomes Output Disable status due to a failure in the corresponding module or in the output channel itself, or after adding new channels during online modification, the SCS will change its operating mode to the Waiting mode. The operating mode changes to the Running mode when the cause of the channel failure is removed, the output enable operation is completed and all output channels are placed in the Output Enable status.

Checking of operation mode

The operating mode of SCS can be checked with the following methods.

- It is possible to check that the operating mode is either the Waiting or Running mode with the SCS State Management window of the SCS Maintenance Support Tool, the SCS Status Display view of HIS and the LED display of a CPU module.
- If the operating mode is either the Waiting or Running mode, the operating mode can be referenced from the application logic as well.

Influence on operating mode

Engineering and occurrence of errors can affect the operating mode as follows.

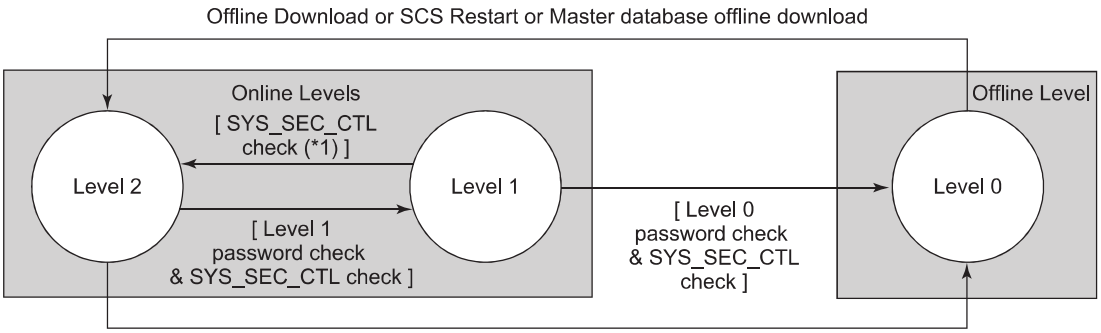
- The operating mode is not affected even if a subsystem communication error, safety subsystem communication error, or communication module error occurs.
- Occurrence of errors in SCS link transmission has no influence on the operating mode.
- If output modules/channels are added via online change download, the added modules/channels are started from the Output Disable status. If the operation mode was Running mode previously, it changes to Waiting mode. Perform the output enable operation.
- If channels in the Output Disable status or output modules that include such channels are deleted via online changes and there are no longer any channels in the Output Disable status in SCS, the operating mode shifts from Waiting mode to Running mode.
- If a single output module is changed to dual redundant configuration by online change download, IOM download is executed in order to initialize the modules. The outputs of the target modules become disabled after downloading. Since some channels are in the Output Disable status, the operating mode of SCS shifts to the Waiting mode. Perform the output enable operation after the output modules recover to normal.
- It is possible to perform the output enable operation regardless of the status of communication modules.
- It is possible to perform the output enable operation even if the status of communication with sub-systems is BAD. In this case, only outputs that are ready to communicate will start.

A8.2 Security level of SCS

The security level of SCS indicates the level of protection against erroneous writing to the memory in SCS from the connected stations or devices. An overview of SCS security level is as follows:

- One SCS has one security level.
- The security level can be confirmed from LED on the CPU module and the SCS State Management window of SCS Maintenance Support Tool or Status Display View of HIS.
- SCS limits changes made from the outside according to security level.
- Security level can be referred to by applicable logic.
- Security level can be changed by an authorized user with the password using the SCS Manager.
- Using the system function block (SYS_SEC_CTL) makes it possible to control whether or not to allow security level change operations from an SENG with an external hardware switch or similar.
- Security level can be changed under the following conditions:
  - The SCS is either in the Waiting or Running mode, AND
  - The SYS_SEC_CTL is set to allow security level changes or is not used.

The following figure illustrates the transition of states of the security level.



*1: It is allowed to reset the security level from Level 1 to Level 2 via the RST input in the SYS_SECURE block, regardless of the security level change enable/disable status of SYS_SEC_CTL.

Figure A8.2-1 Transition of security level status

Definition of each security level

There are two classifications of levels; online level and offline level. The Online level is used when SCS is in normal operation. The Offline level is used when SCS is not in normal operation.

Online level

The Online Level is a security level to be used when normal operation is performed in SCS. The SCS itself provides security of the Online Level by controlling access to the memory from the outside.

The Online Level is separated into two levels according to limits of functions which can be used.

Table A8.2-1 Online level

Level	Description
Level 2	The highest security level. SCS is usually operated at this security level.
Level 1	A temporary security level used by engineers or authorized users for maintenance of equipment or changing applications online

Offline level

The Offline Level is a security level to be used when a regular operation is not performed in SCS. This is displayed as "Level 0" on the LED of SCS or the SCS State Management window of SENG. In the Offline Level, SCS does not limit access to SCS from the outside. However, information which was used at test may be stored in SCS databases depending on operations performed by those tools.

IMPORTANT

To restore an SCS to Online Level from Offline Level, restart the SCS or do offline download. This ensures that the system returns to the security level for normal operation.

Relationship of operational items with SCS security levels

The following are the list of operational items in each security level. It is also possible to write information which is not related to any reference or safety function of the SCS, at any level.

Table A8.2-2 SCS related operations and the required security levels

SCS related writing operation	Security level (*1)			Operation side
	Level 2	Level 1	Level 0	
Override from HIS	OK	OK	OK	HIS
Operation for password block from HIS	OK	OK	OK	HIS
Operation for manual operation block	OK	OK	OK	HIS
Executing the reset function of a function block for fire and gas devices from HIS	OK	OK	OK	HIS
Confirmation of process alarm	OK	OK	OK	HIS
Setting operation mark on mapping block/mapping element	OK	OK	OK	HIS
Confirming and deleting the diagnostic information	OK	OK	OK	SENG
Setting Vnet time	OK	OK	OK	HIS/SENG
Change of security level	OK	OK	ERROR	SENG
IOM Download (*2)	OK	OK	OK	SENG
Resetting of trip signal file	OK	OK	OK	SENG
Change of passwords for security level	OK	OK	OK	SENG
Locking/unlocking of variables	ERROR	OK	OK	SENG
On-demand communication for device management	OK	OK	OK	PRM
Change of variable value with forcing function	ERROR	OK	OK	SENG
Online change of applications	ERROR	OK	OK	SENG
I/O lock function	ERROR	OK	OK	SENG
Communication I/O lock function	ERROR	OK	OK	SENG
Switching control right for redundant AIO/DIO modules	ERROR	OK	OK	SENG

Continues on the next page

Table A8.2-2 SCS related operations and the required security levels (Table continued)

SCS related writing operation	Security level (*1)			Operation side
	Level 2	Level 1	Level 0	
Enabling NIU maintenance port (*3)	ERROR	OK	OK	SENG
Offline download	ERROR	ERROR	OK	SENG
Application debugging function	ERROR	ERROR	OK	SENG
Restarting the SCS from SENG	ERROR	ERROR	OK	SENG
Output enable operation	OK	OK	OK	SENG
Save/download operation marks	OK	OK	OK	SENG
Start output module operation	OK	OK	OK	SENG
Locking and unlocking variables, changing variable values, and locking I/O by using iDefine	ERROR	ERROR	OK	iDefine

*1: OK: Operation allowed
ERROR: Operation failed
*2: You can download only on failed I/O modules.
*3: Can run only SCSP3 which supports NIU maintenance.

Security level at the start of SCS

The security level is Level 2 when SCS starts normally.

Operation of security level

Change operation of security level

To change the security level from Level 2 to Level 1 or to Level 0 or from Level 1 to Level 0, entering a password from SENG is required. When the security level is changed, SCS notifies the user of the change of the security level with the Diagnostic Information Message.

You can change the security level from Level 1 to Level 2 without a password. To change the security level from Level 0 to Level 2, you must restart the SCS.

Protection of security level by hardware switch

It is possible to use SYS_SEC_CTL to control whether or not to allow changing the security level from a SENG using an external hardware switch or similar.

- When the SYS_SEC_CTL is used, it is not allowed to change security level by password entry from SENG if the FIX parameter input of the SYS_SEC_CTL is set to TRUE. To change the security level of the SCS, the user needs to operate an external key switch or similar and change to the status where security level change operations are allowed (set the FIX parameter of the SYS_SEC_CTL to FALSE), and enter the appropriate password from a SENG.
- The SYS_SEC_CTL also controls whether it is allowed to reset the security level from Level 1 to Level 2 (even though password entry is not required).
- If the security change enable/disable status is changed by the SYS_SEC_CTL, the status is notified to user via a diagnostic information message.
- Resetting of the security level to Level 2 via RST input in the SYS_SECURE block and resetting of the security level to Level 2 via the CPU's restart switch are not affected by the security change enable/disable status of the SYS_SEC_CTL.

IMPORTANT

The situation when the FIX parameter of the SYS_SEC_CTL is constantly set to TRUE by erroneous applications should be surely avoided.

Reset function for security level

When a fault occurs in SENG or the communication line while the security level (Level 1) is being changed, it is required to reset the security level (back to Level 2) as soon as possible to ensure security of SCS. The SYS_SECURE block in the application logic can reset the security level with RST input.

- It is possible to reset from Level 1 in the SYS_SECURE block, not from Level 0.
- Connecting a discrete input signal to RST makes it possible to reset the security level with a key switch or a button. When this is not necessary, set FALSE to RST.
- The SYS_SECURE block detects the change of RST input from FALSE to TRUE and resets the security level.

Monitoring function of security level

When the security level of an SCS is in Level 1, the SYS_SECURE block monitors duration of the status. If the status of Level 1 continues longer than the time specified by the CHKT input in the SYS_SECURE block, a diagnostic information message occurs. After notifying the diagnostic information message, the duration is monitored again. The status of Level 0 is not monitored.

The following figure shows an example of application using the SYS_SECURE.

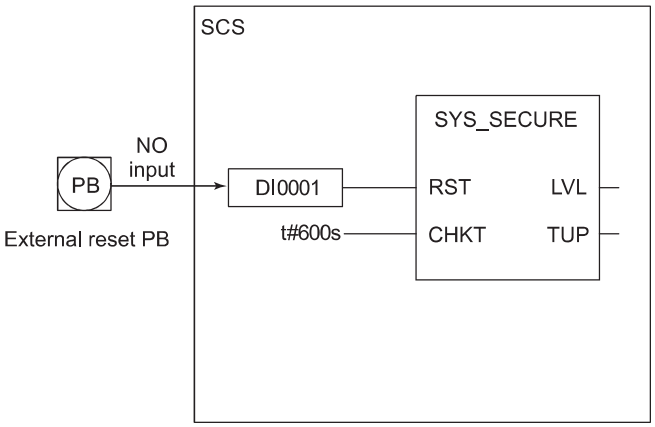


Figure A8.2-2 Example of application using security block

Passwords for changing security level

Specification for passwords

- Passwords for the security level are controlled in SCS.
- A password for the security level is set for each security level.
  It is necessary to set the password to change to Level 1 and Level 0 respectively. A password is not necessary to change to Level 2.
- A password is a maximum 16 of single-byte alphanumeric characters and following symbols including a space character. The password is case-sensitive.
  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~
- Passwords are maintained during a power cut and restart of SCS.
- Passwords are deleted by SCS offline download.

Setting and changing passwords

- Change passwords on the SCS Manager in SENG.
- Passwords can be changed when SCS is in operation.

- To change a password, user must enter the old password before it is changed.
- When a password has been changed, SCS notifies its change with the Diagnostic Information Message.

SEE ALSO For more information about operations for changing the SCS security level and setting the password, refer to:

B3., “Security of SCS” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

Precautions when changing SCS security level

- Set different passwords for each SCS.
- Set a different password for each security level.
- When the security Level of SCS has been changed, confirm that the change is made to an appropriate level with the SCS State Management Window.
- Do not set the security levels to Level 1 or Level 0 for several SCSs at the same time when SCSs are in operation.
- If setting a password to SCS during APC (All Program Copy), APC restarts. It takes about 10 minutes from setting a password, after offline download, to restarting the operation of the dual-redundant system.
  Do not change passwords during APC except the changes required for after offline download.

IMPORTANT

- When a password is not set, entering characters in the Password Entry Dialog causes an error. Considering safety as the safety system, always set passwords to use.
- Power failure or restart does not change or delete passwords.
- Passwords are deleted when offline download is performed. As there is no password after offline download, set new passwords after performing offline download.
- Passwords cannot be referred to after setting them. User should remember the set password. Also, Password should be controlled so that unauthorized users do not know it.

Precautions when using the SYS_SEC_CTL

The SYS_SEC_CTL block can control whether or not to enable the security level change by password entry from SENG. In general, an application containing the following blocks should be created.



Figure A8.2-3 General application example

Connect the toggle switch signal for controlling the security level change output from a DI module to the FIX parameter input of the SYS_SEC_CTL block. This makes it possible to switch the security change permission status via the external toggle switch. By connecting the output parameter to a lamp or similar, the security level change permission status can be displayed on an external device.

If the external toggle switch is connected to SYS_SEC_CTL, make sure to examine all possible states of the DI module or channel to which the toggle switch signal is input.

If an error occurs in the DI module or channel, SYS_SEC_CTL controls the security level change permission status as follows according to the setting of the I/O parameter Input Processing at Fault.

Table A8.2-3 Security level change control operations

Input Processing at Fault	Operation at Errors
1 (TRUE)	Changing security level by password entry via a SENG is disabled until the fault is corrected. (*1) If a fault occurs in Level 1, it is possible to reset to the same security level by the SYS_SECURE block (*2) or reset to Level 2 by restarting the SCS. It is, however, not possible to change to a lower level until the fault is corrected. (*3)(*4)
0 (FALSE)	During a fault, it is possible to change security level by password entry via a SENG.
HOLD	The operation performed before the fault occurred resumes. In other words, if an error occurs in the status where security change is unavailable (FIX is set to TRUE), the status where security change is not allowed is retained after the error occurrence. If an error occurs in the status where security change is allowed (FIX is set to FALSE), the status where security change is allowed is retained after the error occurrence. If an error occurs in the status where security change is unavailable (FIX is set to TRUE), it is necessary to take the same precautions as when inputting TRUE at Input Processing at Fault.

*1: Do not lock the input/output variables connected to FIX and change the security level to Level 2. The variables will not be unlocked even after the causes of errors are removed. (In this case, it is necessary to restart the SCS or reset by SYS_FORCE.)
*2: Use separate DI modules for the DI module for inputting the reset signal of the SYS_SECURE block and the DI module for inputting a toggle switch for security control of the SYS_SEC_CTL block.
*3: It is not necessary to lower the security level during recovery operations. If a DI module fails, replace the module and perform IOM download.
*4: It is necessary to take measures such as incorporating an application in order to avoid situations where the security level cannot be reset to Level 2 due to DI module errors when the security level is Level 1.

A8.3 Operations at SCS startup

An SCS always performs the initial cold start processing when it starts up. It does not have a function that allows it to resume the operating mode it was in before stopping. The operating mode at startup is always the Stop mode.

SEE ALSO For more information about Operating mode, refer to:

A8.1, “SCS operating mode” on page A8-3

Types of SCS startup methods

An SCS can start up in one of the following three ways.

Power recovery start

An SCS starts up in this way when the power supply is resumed after power failure.

Start after offline download

An SCS starts up in this way when the user performs offline download from the SCS manager.

Manual restart

An SCS restarts when the restart switch of the CPU module is pressed or the user performs SCS restart operation from SCS Manager of the SENG.

TIP

- After starting SCS, the operation requests from the SENG and Workbench will be ignored until the operating mode of the SCS changes to Waiting mode. The same error will occur to the communications with FCS or HIS for the CENTUM integration as well as Modbus slave communication. The operating mode of the SCS can be checked on the SCS State Management Window or identified through the LED of the SCS CPU module.
- A diagnostic information message notifying a failure/recovery may generate twice when the SCS is restarted. This does not present any problem in practical operations or on safety.

Internal data at SCS startup

Since an SCS always performs initial cold start when it starts up, all operation areas and variable values maintained dynamically by the SCS are initialized. System programs and databases that were downloaded offline and changes made online are saved in the flash memory and restored at start up.

Moreover, when the SCS is started, data saved in the NVRAM (nonvolatile RAM) may remain without being initialized.

The following are examples of data stored in the NVRAM (nonvolatile RAM):

- System log information
- Diagnostic information (200)
- SOE data log information (1000)
- Retainable data (SCSU1 only)

Table A8.3-1 Data status when starting SCS

Data stored in...	Data in SCS	Started after offline download	Started after power is restored/Manually restarted
Main memory	Variable in application logic	Initial value	Initial value
	Data in function block	Function block performs initialization	Function block performs initialization
	Security level	Level 2	Level 2
	Lock status of the variable	Reset	Reset
	Data of CENTUM integration function	Initial value	Initial value
Flash memory (*1)	System program	Loaded programs	Returns to the program used before the outage/stoppage.
	Database	Loaded database	Returns to the database used before the outage/stoppage.
	Contents of online modification		Changes made before the outage/stoppage are still valid.
	Password for changing the security level	The password used before loading is invalid (should be initialized).	The password used before the outage/stoppage are still valid.
NVRAM (nonvolatile RAM) (*2)	Specific log information	The log information before loading is not initialized.	The log information before outage/stoppage is not initialized.
	Retainable data	Initial value (*3)	The retained data before outage/stoppage is not initialized, but the data will be restored after SCS is started.

*1: This assumes that you have written into the flash memory.
*2: For the CPU modules with a battery on/off switch, NVRAM (nonvolatile RAM) is initialized if the power supply to the SCS is lost while the battery has a problem.
*3: It will not be initialized for master database offline download.

System alarms for the Inter-SCS safety communications and link transmission at the SCS startup

During SCS startup, no system alarm is raised for an error in the inter-SCS safety communications and SCS link transmission. System alarm is sent for the first error after the startup procedure and the error during the startup procedure turns to normal. System alarms related to inter-SCS safety communications and SCS link transmission are sent from the receiving station only.

At SCS startup, make sure that both the inter-SCS safety communications and link transmission are normal.

Do the following to check the normalcy:

- Check the communication status of the receiving function block (NR status of CONS FB, STS of LTRCV FB, and STS of LTFCS FB).
- Check the CMER of the system function block, SYS_DIAG.

A8.4 Diagnostic information management

The SCS detects hardware and software errors through self-diagnosis. It also notifies and saves diagnostic information by using the diagnostic management function. This section explains the diagnostic management function of the SCS.

Overview of self-diagnosis of SCS and diagnostic management function

An SCS performs self-diagnosis regularly to detect hardware and software errors. It analyzes detected errors and system configuration to determine the error level according to the error occurred and executes error-handling operations according to the error level.

The diagnostic management function saves/manages diagnostic information messages generated by self-diagnosis and manages the SCS status. Moreover, it notifies the operation status of the SCS to the SENG and HIS.

Functional relation of diagnostic management function

The following figure illustrates the flow of error information detected by the SCS diagnostic functions. Error information is composed of SCS statuses indicating faulty locations/error causes and diagnostic information messages used to notify the user about the errors. In the case of a CENTUM integration structure, the HIS treats diagnostic information messages as system alarms.

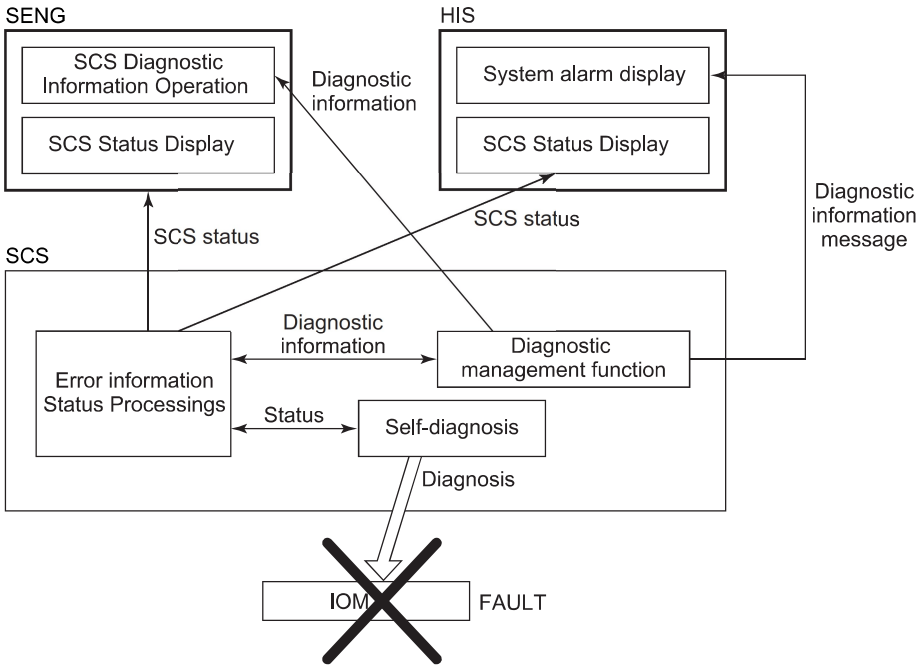


Figure A8.4-1 Functions related to SCS error information and flow of information

Management of diagnostic information

An SCS manages diagnostic information in the following manner.

- The SCS saves diagnostic information messages it sends in its memory as diagnostic information. It sends the saved message information in response to requests from SENG windows that handle diagnostic information.
- The buffer in the SCS that stores diagnostic information message has the capacity limit. In order to save all diagnostic information messages, it is necessary to collect diagnostic information messages from the SENG. The SCS can save up to 5000 diagnostic informa-

tion messages. If the SCS buffer becomes full, diagnostic information messages are deleted starting from the oldest one.

- In the event of power failure, the SCS saves the latest diagnostic information in the NVRAM (nonvolatile RAM). It will restore the saved information upon restart.

Notification of SCS diagnostic information

The diagnostic management function notifies SCS diagnostic information in response to requests from windows that handle diagnostic information. This allows checking and manipulating the information from the SENG and HIS.

- It is possible to check diagnostic information for each failed part from the Diagnostic Information Window of the SENG.
- It is possible to acknowledge/delete diagnostic information messages from the Diagnostic Information Window of the SENG.
- It is possible to see diagnostic information as a list of system alarm messages in SOE Viewer of the SENG and HIS.
- It is possible to check the state of the SCS, including how the CPU module is operating in the SCS Report dialog box of the SCS State Management Window of the SENG.

Notification of diagnostic information to Function Blocks

System status function blocks notify errors that are detected by the system diagnosis. As a result, you can make an application logic that uses the diagnostic information as reference and takes action when errors occur.

SEE ALSO

For more information about Safety system function blocks, refer to:

11., “Safety system function blocks” in POU Reference Manual (IM 32P03B20-01EN)

For more information about interference-free system function blocks, refer to:

12., “Interference-free system function blocks” in POU Reference Manual (IM 32P03B20-01EN)

A8.5 Diagnosis for hardware

The SCS carries out diagnosis at the following timing to check whether various types of hardware including I/O modules are in the normal state:

- At the start of the hardware
- At specified periodical intervals during operation

This section describes the HKU function in the CPU module, and the cabinet status monitoring function in the N-IO node.

HKU (House Keeping Unit)

The HKU function in the CPU module monitors the operation environment of the CPU module. An error in the CPU operating environment is notified to the user via diagnostic information messages and status display window. The following items are monitored by the HKU function.

- Fan status in the safety control unit
- Surrounding temperature of the safety control unit
- Battery temperature

Cabinet status monitoring

The N-ESB bus module of N-IO node monitors the operating environment of the cabinet. An error in the operating environment of the cabinet is notified to the user via diagnostic information messages and status display window.

Temperature monitoring

The SCS monitors the surrounding temperature of the N-ESB module, as well as the upper limit and lower limit value in the hardware. It monitors whether the temperature exceeds the prescribed value or not.

Power supply diagnosis

The SCS monitors the status of the power supply unit (PSU) connected to the N-ESB module unit. The following are the methods in diagnosing a power supply:

- PSU output stop diagnosis
  The SCS monitors the output voltage in redundant PSUs. It is judged as an error if output in either of the PSUs stops.
- Output over-voltage diagnosis
  The SCS monitors the output voltage of the PSUs, as well as the upper limit and lower limit value in the hardware. It monitors whether the output voltage exceeds the prescribed value or not. It is judged as an error if it exceeds the maximum value.

Input monitoring from external devices

By inputting a single point of discrete signal from an external device, which can detect power supply and fan abnormalities, in an external alarm input of the base plate, errors from the external device can be notified.

The safety control unit outputs the diagnostic information message according to the discrete signal that is inputted from the external device.

Because this function is interference-free, it cannot be used for safety logic.

A8.6 Dual-redundancy in the SCS

ProSafe-RS supports dual-redundant configurations of SCS CPU modules and input/output modules. With the dual-redundant configuration, the continuous controllability and operating efficiency can be improved. Moreover, with dual-redundantly configured hardware, the continuity of plant safety monitoring will be guaranteed by switching the control rights when an error occurs in the SCS hardware.

A8.6.1 Redundant configuration in SCS

In SCS, redundant configuration can be selected for the CPU module and I/O modules. The control bus, power supply module, ESB bus, ESB bus interface module, optical ESB bus repeater module, N-ESB bus, N-ESB bus module, and F-SB bus are always in redundant configurations.

CPU module

- The CPU module on the standby side performs the same control processing as the control side even while it is in the standby status. For this reason, it is possible to take over outputting data immediately after the control right is switched. Moreover, the operating mode of the SCS does not change.
- Only the CPU on the control side accesses the hardware composing the SCS and the CPU on the standby side always sets the equivalent value as the processing result. Therefore, the CPU modules on both sides always perform processing using the same data.
- In redundant configuration, if the CPU module on the standby side is not in the STBY status and the control right cannot be switched, the same operation as single configuration CPU module is performed.
- SOE data related to discrete inputs might be lost when the control right is switched between the CPU modules.
- With the CPU module of SCSL2 and the CPU module of SCSP2, the data loaded with the previous scan may be used instead of updating the data with the value from the input module when performing a scan immediately after a control right switchover of the CPU. Also note that data loaded from 1 or 2 scans earlier may be used with subsystem communication modules.
- With the CPU module of SCSP3, the data loaded with the previous scan may be used instead of updating the data with the value from the input module or fire and gas communication module when performing a scan immediately after a control right switchover of the CPU. Also note that data loaded from 1 or 2 scans earlier may be used with subsystem communication modules.

FIO I/O modules

Redundant configuration is possible in the FIO node(*1) by mounting the same type of FIO I/O module to two adjacent slots. In the case of redundant configuration, one side becomes the control side and the other becomes the standby side. Switching of the control right is performed by input/output modules. The switching has no influence on the application logic.

*1: An odd-numbered slot and the even-numbered slot obtained by adding 1 to the odd slot number

- It is not allowed to have redundant configuration across two nodes.
- SOE data related to discrete inputs might be lost when the control right is switched between the input modules even though the frequency is low.
- A HART communication error may occur when the control right is switched between analog input/output modules that support HART communication.

Table A8.6.1-1 Operation of redundant AIO/DIO modules

AIO/DIO module	Redundant operation
Analog input module Digital input module	The input data of the input module on the control side is stored in the input variable.

Continues on the next page

Table A8.6.1-1 Operation of redundant AIO/DIO modules (Table continued)

AIO/DIO module	Redundant operation
Analog output module Digital output module	The SCS outputs the same value for output modules on both the control and standby sides. Only the output module on the control side outputs signals to the field. If an error occurs on the module on the control side, the control right is switched and outputting is continued

SEE ALSO For more information about duplexing subsystem communication, refer to:

D1.2, “Dual-redundant communication” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

NIO I/O modules

Redundant configuration is possible in the N-IO node by mounting the same type of N-IO I/O module to two adjacent slots. In the case of redundant configuration, one side becomes the control side and the other becomes the standby side. Switching of the control right is performed by input/output modules. The switching has no influence on the application logic.

- SOE data related to discrete inputs might be lost when the control right is switched between the input modules even though the frequency is low.
- A HART communication error may occur when the control right is switched between analog input/output modules that support HART communication.

Table A8.6.1-2 Redundant operation in N-IO I/O modules

Signal type	Redundant operation
AI/DI	The input data of the input module on the control side is stored in the input variable.
AO/DO	The SCS outputs the same value for output modules on both the control and standby sides. Only the output module on the control side outputs signals to the field. If an error occurs on the module on the control side, the control right is switched and outputting is continued

Optical ESB bus repeater module

The optical ESB bus repeater modules are always used in a redundant configuration.

Power supply module

A redundant power supply module is installed on each of CPU nodes, I/O nodes, and N-IO nodes of the SCS. The SCS monitors the status of the power supply at regular intervals and, if an error occurs, it notifies the user about the error via the SCS State Management window of the SENG, the Status Display view of the HIS, and diagnostic information messages. If one of the two power supplies mounted on the CPU node has generated an error, it notifies two diagnostic information messages; one corresponding to the error of the power supply module on the CPU node and the other corresponding to the error of the power supply module on node 1.

ESB bus and ESB bus interface module

The ESB bus is redundant. The two ESB buses are connected to their corresponding ESB bus interface modules. The following operations also apply when optical ESB bus repeater devices are present along the communication route.

- Normally, redundant ESB buses are used in an alternating fashion.
- If an error occurs in either ESB bus interface module, the user is notified of the error with a diagnostic information message. If both buses fail, the error is treated as a node failure.

- If an error occurs in one ESB bus or ESB bus interface module, the SCS continues communication by using only the other ESB bus that is normal.
- An erroneous bus is monitored for normal recovery at regular intervals.
- Errors in communication with all I/O nodes, except CPU node, are judged to be ESB bus error.

N-ESB bus and N-ESB bus module

The ESB bus has redundant configuration. Each N-ESB bus module is connected to N-ESB bus, respectively.

- Normally, redundant N-ESB buses are used in an alternating fashion.
- If an error occurs on either N-ESB bus module, the error is notified to the user via a diagnostic information message. If both buses fail, the error is treated as a node failure.
- If an error occurs in either N-ESB bus or N-ESB bus module, the SCS continues communication using only the normal ESB bus on the other side.
- An erroneous N-ESB bus is monitored for normal recovery at regular intervals.

F-SB bus

The F-SB bus has redundant configuration.

- The F-SB bus is normally used at the same time on both sides.
- If an error occurs in either F-SB bus, the SCS continues communication using only the normal ESB bus on the other side.
- An erroneous F-SB bus is monitored for normal recovery at regular intervals.

Vnet/IP communication

Vnet/IP is redundant. Independent subnets using bus 1 and bus 2 comprise redundant buses.

Normally, bus 1 is used for control communication. If a communication error occurs on bus 1, bus 2 is used to perform control communication.

A8.6.2 CPU redundant status

The availability of an SCS can be improved by making CPUs redundant. Each of the redundant CPUs can be in either control or standby states, which are unique to the CPU.

CPU status

In order to show the status of a redundant configuration, it is necessary to indicate the status of each CPU separately. The operating status of the CPU is called the CPU status.

- The CPU status indicates the operating status of the CPU.
- The processing of the SCS references the CPU status as necessary. The user can check the CPU status via the CPU's LED, the SCS State Management window of the SENG, and the Status Display view of HIS.
- If an error occurs in the standby CPU, the FAIL status is notified to the application logic via a system block.

The figure below illustrates the CPU status shift. Note that in order to explain the CPU status, the operating modes it can shift to the Initial mode are called "CTRL" and "STBY." These indicate whether the CPU has the control right and are specific to the redundant status, i.e., not related to the operating mode.

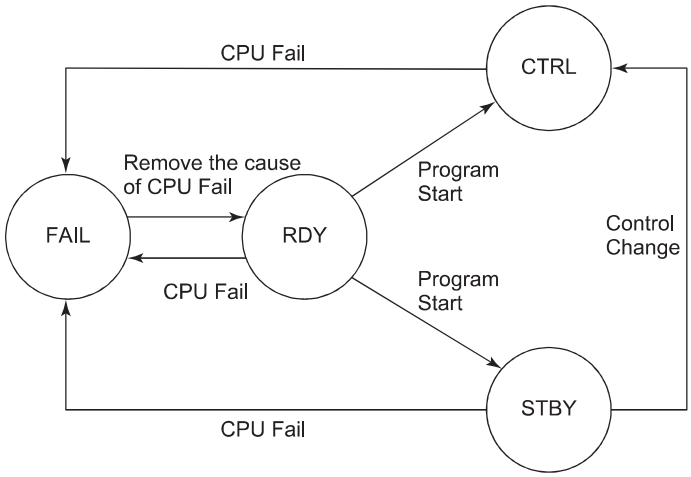


Figure A8.6.2-1 CPU status

FAIL (CPU stopped)

The power is supplied to the CPU, but the software is not running in this status.

RDY (CPU initializing status)

The system program is being set in the main memory in this status.

CTRL (control status)

The system program runs inside the CPU and the CPU has the right to access input/output modules in this status.

STBY (standby status)

The system program runs inside the CPU but the CPU does not have the right to access input/output modules in this status.

CPU status shift in redundant configuration

The figure below illustrates each CPU status and how it may shift in redundant configuration. The thick arrows from (a) to (d) indicate the flow from the startup to normal operation in redundant configuration. Note that the figure below does not represent the status by the mounting positions of the CPUs. Even if the states of the two CPUs are switched, the indication in the figure shows them in the same status.

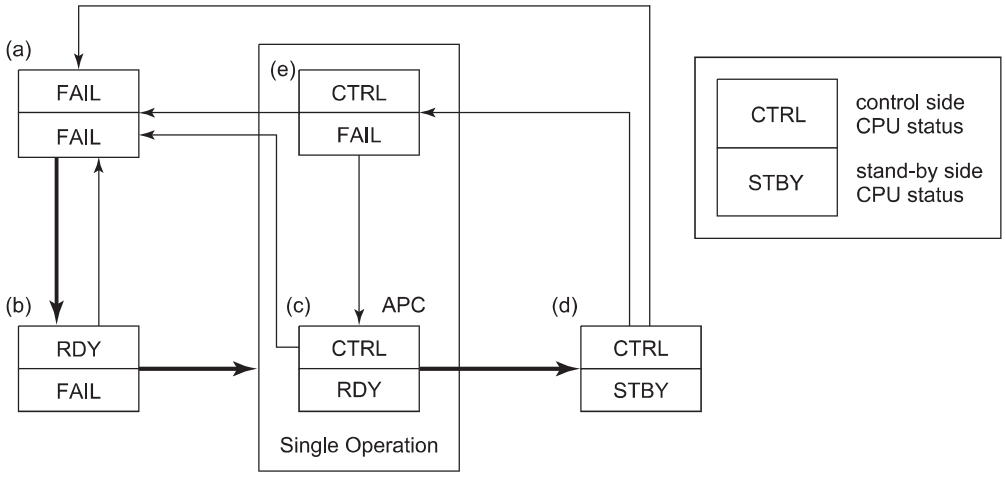


Figure A8.6.2-2 States at redundant configuration

Table A8.6.2-1 CPU status

Status	Description
(a)	CPUs on the both sides stopped.
(b)	The controlling CPU starts up and sets programs and databases in the main memory.
(c) (*1)	The controlling CPU obtains the control right and starts up the standby CPU. Upon launching, the standby CPU copies the image of the main memory of the controlling CPU into its main memory (this status is displayed as "APC" and not the same as status (e)). The controlling CPU executes the user application.
(d)	Both the controlling and standby CPUs operate normally in redundant configuration. This status is called the redundant control status.
(e) (*1)	In this status, the standby CPU is stopped in redundant configuration, or the controlling CPU is stopped and the control right is switched. The same operation as in single configuration is performed.

*1: Single operating status.

The CPU shifts to each status in the following manner.

Table A8.6.2-2 Conditions of CPU status shift

Before	After	Shifting conditions
(a)	(b)	• The power supply to the SCS is started. • SCS offline download is completed. • The system is restarted.
(b)	(c)	The controlling CPU started normally.
(c)	(d)	APC of the standby CPU is completed.
(d)	(e)	The control right is switched due to a failure of the controlling CPU hardware or the standby CPU failed.
(e)	(c)	The standby CPU is replaced or a CPU recovered from transient failure.
(b)	(a)	An error occurred in the self-diagnosis at startup.

Continues on the next page

Table A8.6.2-2 Conditions of CPU status shift (Table continued)

Before	After	Shifting conditions
(c)	(a)	A fatal error occurred while operating in single CPU operation.
(d)	(a)	Power failure occurred in the SCS (including momentary power failure).
(e)	(a)	A fatal error occurred while operating in single CPU operation.

APC status

The APC status refers to the status where the data in the CPU memory is being copied from the control side to the standby side.

The APC status can be checked by the LED on the CPU, the SCS Status Display window of the SENG or the Status Display view on the HIS. The start and end of the APC status are notified via a diagnostic information message.

A8.7 NIU status and security

The N-ESB bus module (S2EN501) that is installed in the node interface unit (NIU) is equipped with a maintenance port.

For the security reason, you should disable the maintenance port when operating the system.

The status of the NIU is determined by the status of the NIU maintenance port and operating mode of the NIU. This section describes the status of the NIU maintenance port, NIU operating mode, and shifting of the NIU status.

Overview of the NIU status and tools

The status of the NIU is determined by the status of the NIU maintenance port and operating mode.

- Status of the NIU Maintenance Port
  The status of the NIU maintenance port can be either enabled or disabled. The status of the maintenance port can be switched between enabled and disabled by using the NIU maintenance port settings tool that is called from the SCS State Management window in the SCS Maintenance Support Tool.
- Operation mode of the NIU
  The NIU operation mode can be either online mode or maintenance mode. The operation mode can be switched between online mode and maintenance mode by using the N-IO maintenance tool in the computer that is connected to the maintenance port.

  The N-IO maintenance tool can be used if the NIU maintenance port is enabled.

IMPORTANT

The Node number setting tool and FieldMate Validator are included in the N-IO maintenance tool.

A8.7.1 Status of the NIU maintenance port

You can run the NIU maintenance port settings tool and enable or disable access from an external device such as a computer connected to the maintenance port of the N-ESB bus module.

Disabled status

The disabled status of the maintenance port prohibits access from the maintenance port.

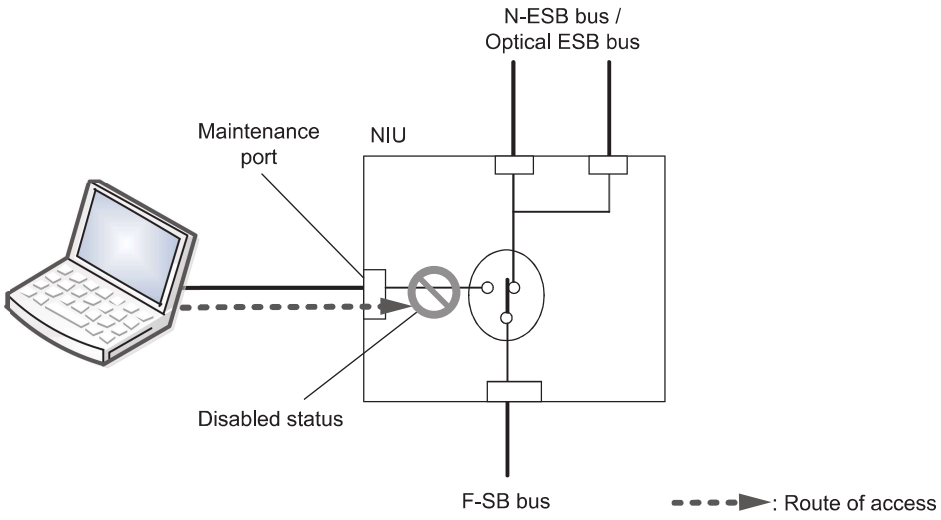


Figure A8.7.1-1 Disabled status of the maintenance port

Enabled status

The enabled status of the maintenance port allows access from the maintenance port.

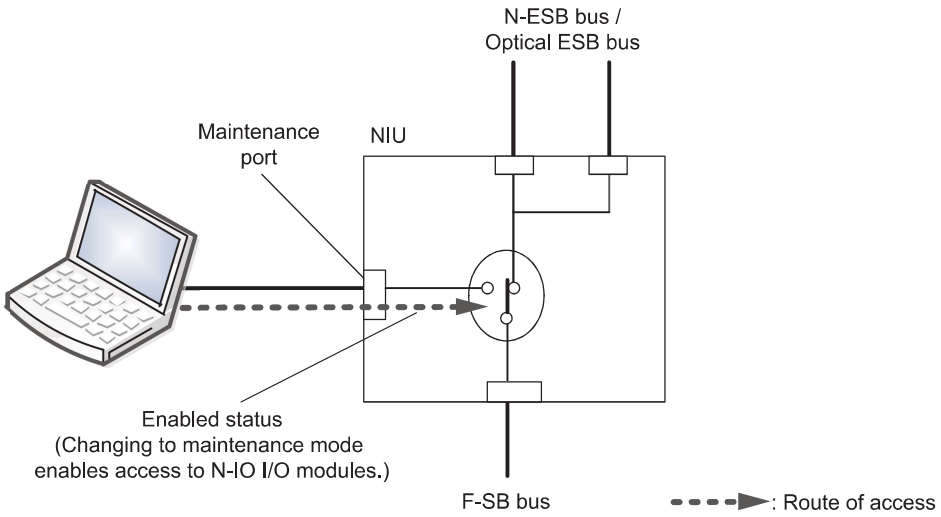


Figure A8.7.1-2 Enabled status of the maintenance port

SEE ALSO For more information about how to enable/disable the maintenance port, refer to:

I4.5, “NIU maintenance port setting tool” on page I4-77

A8.7.2 Operation mode of the NIU

The NIU operation mode can be either online mode or maintenance mode.

Online mode

In online mode, you can access the N-IO I/O modules from the N-ESB bus or the optical ESB bus.

You cannot access the N-IO I/O modules from the maintenance port.

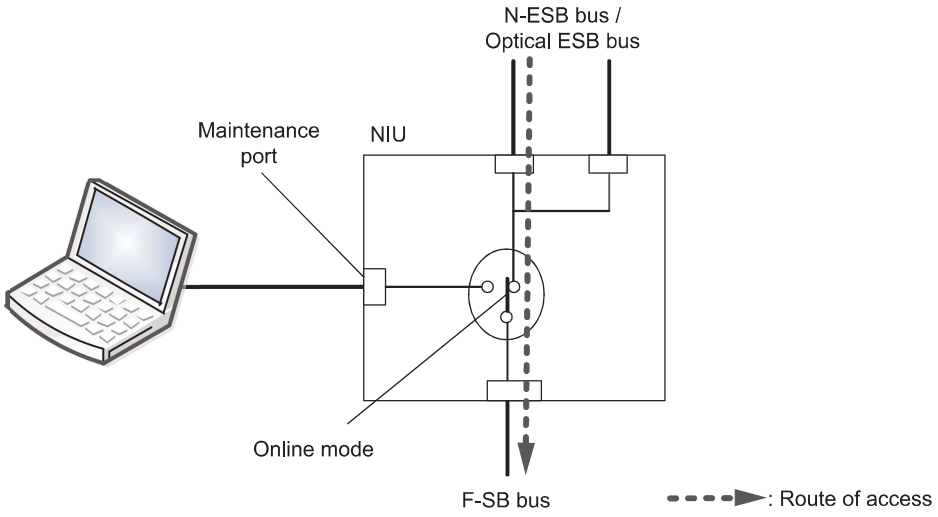


Figure A8.7.2-1 Online mode

Maintenance mode

In maintenance mode, you can access the N-IO I/O modules from the maintenance port.

You cannot access the N-IO I/O modules from the N-ESB bus or the optical ESB bus.

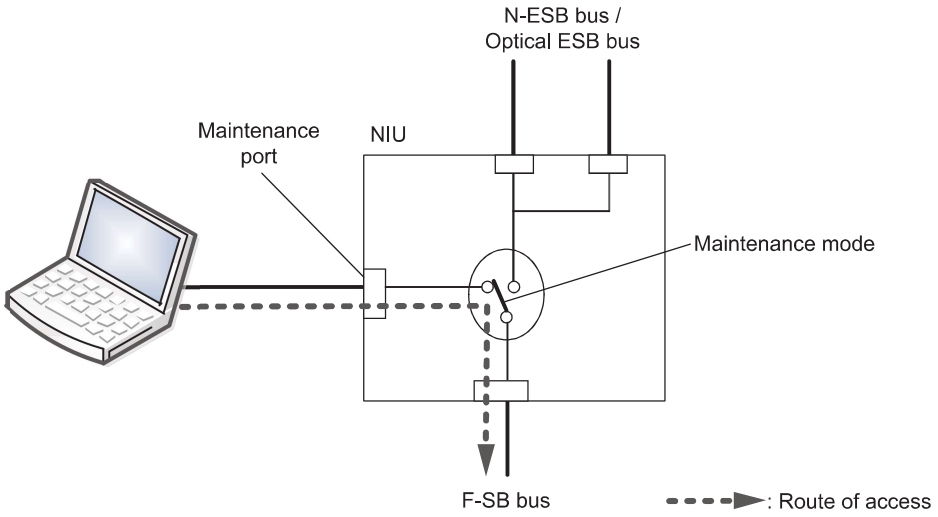


Figure A8.7.2-2 Maintenance mode

Switching between operation modes

This section describes how to switch between the NIU operation modes.

- Switching from the online mode to the maintenance mode

When the maintenance port is enabled, perform the "maintenance instructions" operation from the N-IO maintenance tool connected to the maintenance port to switch from the online mode to the maintenance mode.

- Switching from the maintenance mode to the online mode.
  Perform on of the following to switching from the maintenance mode to the online mode.
  - Perform the "release maintenance instructions" operation from the N-IO maintenance tool connected to the maintenance port.
  - Disconnect the USB cable that is connected to the maintenance port
  - Turn off the power of the NIU, then turn it on

IMPORTANT

When the node number setting tool is used as a N-IO maintenance tool, the unit will switch to the maintenance mode when a node address is configured. After the node address is configured, the unit will switch to the online mode.

TIP

- Switching the maintenance mode of the dual-redundant N-ESB bus modules
  Because the N-ESB bus modules are dual-redundant, when you change the operation mode on one side, the operation mode of the other side will switch accordingly.

SEE ALSO

For more information about Node Number Setting Tool, refer to:

F2.1.1, “Using the Node Number Setting Tool” on page F2-3

For more information about FieldMate Validator, refer to:

Manual of FieldMate Validator

A8.7.3 Shifting the Status of the NIU

The following figure shows the status and the operation mode of the NIU maintenance port, and the status shift with regards to external access.

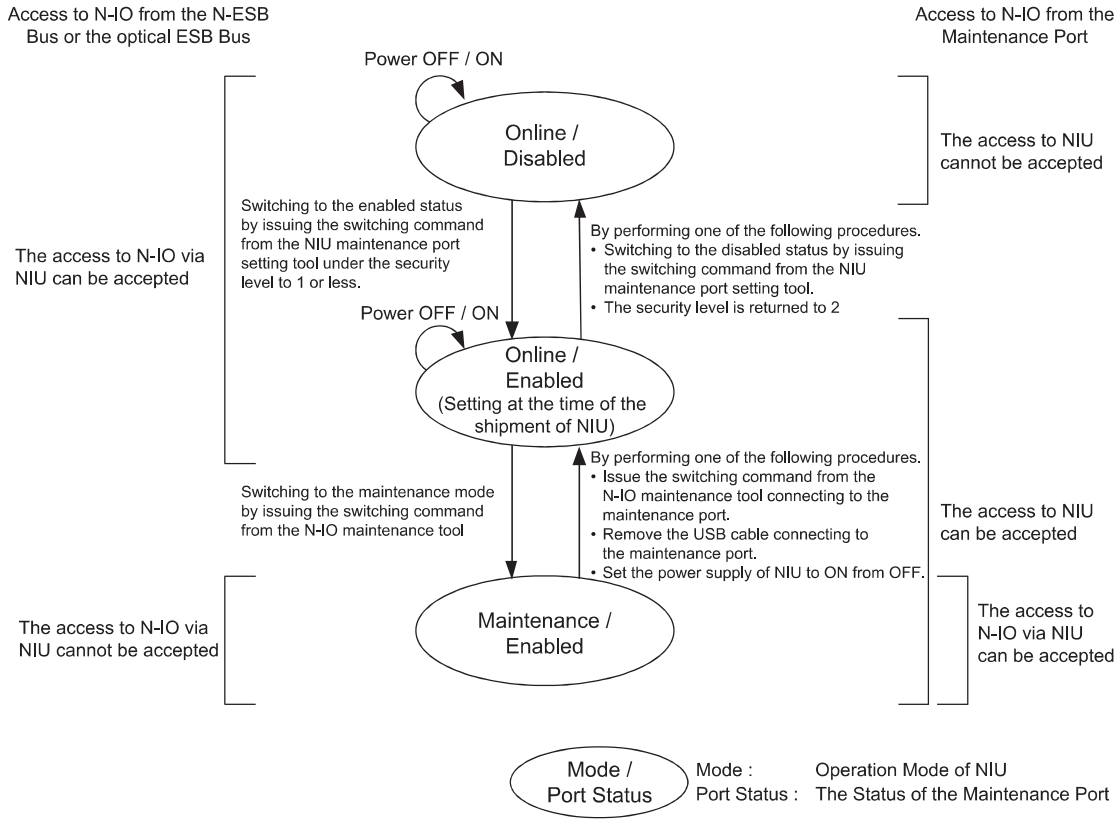


Figure A8.7.3-1 NIU status shift

The following table shows the factory settings of the N-ESB bus modules (S2EN501) that are installed in the NIU.

Table A8.7.3-1 NIU factory settings

Target	Setting	Status
Operation mode	Online mode	The CPU module accesses the N-IO modules from the N-ESB bus and optical ESB bus through the NIU.
Status of the maintenance port	Enable	You can access the NIU from the N-IO maintenance tool.
Node number	Not set	The NIU is not operating correctly. You need to set the node number before connecting to the SCU.

A9. Capacity of SCS applications

This section describes the application capacity related to the SCS.

Table A9-1 Capacity of SCS applications

Types	Items	SCSP3 Max. capacity		SCSL2 Max. capacity	SCSP2 Max. capacity	SCSV1, SCSP1, SCSU1 Max. capacity	Note
		When using N-IO	When using FIO				
I/O	Number of nodes	32	13	13	13	9	CPU node is not included in the number of nodes.
	Number of units	6	-	-	-	-	Maximum 108 units per SCS
	Number of slots	2	8	8	8	8	When connecting I/O node, the maximum slot number of CPU nodes is 6.
	Number of I/O modules	108 non-redundant modules, or 108 pairs of redundant modules	110	110	110	110	The total number of FIO and N-IO I/O modules can be up to 110. However, the total can only be up to 109 when the total number of ESB bus coupler modules and N-ESB bus coupler modules is 4 sets. The number of I/O modules is the number of sets in a redundant configuration and the number of modules in a single configuration. Communication modules are included in the number of FIO I/O modules.
	Number of communication modules	2		2	2	2	For Modbus Slave Communication
		-		-	-	2	For communication as a DNP3 slave (SCSU1 only)
		4		4	4	4	For Subsystem Communication
		8		-	-	-	For safety subsystem communication
	Number of I/O points	1500 (1500 in redundant I/O modules)	1500 (800 in redundant I/O modules)	1500 (800 in redundant I/O modules)	1500 (800 in redundant I/O modules)	1000 (500 in redundant I/O modules)	The numbers are provided only as a guide.
	Number of Subsystem Communication Data	2000 data		2000 data	2000 data	500 data (SCSV1) 2000 data (SCSP1, SCSU1)	Per SCS

Continues on the next page

Table A9-1 Capacity of SCS applications (Table continued)

Types	Items	SCSP3 Max. capacity		SCSL2 Max. capacity	SCSP2 Max. capacity	SCSV1, SCSP1, SCSU1 Max. capacity	Note
		When using N-IO	When using FIO				
I/O	Number of safety subsystem communication data	2000 data		-	-	-	Per SCS The safety subsystem communication I/O area is 4000 words and the minimum unit of data that can be assigned to this area is 2 words. For this reason the maximum number of data is 2000 data. The maximum number of data when only GS01 is connected is approximately 1350 data. (*1)
Application logic	Number of programs and user-defined FU/FB (number of POUs)	Max. 500		Max. 500	Max. 500	Max. 500	When more than 500 POUs are defined, a build error occurs. It may not be possible to define 500 POUs depending on the type and number of FU/FB or LD elements. A restriction may be imposed depending on SCS performance.
	Definable number of variables	1500 I/O variables. 4500 internal variables		1500 I/O variables. 4500 internal variables	1500 I/O variables. 4500 internal variables	1000 I/O variables. 3000 internal variables.	The numbers are provided only as a guide. It may not be possible to define the maximum number of variables shown in the left columns depending on each type of defined variables and the performance of SCS.
Inter-SCS Safety Communication	Send data	200 data		200 data	200 data	200 data	This is the maximum number of send data per SCS.
	Receive data	200 data		200 data	200 data	200 data	This is the maximum number of receive data per SCS.
SCS Link Transmission	Send data	128 data		128 data	128 data	128 data	This is the maximum number of send data per SCS.
	Receive data	1000 data		1000 data	1000 data	1000 data	This is the maximum number of receive data per SCS.

Continues on the next page

Table A9-1 Capacity of SCS applications (Table continued)

Types	Items	SCSP3 Max. capacity		SCSL2 Max. capacity	SCSP2 Max. capacity	SCSV1, SCSP1, SCSU1 Max. capacity	Note
		When using N-IO	When using FIO				
CENTUM integration function and CI Server integration function (*2)	Annunciators (%AN)	2000		2000	2000	1000	-
	Common switches (%SW)	800		800	300	200	All are system switches.
	External Communication FB	(*3)		(*3)	(*3)	(*3) (*4)	-
	External communication FB (with data retaining function)	-		-	-	(*4)	SCSU1 only. The maximum capacity is limited by the size of the area for data retention.
Gas flow rate calculation function	Gas flow rate calculation FB (Total of AGA_*)	-		-	-	1	SCSU1 only
	Report data creation FB (AGA_R)	-		-	-	1	SCSU1 only
Mapping block	Analog input blocks (ANLG_S, ANLGI, HSDTR, GASDTR)	Total 2700		Total 2700	Total 2700 (*5)	Total 1800 (*5) (*6)	-
	Velocity alarm blocks (VEL)						-
	Maintenance override blocks (OVR_*, GOV_*)						OVR_B, OVR_I, OVR_R, OVR_IB, OVR_IR, GOV_B, GOV_IB
	Password blocks (PASSWD)						-
	Manual operation blocks (MOB_*, MOA)						MOB_11, MOB_21, MOB_RS, MOA
	Gas flow rate calculation blocks (AGA_3, AGA_7, AGA_R)	-		-	-		-
	Annunciator blocks (ANN, ANN_FUP)	2000		2000	2000	1000	Mapping to %AN element

Continues on the next page

Table A9-1 Capacity of SCS applications (Table continued)

Types	Items	SCSP3 Max. capacity		SCSL2 Max. capacity	SCSP2 Max. capacity	SCSV1, SCSP1, SCSU1 Max. capacity	Note
		When using N-IO	When using FIO				
Communication I/O area	Overall size of %W	4000 Words		4000 Words	4000 Words	4000 Words	1 Word = 16 Bits
	%W: For mapping (BOOL)	200 Words (3200 Bits)		200 Words (3200 Bits)	200 Words (3200 Bits)	200 Words (3200 Bits)	1 data = 2 words, 100 data
	%W: For mapping (32-bit analog data)	1800 Words		1800 Words	1800 Words	1800 Words	900 data
	%W: For subsystem communication	1000 Words		1000 Words	1000 Words	1000 Words	Up to 2000 data in total of bit data and analog data can be assigned.
	%W: Not used	1000 Words		1000 Words	1000 Words	1000 Words	
Safety subsystem communication I/O area	%X: For safety subsystem communication	4000 Words		-	-	-	1 Word = 16 Bits The minimum unit of data that can be assigned to the safety subsystem communication I/O area is 2 words. For this reason the maximum number of data is 2000 data.
Modbus Slave	Coil	1000 Bits		1000 Bits	1000 Bits	1000 Bits	-
	Input relay	4000 Bits		4000 Bits	4000 Bits	4000 Bits	-
	Input register	4000 Words		4000 Words	4000 Words	4000 Words	1 word = 16 bits, 1 data = 2 words, 2000 data
	Holding register	1000 Words		1000 Words	1000 Words	1000 Words	500 data
SOE	Event	15000 events		15000 events	15000 events	15000 events	Saved in the SOE storage area (RAM)
		Last 1000 events		Last 1000 events	Last 1000 events	Last 1000 events	Saved in the NVRAM (nonvolatile RAM)
	Trip signal file	2 trip signal files of up to 1500 events		2 trip signal files of up to 1500 events	2 trip signal files of up to 1500 events	2 trip signal files of up to 1500 events	Saved in the NVRAM (nonvolatile RAM)
Diagnostic information message	Diagnostic information message	5000 messages		5000 messages	5000 messages	5000 messages	Saved in the area for saving diagnostic information messages (RAM)
		Last 200 messages		Last 200 messages	Last 200 messages	Last 200 messages	Saved in the NVRAM (nonvolatile RAM)
Data buffering	Number of buffers	-		-	-	135000	SCSU1 only
Area for data retention	Size of area for data retention	-		-	-	6 Kbyte	SCSU1 only

*1: Example of when 3 definitions (1 definition of data used with safety communication where the number of data is 2 with 8 words, 2 definitions of data used with an interference-free function where the number of data is 1 with 2 words) are used with

a single GS01. The formula is: (4000 words / 12 words) x 4 data = approximately 1350 data. In this case, the number of GS01 units connected is approximately 300 units (4000 words / 12 words).

*2: The CENTUM integration function can be used with SCS of types SCSP3, SCSL2, SCSP2, SCSP1, and SCSV1. The CI Server integration function can be used with SCS of types SCSP3, SCSP2, SCSP1, and SCSU1.

*3: For SCS other than SCSU1, the maximum capacity can be defined as follows:
- When using Modbus, the maximum definable number of external communication FB is up to 1000 for ECW_B and 500 for ECW_I and ECW_R in combination.
- In tag assignment, up to 3200 Boolean internal variables and ECW_B FB in combination can be defined.
- In tag assignment, up to 900 DINT and REAL internal variables, input variables of IO_REAL and FB of ECW_I and ECW_R in combination can be defined.

*4: For SCSU1, the maximum capacity can be defined as follows:
- When using Modbus, ECW_B and ECWR_B can be defined up to 1000 in total. ECW_I, ECWR_I, ECW_R, and ECWR_R can be defined up to 500 in total.
- Up to 3200 tag names can be defined in total for Boolean internal variables and function blocks of ECW_B and ECWR_B.
- Up to 900 tag names can be defined in total for DINT and REAL internal variables, input variables of IO_REAL, and function blocks of ECW_I, ECWR_I, ECW_R, and ECWR_R.

*5: In CI Server integration, HSDTR, GASDTR, OVR_*, GOV_*, PASSWD, MOB_*, and MOA cannot be used.

*6: For SCSU1, this is the total including AGA_3 or AGA_7 and AGA_R.

A10. Outline of the safety system generation function

This section gives an overview of the tools used to configure and maintain a safety system.
It also describes the different types of applications that can be created by using ProSafe-RS.

A10.1 Engineering method by using the safety system generation function

You can perform ProSafe-RS engineering by using SCS Manager and AD Suite. AD Suite can be largely separated into AD Server, which manages project data, and AD Organizer, which is an engineering tool. Project data is registered and managed in AD Server.

SEE ALSO For more information about AD Suite, refer to:

A., “Overview of Automation Design Suite” in Engineer's Reference Manual (IM 32P04B10-01EN)

Guidelines for selecting an engineering method

There are two engineering methods for ProSafe-RS: I/O list engineering and RS original engineering. They are each defined as follows:

- I/O list engineering
  The safety I/O list is loaded to AD Organizer and the data is engineered by using the I/O List Engineering Package.

  When using iDefine and when performing engineering for safety subsystem communication, select I/O list engineering.

- RS original engineering
  This method is performed without using the I/O List Engineering Package. The engineering tools of SCS Manager are used.

  If RS projects, including SCS projects, are registered in AD Server, the history management function of AD Suite can be used.

Select the appropriate engineering method depending on whether you are using the I/O List Engineering Package. The engineering method can only be selected when creating a new SCS project. You cannot change the engineering method later.

TIP If you upgrade to version R4, the metered license is applied regardless of the engineering method that you select.

SEE ALSO For more information about SCS project and RS project, refer to:

C1.1, “Type of project” on page C1-2

Precautions when using RS projects that were created before introducing AD Suite

In AD Server, we recommend that you register SCS projects that were created before introducing AD Suite. In this user’s manual, descriptions about RS original engineering are explained with the assumption that RS projects have been registered to AD Server. If you use SCS projects that have not been registered in AD Server, you will not be able to use the AD Suite functions described in this user’s manual.

A10.2 SCS Manager

You can call SCS Manager from AD Organizer. You can create a new SCS project by using SCS Manager and call the SCS engineering and maintenance tools.

From the [Tools] menu of SCS Manager, three launchers can be started.

From each launcher, various engineering functions such as builders, SCS related tools and SCS Maintenance Support Tool can be launched. This section mainly explains the precautions when closing and opening SCS projects and launchers started from SCS Manager.

Precautions when opening SCS projects

IMPORTANT

SCS projects cannot be opened if you cancelled password input (except when read-only access is permitted without entering a password) or failed to enter the correct password three times while attempting to open SCS projects for which passwords are set. Close SCS Manager and try opening it again.

Projects that have not been created as databases to be edited in SCS Manager of ProSafe-RS cannot be opened.

It is not possible to open the same SCS project in SCS Manager, Version Control Tool and Master Database Restoring Function at the same time.

Precautions when closing SCS projects

This section describes the precautions when closing SCS Manager.

- Closing SCS Manager closes the currently opened SCS project.
- When you close SCS Manager, all the related builders, Safety Analyzer and launchers close. If the security level is not Level 2 when closing, a message prompting the user to return to Level 2 appears. Set the SCS's security level to Level 2 by using the SCS Security Level Management Function.
- SCS Maintenance Support Tool is not closed even if SCS Manager is closed.

TIP

The SCS project opened in SCS Manager cannot be opened in Version Control Tool or Master Database Restoring Function. To use these tools, close SCS Manager.

SEE ALSO

For more information about how to operate the SCS security level operation function, refer to:

B3., "Security of SCS" in ProSafe-RS User's Guide (IM 32P01B10-01EN)

Starting and closing launchers

From the [Tools] menu of SCS Manager, the following three launchers can be started.

- [Engineering]
  Starts the Engineering launcher such as builders.
- [Controller]
  Starts the SCS launcher.
- [Maintenance]
  Starts the Maintenance launcher.

TIP The menu items for starting launchers are also displayed in the pop-up menu opened by right-clicking when a configuration and/or resource are selected in SCS Manager or Dictionary View is opened.

Starting launchers

Each launcher is started from the [Tools] menu. If the same launcher has already been started, a new launcher is not started; instead, the already started launcher is displayed on the foreground and given the focus.

The Engineering launcher and the Maintenance launcher have a push-pin icon. If you place the push-pin icon in the pressed status, the corresponding launcher is always displayed on the foreground without being hidden by other windows. If you disable the push-pin icon, the launcher may be hidden by other windows.

The Controller launcher is always displayed on the foreground.

If two or more launchers are set to be displayed on the foreground, the launcher started up later is displayed on the foreground.

Closing launchers

Each launcher is closed if you click "Close" button of the launcher or close SCS Manager. If you close a launcher by clicking "Close" button, only the launcher is closed and windows opened from the launcher are not closed.
The Controller launcher closes if a menu is selected and the corresponding tool is started.

Engineering launcher

The table below shows builders and tools that can be started from the Engineering launcher.

Table A10.2-1 Engineering launcher menu

Menu item	Operation
SCS Project Properties	Opens the SCS Project Properties dialog box
SCS Constants Builder	Starts SCS Constants Builder
I/O Parameter Builder	Starts I/O Parameter Builder
Communication I/O Builder	Starts Communication I/O Builder
SCS Link Transmission Builder	Starts SCS Link Transmission Builder
Modbus Address Builder	Starts Modbus Address Builder
DNP3 Communication Builder (*1)	Starts DNP3 Communication Builder
Tag Name Builder (*2)	Starts Tag Name Builder
Alarm Priority Builder (*2)	Starts Alarm Priority Builder
Alarm Processing Table Builder (*2)	Starts Alarm Processing Table Builder
Integrity Analyzer	Starts Integrity Analyzer
Cross Reference Analyzer	Starts Cross Reference Analyzer
Database Validity Check	Starts Database Validity Check Tool
SCS Information	Opens the SCS Information dialog box

*1: DNP3 Communication Builder is displayed only for the SCS projects of SCSU1 that are created by the software version R3.02.20 or later.
*2: Only opened in the case of CENTUM integration structures.

If a library project is open in SCS Manager, only the [SCS Project Properties] and [Integrity Analyzer] menu items are displayed.

Controller launcher

The table below shows tools that can be started from the Controller launcher.

Table A10.2-2 Controller Launcher Menu

Menu item		Operation
Save Operation Marks (*1)		Save the operation marks set on CENTUM HIS to SENG
Download Operation Marks (*1)		Download the saved operation marks to SCS
Reset SCS	Restart SCS	Restarts an SCS
	Master Database Offline Download	Performs master database offline download

*1: Only opened in the case of CENTUM integration structures.

If a library project is open in SCS Manager, the Controller launcher cannot be started.

Maintenance launcher

The table below shows tools that can be started from the Maintenance launcher.

Table A10.2-3 Maintenance launcher menu

Menu item	Operation
SCS Status Overview	Starts the SCS Status Overview of SCS Maintenance Support Tool
SCS State Management	Starts the SCS State Management of SCS Maintenance Support Tool
Set SCS Security Level	Opens the Set SCS Security Level dialog box.
I/O Lock Window	Starts the I/O Lock Window
Communication I/O Lock Window	Starts the Communication I/O Lock Window
SCS Link Transmission Lock Window	Starts SCS Link Transmission Lock Window
Inter-SCS Communication Lock Window	Starts Inter-SCS Communication Lock Window
SCS Test Function (*1)	Starts SCS Test Function
Update SCS Test Database (*1)	Updates SCS Test Database

*1: In the case of CENTUM integration structures, this menu item is displayed when the SCS project is a default project or a user-defined project.

If a library project is open in SCS Manager, the Maintenance launcher cannot be started.

IMPORTANT

If SCS Manager is in the logic simulation mode, the I/O Lock window, Communication I/O Lock window, SCS Link Transmission Lock window, and Inter-SCS Communication Lock window cannot be started.

Show/hide SCS Manager toolbars

If you launch SCS Manager or Multi-Language Editor, the displayed toolbar will be the same as that before, when you closed last time. The toolbar display is retained per each Safety Engineering PC (SENG) and cannot be set per each user. If you hid the toolbar last time you used the SCS Manager or Multi-Language Editor and if you want the toolbar to show this time, for example, change the show/hide status of the toolbar.

Follow the steps below to show or hide the toolbar.

1. On the [Options] menu, click [Layout].
   The Layout dialog box appears.

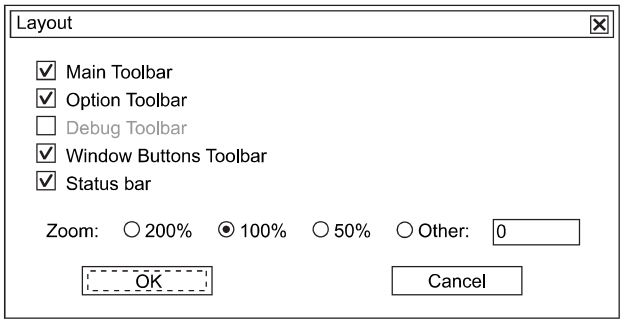


Figure A10.2-1 Layout dialog box

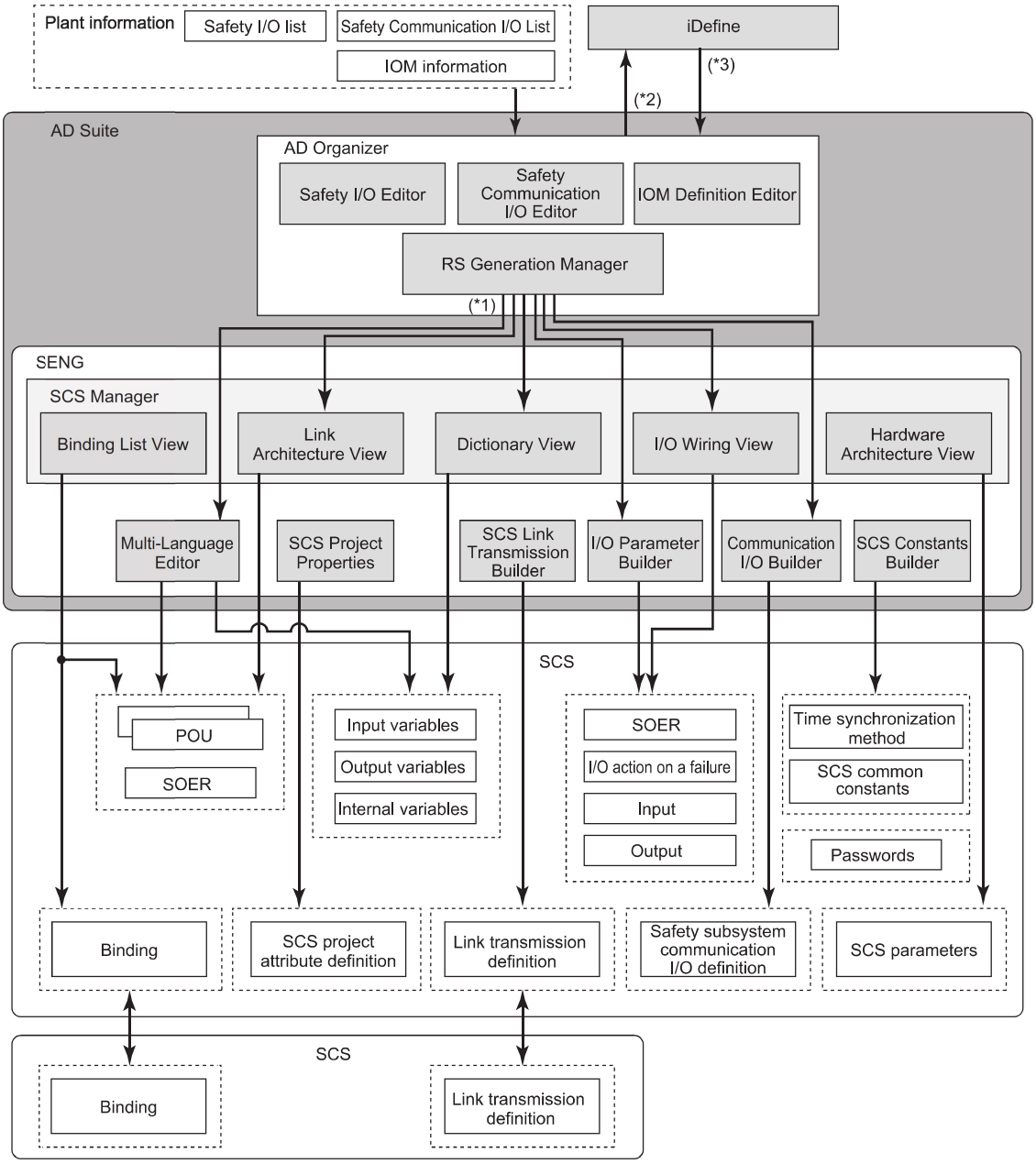
2. Select the check boxes of the toolbar you want to show.
   If you want to hide the toolbar, clear all the check boxes.
3. Click [OK].
   To change the docking or floating status of the toolbar, drag it to the position you like.

A10.3 Safety application definition

Safety applications are created with tools and builders called from the AD Organizer and the SCS Manager.

When using AD Suite to perform I/O list engineering, you need to use the editors in AD Organizer to set the items instead of using I/O Wiring View, I/O Parameter Builder, and Communication I/O Builder.

If you select I/O list engineering and use iDefine, you can create the application logic by using iDefine based on the ProSafe-RS I/O file that was exported from AD Organizer. The ProSafe-RS I/O file is a file generated for engineering with iDefine based on the safety I/O list, safety communication I/O list, and IOM definition.



*1 : In the case of I/O list engineering, you can reflect the safety I/O list, safety communication I/O list, and IOM definition to the SCS Manager builder by running the reflection process through RS Generation Manager. If you run the reflection process on the engineering data that was created by using iDefine through RS Generation Manager, the application data can be reflected to the Multi-Language Editor and SCS.

*2 : AD Organizer exports the data that was created from the safety I/O list, safety communication I/O list, and IOM definition to iDefine.

*3 : AD Organizer imports the engineering data that was created by using iDefine.

Figure A10.3-1 Overview of safety application definition

AD Organizer

AD Organizer is installed in the SENG computer. You can perform the ProSafe-RS engineering by using AD Organizer. AD Organizer comes with some built-in engineering tools, and SCS Manager is one of them.

Safety I/O Editor

This is an engineering tool that can be used from AD Organizer.

The tool is used to create safety I/O lists based on plant information data and import them as engineering data.

It is also used to define variables that are related to the safety I/O. You specify the SCS node and IOM applicable to the P&ID tag and the associated connection information based on the information that is displayed in the Safety I/O Editor.

With this editor, you can export a file containing data for engineering with iDefine.

Safety Communication I/O Editor

This is an engineering tool that can be used from AD Organizer.

This tool is used to create safety communication I/O lists based on plant information data and import them as engineering data.

It is also used to define variables that are related to the safety communication I/O. You specify the SCS node and IOM applicable to the P&ID tag and the associated connection information based on the information that is displayed in Safety Communication I/O Editor.

With this editor, you can export a file containing data for engineering with iDefine.

IOM Definition Editor

This is an engineering tool that can be started from AD Organizer.

In the IOM Definition Editor, a list of nodes and I/O modules are displayed with their properties.

You can use the IOM Definition Editor to define the I/O module configuration and set the properties of nodes and I/O modules. If I/O module assignment information is not defined in the safety I/O list or safety communication I/O list, you can define the assignment of I/O modules to nodes by using IOM Definition Editor.

ADMDB

This is the server database that stores all the engineering data that is included in the AD Server. The revision history of the engineering data and the hardware configuration information are also stored in this database.

The AD Server manages the engineering data.

Generation Manager

For SCS projects that are created with I/O list engineering, Generation Manager reflects the information of the safety I/O lists, safety communication I/O lists, and I/O module configuration and builds SCS projects.

SCS Manager

This is installed in the computer of SENG. It is an environment for creating application logic.

Hardware Architecture View

- Set the configuration name.

- Define the IP address of the SCS.

Link Architecture View

- Configuring the security settings of the SCS project.
- Defining the POU.(*1)
- Adding variable groups.
- Starting the Multi-Language Editor to edit the POU that you have defined.

*1: POU: Program Organization Unit It is a generic term for the programs, function blocks (FB), and functions (FU) that are written with the function block diagram (FBD) and ladder diagram (LD)

SCS Project Properties

Defining Project properties including station type, domain number, and station number of SCS.

Designating location of the integrated CENTUM project folder, in the case of CENTUM Integration Configuration.

SCS Constants Builder

Setting SCS common constants and time synchronization method.

Dictionary View

If you select the RS original engineering method, the Dictionary View is used to set the parameters of FUs and FBs and define project variables. If you select the I/O list engineering method, the variables that were defined by using AD Organizer and iDefine are read-only in Dictionary View.

Multi-Language Editor

Edit the POUs for the LBD, LD, and ST.

POUs that were defined by using iDefine are read-only in Multi-Language Editor.

Binding List View

Binding variables from the producer to the consumer of Inter-SCS safety communication.

SCS Link Transmission Builder

Defining SCS link transmission safety communication and SCS global switch communication.

I/O Wiring View

In the SCS project where the RS original engineering method is selected, the I/O Wiring View is used to define the following:

- Analog I/O module, digital I/O module, universal type I/O module (these three types of modules are collectively called "AIO/DIO modules"), and communication module
- Wiring between I/O module channels and I/O variables

If you select I/O list engineering, this builder is read-only.

I/O Parameter Builder

In the SCS project where the RS original engineering method is selected, I/O Parameter Builder is used to configure the node, module, and channel parameters, including the settings for the operation when a fault is detected in an I/O module or channel, and to define SOER collection through DI/DO.

If you select I/O list engineering, this builder is read-only.

- ### Communication I/O Builder

  For SCS projects for which I/O list engineering is selected, this builder becomes read-only. Use Safety Communication I/O Editor when you assign communication I/O data for safety subsystem communication and perform wiring of communication I/O variables. The contents of Safety Communication I/O Editor will be reflected in this builder by running a reflection from AD Organizer.

iDefine

iDefine is an external engineering tool. Using iDefine, you can create application logic based on data such as the safety I/O list, safety communication I/O list, and IOM information obtained from AD Organizer.

Once data related to the application logic that was created using iDefine is exported to a file and then imported using AD Organizer, the content can be reflected in SCS Manager by using RS Generation Manager.

The safety I/O list, safety communication I/O list, and IOM information created with AD Organizer are read-only in iDefine.

The engineering data that were created in iDefine and reflected in SCS Manager are read-only in SCS Manager.

A10.4 CENTUM integration application definition

The following figure shows the outline of CENTUM integration application definition and the associated builders.

These builders are opened from the engineering launcher of the SCS Manager.

- Tag Name Builder
  This builder defines tag names for FBs and variables which can be used for CENTUM Integration Configuration, and also defines annunciator messages.

  Defining a tag name results in the creation of a mapping block for CENTUM Integration Configuration.

  When engineering by using iDefine, you can also define the tag names for FBs and variables by using iDefine. Use the reflection process from Generation Manager to reflect the definitions in Tag Name Builder. Tag names that were defined by iDefine are read-only in Tag Name Builder.
- Alarm Priority Builder
  This builder defines alarm priority. The condition of alarm activation is set to each alarm priority as in CENTUM.
- Alarm Processing Table Builder
  The Alarm Processing Table Builder is used to import the ‘Alarm Processing Table defined in CENTUM’ to SCS project.

  This table determines the priority of process alarms that are generated from mapping blocks when integrating with CENTUM.

When engineering by using iDefine, you can also configure the tag names in iDefine. The tag names are read-only except for configured tools.

In a CENTUM integration structure, the application of ProSafe-RS needs to be defined with those builders. Furthermore, engineering of CENTUM including SCS definition and tag list generation needs to be executed on CENTUM ENG. This allows HIS to access SCS data with a tag name and to display annunciator messages.

The following figure provides an overview of CENTUM Integration Application Definition.

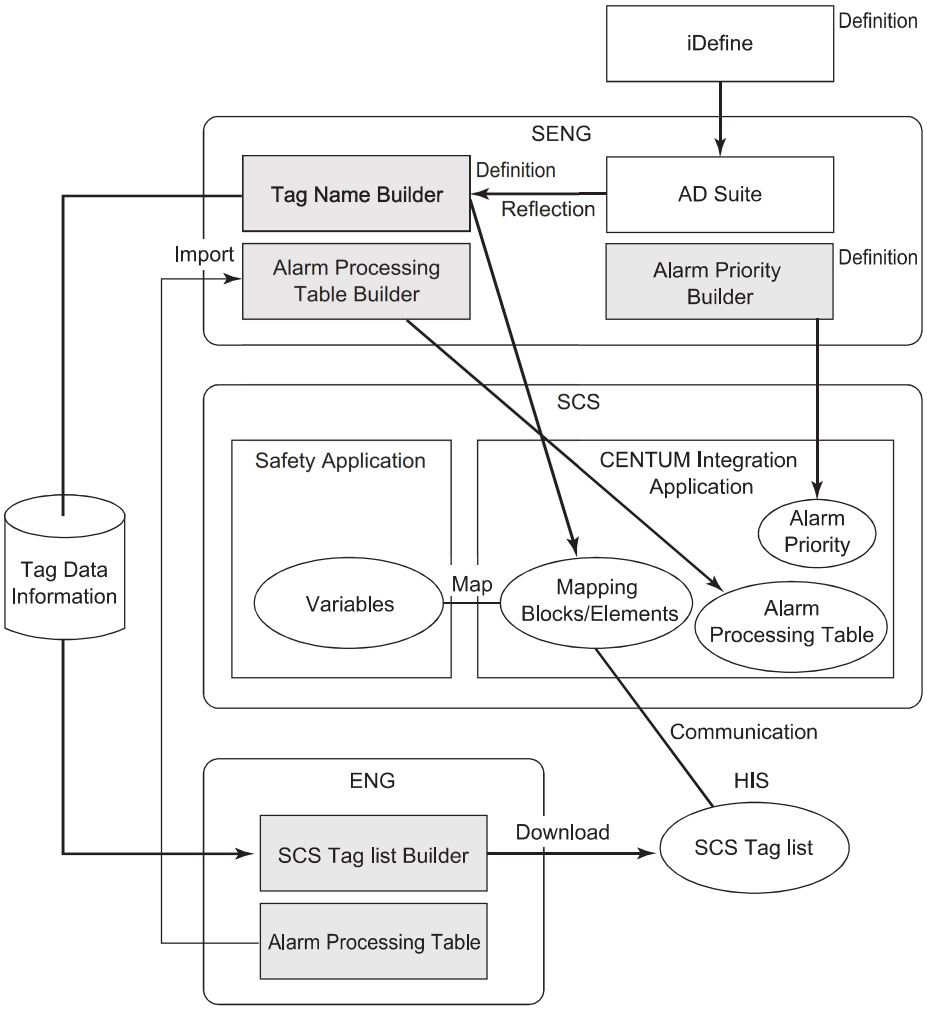


Figure A10.4-1 Outline of CENTUM Integration Application Definition

A10.5 Defining applications that use communication modules

In ProSafe-RS, you can create an application that exchanges data with other system through a communication module. Modbus slave communication, Modbus subsystem communication, and safety subsystem communication are supported. Safety subsystem communication can be used with SCSP3 only. In addition, you can create DNP3 communication applications in SCSU1. Modbus slave communication and Modbus subsystem communication are interference-free functions. Safety communication is included in safety subsystem communication.

The following builder is used for Modbus slave communication:

- Modbus Address Builder
  It defines the Modbus device address.

The following figure shows the outline of the definitions of Modbus slave communication application.

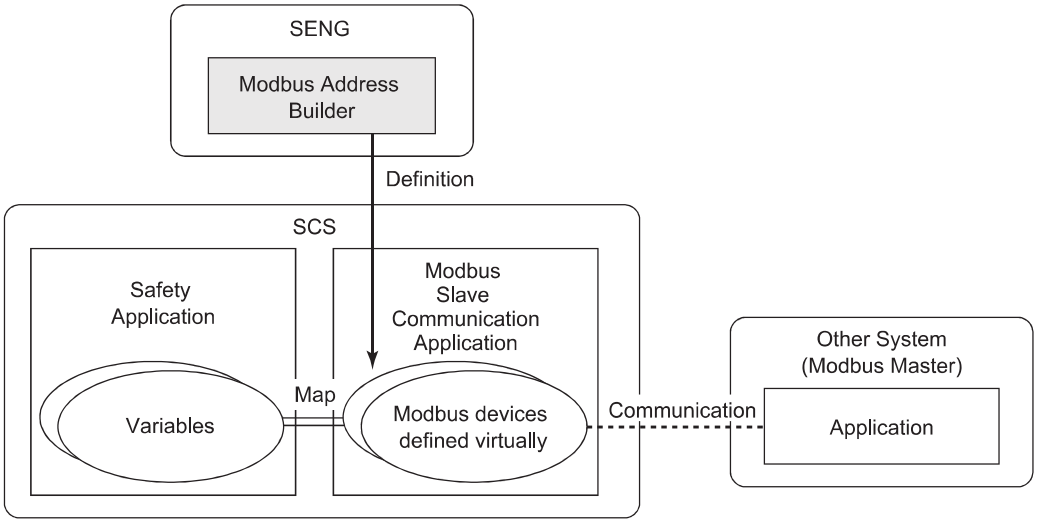


Figure A10.5-1 Outline of Modbus slave communication application definition

The following builder or editor is used for subsystem communication:

- Communication I/O Builder (for RS original engineering)
- Safety Communication I/O Editor of AD Organizer (for I/O list engineering)
  It defines the communication data, and allocates the communication I/O FB there.

The following two types of subsystem communication are supported:

- Using the serial communication module, you can create an application for subsystem communication between SCS and Modbus PLC. By creating an application for subsystem communication between SCS and ProSafe-SLS, you can acquire events and data of ProSafe-SLS.
- Using Ethernet communication module, you can create an application for the subsystem communication between the SCS and Modbus/TCP PLC.

The following editor is used for fire and gas communication:

- Safety Communication I/O Editor of AD Organizer
  Define communication data and assign the PROFINET communication I/O FB and fire and gas communication FB to the communication data.

  Using fire and gas communication modules, you can create an application for safety subsystem communication between the SCS and fire and gas devices.

The following builder is used to define DNP3 communication applications:

- DNP3 Communication Builder
  This builder enables SCS to act as a DNP3 slave station and associates DNP3 data with application logic variables.

The following figure shows the outline of the DNP3 communication application definitions.

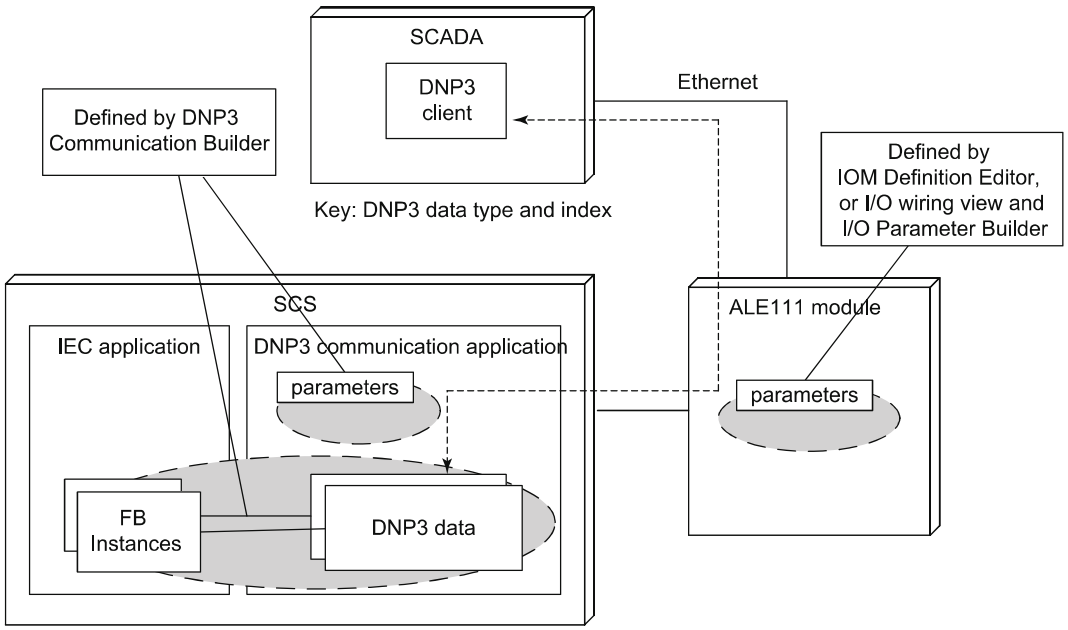


Figure A10.5-2 Outline of DNP3 communication application definition

A10.6 CI Server integration application definition

The following describes the builder and outline of the CI Server integration application definitions. CI Server integration is an interference-free function.

In CI Server integration, you can define I/O modules and create function blocks in addition to using the following builders and tools:

- Domain Properties Setting Tool
  It selects the operating mode of Vnet/IP-Upstream.
- Message Cache Tool
  A group is defined when the network configuration of Vnet/IP-Upstream is in the narrow-band mode.
- Tag Name Builder
  You can enter tag name, and other information to the data to be handled in CI Server.

  When engineering by using iDefine, you can also define the tag names for FBs and variables by using iDefine. Use the reflection process from Generation Manager to reflect the definitions in Tag Name Builder. Tag names that were configured by using iDefine are read-only in Tag Name Builder.

A10.7 Engineering tools

The following describes the tools that are used after you have created a ProSafe-RS application:

Integrity Analyzer

The Integrity Analyzer is used to analyze the safety of existing created application logics. It detects unauthorized FB /FU as the safety function, and outputs results of analyzing on screen or on the analysis report.

Cross Reference Analyzer

It shows, on screen or on the analysis report, the difference between the application previously downloaded (which runs currently on SCS) and the application to be downloaded soon as well as the extent of impact in case of downloading. The Cross Reference Analyzer is for limiting the scope of retesting when application logic is modified.

Self-Documentation function

This is for printing user applications. The entire definitions of an SCS project or any parts can be selected as a printed item.

Project Attribute Tool

This tool can be used to display the attribute of an SCS project.

Test Project Creation Tool

This tool can be used to copy a project that is running at a plant site and create a project for test purpose.

Import/Export function

Import or export functions can be used to import or export SCS project data. Therefore, these data can be used for test functions or for reusing applications.

Project Comparing Tool

This tool can be used to detect the difference between two specified SCS projects and to display and print the result.

Version Control Tool

This is for controlling the version history of an SCS project to support the project updates by users.

By using Version Control Tool, you can save (check-in) the project data of an SCS project at a certain point upon adding a version number and restore (check-out) project data of a certain version. If you are performing I/O list engineering, start this tool from AD Organizer. If you start it from the Start menu, the data of AD Suite cannot be handled by the tool.

SEE ALSO For more information about precautions for handling an SCS project engineered by I/O list engineering that was checked in with Version Control Tool of a revision earlier than R4.03.10, refer to:

"■ Precautions for handling an SCS project that was checked in with Version Control Tool of a revision earlier than R4.03.10" on page C3-2

Master Database Restoring Function

This function is used to restore the contents of the master database as the work database. Use this function to discard changes made to the work database and use the master database as the data subject to engineering (work database). If you are performing I/O list engineering, start this tool from AD Organizer. If you start it from the Start menu, the data of AD Suite cannot be handled by the tool.

SEE ALSO For more information about precautions for restoring an SCS project that was generated by RS generation with AD Organizer of a revision earlier than R4.03.10, refer to:

"■ Precautions for restoring an SCS project that was generated by RS generation with AD Organizer of a revision earlier than R4.03.10" on page C3-2

Database Validity Check Tool

The Database Validity Check Tool is used to check the integrity of the database in the work database and master database of SCS project, and SCS database in SCS. The master database can be repaired if the master database has lost validity due to such as an error that has occurred during online change download. This repair function of the tool repairs the master database by replacing it with the work database.

SCS Information

This function is used to display and print SCS project usage conditions such as POUs used within the SCS and the number of variables. The number of licenses available is displayed separately for SIL 2 and SIL 3. This function can also be used to check the database revisions in the SCS project, number of project I/O licenses and their usage. You need to build an SCS project before using this function.

B. Designing applications

In the basic design of ProSafe-RS system configuration, you must consider the safety functions, architecture, installation method, and field I/O devices of the systems, as well as the management of documents and software.

B1. Key points of basic design

Having a proper basic design is very important for designing and building a safety instrumented system.

This section explains the important points to be considered for the basic design.

When the user has set a requirement for the safety integrity level (SIL), the requirement should be reviewed before calculating the PFD (Probability of Failure on Demand) of each safety loop in order to create a basic design that meets the required SIL.

Independence of safety instrumented system and process control system function

Establish independence of safety functions in a ProSafe-RS system and of control functions in a Process control system such as DCS.

Safety function and safety integrity

Consider the following items for Safety Function and Safety Integrity.

- Whether Redundancy for ProSafe-RS is needed or not (CPU and I/O modules)
- The failure rate of each component comprising the safety loop (Sensors, transmitters, relays, logic solver and final elements)
- Requirements for SIL and PFD value of a loop
- Interval between proof tests
- The possibility to easily perform validity check and proof tests for the applied system

Safety applications that can be used in ProSafe-RS

The ProSafe-RS system can primarily be used for the following applications.

- Emergency Shutdown System (ESD)
- Fire and Gas System (FGS)
- Burner Management System (BMS)

ProSafe-RS is capable of handling both applications configured of a combination of a NC (Normally-Closed) input and a DTS (De-energized-To-Safe) output and applications configured of a combination of a NO (Normally-Open) input and an ETS (Energized-To-Safe) output.

Architecture (basic functions)

Consider the following items for Architecture.

- Choice of “Normally Open (NO)” or “Normally Close (NC)”
- Choice of "Energized-to-Safe state principle (ETS)" or "De-energized-to-Safe state principle (DTS)"

IMPORTANT

It is recommended that SCS be separated into two SCSs. : One SCS with applications comprised of NC inputs and DTS outputs are performed. The other SCS with applications comprised of NO inputs and ETS outputs are performed.

- Redundant structure of safety loops
- Actions under fault conditions
- Safety time and scan period for process
- Requirements for Sequence Of Event Recorder (SOER) Data Collection and Time Synchronization System
- Man Machine Interface
- Requirements for each communication line
- Consideration for maintenance
- Maintenance override and bypass

Power supply and grounding

See and follow the ProSafe-RS Installation Guidance for installation.

SEE ALSO

For more information about power supply and grounding for SCS that supports SIL 3, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

For more information about power supply and grounding for SCS that supports SIL 2, refer to:

ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

Common cause failure

Consider the distribution of functions of the ProSafe-RS system in order to deal with common cause failures.

Field input devices (sensors, transmitters and signal converters)

Consider the following items for field input devices:

- Number of points for each signal type (DI or AI)
- Independence from control system
- Process parameter in normal operation and trip point
- Redundancy of input devices: 1oo1, 1oo2, 2oo3 and 2oo4
- Failure rate of input devices, especially the dangerous failure rate
- Whether Wiring Check is needed or not

Field output devices (actuator, solenoid valve, shutdown valve, etc.)

Consider the following items for field output devices:

- Number of points for each signal type.(DO or AO, voltage value and current value separately)
- Independence from control system
- Choice of Actuator and final element, and their speed of actions (Open direction and Close direction)
- Redundancy of actuators and final elements
- Considering the case of using relay output
- Failure rate of actuators and final elements, especially the dangerous failure rate

- Whether Wiring Check is needed or not

Man machine interface

Consider the following items for the Man Machine Interface.

- For Operator Interface
  - Screens such as CRT and LCD
  - Annunciators:
    size of display/actions/colors/sounds
  - Switches and lamps for a monitoring board
  - Print items of a printer
- Manual shutdown
- Reset function on recovery
- Interface for maintenance and engineering
  - Configuration definition of system hardware
  - Building application logics and downloading them to SCS
  - Modification, testing and monitoring of the application logics
  - Maintenance override
  - Monitoring system status of SCS and diagnostic information
  - Controlling SCS security level
  - SOER

Management for design documents and software

Consider the following items.

- Print and storage management of design documents
- Management of changes for hardware and software

TIP

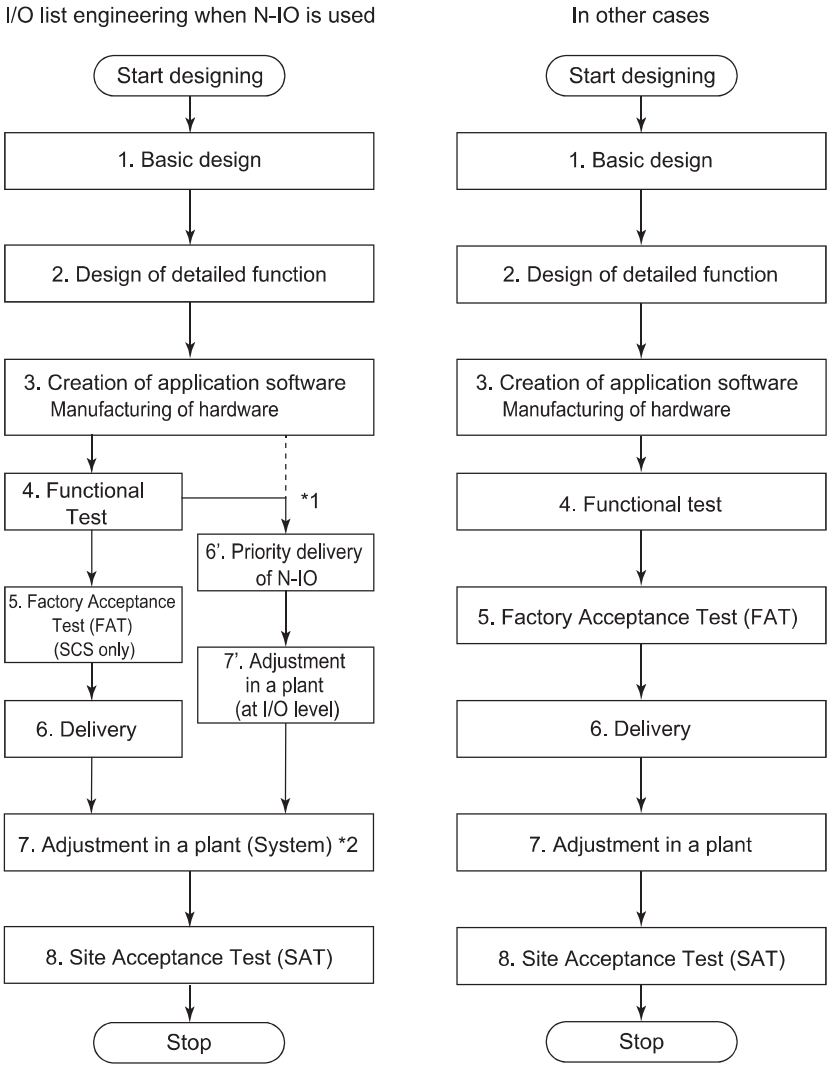
If you use iDefine, you can use the functional safety management (FSM) function of iDefine.

B2. Procedure for engineering

The regular engineering procedures from design to actually starting the operation, including production, inspection and commissioning, vary depending on the engineering method that you select and the type of nodes to be used.

If you are using N-IO and you have selected I/O list engineering, you can ship the N-IO before SCU. In the shipping destination, you can perform loop check between the N-IO and field devices first. The entire system is calibrated after the SCU has reached the shipping destination.

In all other cases, engineered SCUs and I/Os are shipped at the same time.



*1: You can flexibly decide the timing of priority delivery in a range from step 3 to 5 depending on the customer's request.
*2: Perform the remaining functional test items.

Figure B2-1 Procedure for engineering

1. In Basic Design, the following items should be decided based on user's requirements and specifications.
   - The making of safety specification
   - System configuration and hardware
   - The number of I/Os

- Safety Integrity Level (SIL) of loops
- Signal interface with another system

The following documents are made as a result of these work.

- Diagrams of the system structure
- Hardware specifications
- System basic design document
- Safety I/O list
- Safety communication I/O list
- List of interfaces with other systems (items not included in the safety communication I/O list)

2. Prepare a functional specifications document based on the user's requirements and specifications. Detailed logics such as shutdown logic and others are included in the functional specifications.
3. Create ProSafe-RS projects and applications on a computer installed with the SENG function. The hardware is also manufactured.

IMPORTANT

When prioritizing the N-IO delivery, you can flexibly decide the priority delivery timing in a range from step 3 to 5 depending on the customer's request.

4. Functions of the created application are checked. After making a document about the Test Specification, usually testing of functions is conducted in the following order.

   (1) Desk test

   The created applications are checked with self documents on the desk.

   ↓

   (2) Unit test-1

   Verify the created logic operations. You can use the SCS simulation test and logic simulation test environments on the computer for verification.

   ↓

   (3) Unit test-2

   In the target test using SCS, the overall logic etc. are verified.

   ↓

   (4) Integration test

   The integrated final test is conducted on the SCS target. Before the test, it is required to provide an environment, where SCS can be used, in combination with panel, console, a host computer and other subsystems. The testing for system failure such as hardware failure is also conducted.
5. Conduct the hardware and software Factory Acceptance Test (FAT) in the presence of the user. When prioritizing N-IO delivery, perform the Factory Acceptance Test (FAT) only for the SCS.

6'. When prioritizing N-IO delivery, deliver the N-IO hardware.

6. Deliver the hardware and software after they are confirmed by the users during FAT.

7'. When prioritizing N-IO delivery, calibrate the N-IO hardware that is installed on site.

7. Adjust the hardware and software that are installed on site through the system. When prioritizing N-IO delivery, perform tests on the remaining items of the function inspection.
8. Hand over the system to the user after conducting a final Site Acceptance Test (SAT).

TIP

iDefine can be used to create and test applications.

SEE ALSO

For more information about the engineering flow when using iDefine, refer to:

C2.2.3, “Engineering by using iDefine” on page C2-17

B3. Example of ProSafe-RS system configuration

This chapter describes the standard configuration of ProSafe-RS systems.

ProSafe-RS basic configuration

The basic configuration of ProSafe-RS consists of SENG and SCS. The following figure illustrates an example of the basic configuration of ProSafe-RS consisting of one SENG and two SCSs.

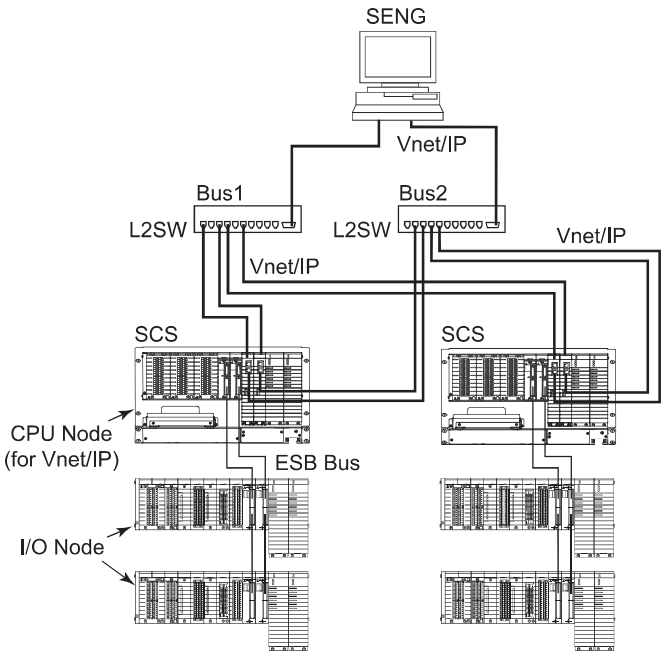
SCS and SENG are connected via control buses. Safety communication through control buses allows data to be sent and received between SCSs.

In SCS, I/O can be expanded by increasing the number of I/O nodes.

In the following figure, each of two SCSs has a Safety Control Unit (CPU node) which is connected to two Safety Node Unit (I/O nodes). I/O modules may also be installed in the CPU node.

Example of Vnet/IP system configuration

The following figure shows an example of the basic configuration of a ProSafe-RS system on a Vnet/IP network.

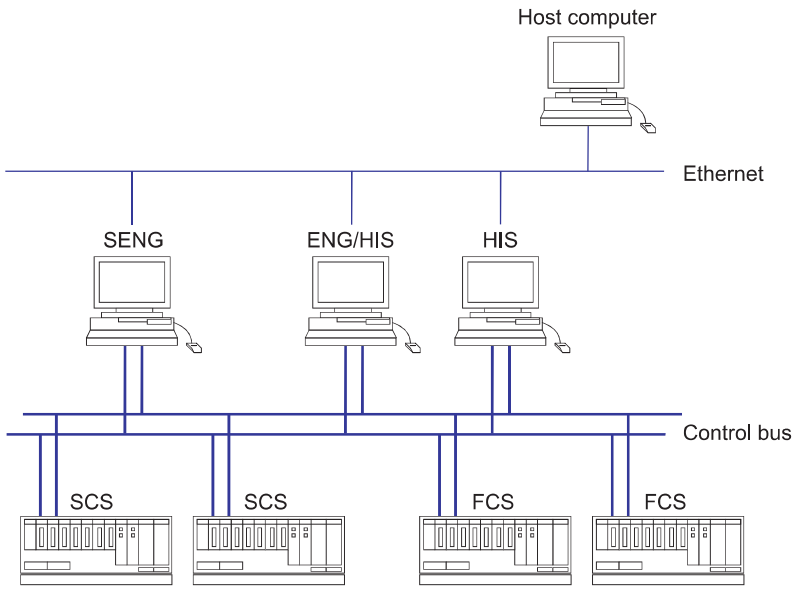


SCS: Safety Control Station to perform safety applications (for Vnet/IP)
SENG: PC for engineering functions like editing applications, downloading, tests and for maintenance.
L2SW: Layer 2 Switch

Figure B3-1 Example of a ProSafe-RS configuration

CENTUM integration configuration

The structure of a ProSafe-RS connected with CENTUM projects is called CENTUM Integration Configuration.



SCS: Control Station to perform safety applications
SENG: PC for engineering functions like editing applications, downloading, tests, and for maintenance.
FCS: Field Control Station to execute process control.
HIS: Human Interface Station
PC which provides interfaces for operators who monitor and operate the plant
ENG: PC installing CENTUM engineering function

Figure B3-2 CENTUM integration configuration

- For CENTUM Integration Configuration, both FCS and SCS can be operated and monitored from HIS.
  FCS can read or write data in SCS via Control bus. But the SCS is designed so that its safety function is not affected even when data is written by FCS.
- SCS engineering is performed from SENG. FCS and HIS engineering is performed from ENG. Engineering of CENTUM integration function is performed from both SENG and ENG.
  SENG functions, ENG functions and HIS functions can be installed in several PCs as well as to the same PC.
- The Exaopc OPC interface package of CENTUM (for installation on HIS) on HIS enables a host computer for production management, to access the data of FCS and SCS by using the OPC Interface.
  Moreover, using the ProSafe-RS SOE OPC interface package allows access to SOE information in SCS from the host computer.
- As a type of the CENTUM Integration Configuration, it is possible to connect only HIS function to ProSafe-RS.
  In this case, the structure is the same as in the previous figure without FCS.
- SENG is connected to control buses in CENTUM integration configuration. In addition, SENG, HIS and ENG terminals are connected via Ethernet.

Structure of connection with other systems

The SCS supports the Modbus slave communication function, subsystem communication function, safety subsystem communication function, and DNP3 communication function as functions for connecting with other systems. The Modbus slave communication function, subsystem communication function, and DNP3 communication function are interference-free functions. Safety subsystem communication is a safety communication but includes partially interference-free communication.

Connections with other systems are realized by installing communication modules in the SCS nodes. Application logic that is created for the communication functions of the Modbus slave

communication function, subsystem communication function, and DNP3 communication function cannot be used in safety loops.

The functions and configurations for connection are as follows.

- Modbus slave communication function
  In this configuration, an external system acts as an Modbus master and the SCS acts as a Modbus slave. You can, for example, construct an operator interface in other system by accessing data in the SCS from the other system that acts as the communication master. You can make redundant Modbus slave communication by creating a user application on the Modbus master.

  Serial communication modules or Ethernet communication modules need to be installed in the SCS nodes to be connected to other systems.

- Subsystem communication function
  The subsystem communication function allows the SCS to act as the communication master and communicate with other systems. The subsystem communication function of the SCS supports Modbus protocol. By using the SCS that acts as a communication master, you can read and set I/O data in the subsystems from the SCS. The subsystem communication can be made redundant.

  Serial communication modules or Ethernet communication modules need to be installed in the SCS nodes to be connected to other systems.

- Safety subsystem communication function
  The function within the safety subsystem communication function where the SCS serves as the communication master and connects with field devices by using fire and gas communication is referred to as the fire and gas communication function. This is a safety communication function which connects field devices with the SCS via communication modules and field wireless control stations, etc. Communication modules cannot be redundantly configured.

  Fire and gas communication modules are installed in SCS nodes to connect with field devices.

- DNP3 slave function
  The function using the DNP3 open protocol wherein the SCS operates as a DNP3 slave and communicates with a DNP3 master such as SCADA is referred to as the DNP3 slave function.

  The Ethernet communication module is installed in SCS nodes to connect to the DNP3 master.

The following figure shows an example of connection.

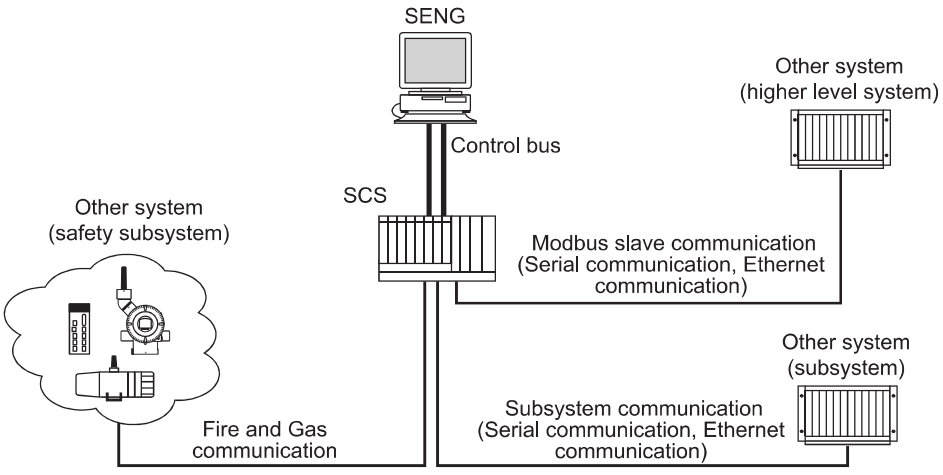


Figure B3-3 Connection with systems except CENTUM

Stand-alone SCS configuration

You can construct a stand-alone SCS configuration system environment without connecting to the Vnet/IP network when operating the SCS. The SCS and SENG can be connected temporarily via network while performing engineering and maintenance. The following figure shows a stand-alone SCS configuration system.

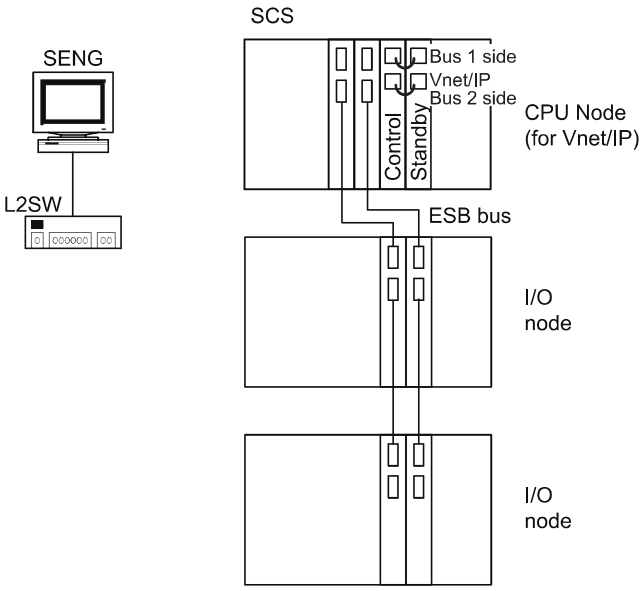


Figure B3-4 Stand-alone SCS configuration system

- Prepare an environment where an SENG can be connected to a stand-alone SCS for its maintenance. When connecting an SENG in a stand-alone SCS configuration environment, connect it to the SCS via a Layer 2 switch (L2SW).
- For maintenance, you need to connect an SENG to the SCS. Use network cables that are long enough for connection of the SENG.

IMPORTANT

- System status and errors should be notified by outputting them on a hardware-wired panel, or should be checked on the SCS State Management window on a connected SENG.
- In order to enable outputs automatically without using an SENG after turning on the power of the SCS, it is necessary to use SYS_STAT to perform the output enable operation from the application logic. The output module status is available through parameters such as the NRO parameter of SYS_IOALLST.
- While operating in a stand-alone configuration, the SCS itself becomes the Vnet/IP time master and its time may gradually deviate from the absolute time. Check the system time and adjust it accordingly when the SCS is connected to an SENG for maintenance and so forth.
- In a stand-alone SCS configuration system, do not turn on the power to the SCS when the battery of the CPU module has run out. If you do so, the date setting in the SCS will be changed to January 1st, 1970.

Size of system

The number of maximum connectable stations in the system which consists of stand-alone ProSafe-RS system and in ProSafe-RS integrated with CENTUM system is shown below respectively. Each system can be expanded as follows:

Number of stations (ProSafe-RS integrated with CENTUM)

- Connectable control bus: V net or Vnet/IP
- Number of connectable domains: 16
- Number of connectable stations in a domain: 64
- Number of connectable stations: 256
- Hierarchy: three-level hierarchy (three levels of control bus) (Up to two BCVs or two pairs of CGWs)

For HIS, 16 stations/domain at maximum.

For multiple domains, system generation function of CENTUM is required. In addition, V net requires BCVs and Vnet/IP requires Layer 3 switches.

Number of stations (stand-alone ProSafe-RS system)

- Connectable control bus: V net or Vnet/IP
- Number of connectable domains: 1
- Number of connectable stations in a domain: 64

A stand-alone ProSafe-RS system cannot be configured as a multiple-domain system. Only single-domain configuration is supported.

Vnet/IP domain connection specifications (when integrated with CENTUM)

Connect between Vnet/IP domains with a Layer 3 switch (L3SW) on each bus. This also requires the CENTUM system builder function.

- Number of connectable domains: 16 (Total of Vnet/IP domains and V net domains)
- Number of Layer 3 switches (L3SW) allowed: 15 levels

Connection specifications in a Vnet/IP domain (when integrated with CENTUM)

- Number of connectable Vnet/IP stations: Max. 64 (Vnet/IP stations including V net routers)
- General-purpose Ethernet communication devices: Max. 124 (PCs, Routers, etc.)
- Distance between stations in a Vnet/IP domain: Max. 40 km
- Distance between Layer 2 switch and a station: Max. 100 m (for Unshielded Twisted Pair (UTP))
- Distance between Layer 2 switches: Max. 5 km (for fiber-optic cable)
- Number of connectable Layer 2 switches in a domain: Max. 7 per each Bus. (Multilayer by cascade connection allowed)

B4. System reaction time

This section describes Reaction Time and PFD Calculation.

System reaction time

The system reaction time of SCS consists of the reaction time for the external demand (Demand reaction time) and the reaction time when a fault is detected in the SCS (Fault reaction time).

- Tr: system reaction time
- Tscan: scan period for application logic execution

Demand reaction time

The demand reaction time differs as follows, depending on whether the loop includes safety communication.

- When not using the inter-SCS safety communication



Figure B4-1 Reaction time 1

Tr = Tscan x 2 + Input processing time + Output processing time-Idle time

Idle time = Tscan - Application logic execution time

The output module processing time is shown in the following table.

Table B4-1 Output response time of the output module

Output module	Output response time
SDV531/L1DV531	30 ms
S2MMM843	110 ms for AO mode (90% response)
	30 ms for DO mode
S2MDV843	30 ms

- When using the inter-SCS safety communication
  When using the inter-SCS safety communication, the calculation formula varies depending on the relation between the scan periods of producer SCS and consumer SCS.
  - If Tscan on the producing side > Tscan on the consuming side:
    Tr = Tscan on the producing side x 2 + Tscan on the consuming side x 2 + transmission delay
  - If Tscan on the producing side ≤ Tscan on the consuming side:
    Tr = Tscan on the producing side x 2 + Tscan on the consuming side x 3 + transmission delay

  Transmission delay (For Vnet)
  - No BCV/CGW used: 10 ms
  - BCV/CGW used: number of BCV used x 50 ms + number of pairs of network levels via CGWs x 500 ms

  Transmission delay (Vnet/IP)

Table B4-2 Transmission delay in the case of Vnet/IP

Range	Mandatory values
Within a Vnet/IP domain	10 ms
Between Vnet/IP domains without a wide area connection (*1)	50 ms (Regardless of the number of L3SWs)
Between Vnet/IP domains with a wide area connection	250 ms (Regardless of the number of L3SWs and existence of WAC routers)
If the Vnet/IP domain and V net domain are connected using a V net router	Number of the hops of V net router x 50 ms

*1: Connecting two domains through wide-area network is called "wide area connection."



Figure B4-2 Reaction time 2

- When using SCS link transmission safety communication
  Tr= Sender Tscan x 2 + Receiver Tscan x 2 + Transmission Delay

  Transmission Delay: 100 ms
- When fire and gas communication is being used
  The demand reaction time is the total value of the following items (1) through (6):

Table B4-3 Demand reaction time when fire and gas communication is being used

Item	Description
(1) Time until GS01 detects the gas concentration	Refer to the GS01 User Manual.
(2) SCS reaction time	SCS reaction time = Tscan x 2 + Input processing time + Output processing time - Idle time Input processing time = 100 ms (for S2LP131) Idle time = Tscan - Application logic execution time
(3) Time until communication between S2LP131 and YFGW410 is restored after control rights of a redundant YFGW410 is switched over	5 seconds. This time includes the 1 second for switching of YFGW410 to be completed. In the following cases, the time is 0 seconds: • When YFGW410 is of a single configuration • When assuming that detection of gas and switching of YFGW410 will not occur at the same time
(4) PROFIsafe communication time from the SCS to GS01	8 seconds is recommended.
(5) PROFIsafe communication time from GS01 to the SCS	Always 2 seconds.
(6) SCS reaction time	Same as the description for (2).

Fault reaction time

How to calculate the fault reaction time of the ProSafe-RS system is shown as follows:

- In the case of faults within the Safety Control Station

  Basically, fault reaction time (maximum) is calculated by the following formula:

  Tr = (Fault detection time) + Tscan × 2 + Output module processing time - Idle time

  In the formula, the maximum value (of fault detection time) is as follows for each module.

Table B4-4 Fault detection dime of each I/O module

I/O module types	Fault detection time
SDV144, SDV521, SDV531, SDV526, SDV541, SDV53A, L1DV144, L1DV521, L1DV531, L1DV526, L1DV541, and L1DV53A	520 ms
SAI143, SAI533, L1AI143, L1AI533	600 ms
SAV144, L1AV144	1360 ms
SAT145, SAR145, L1AT145, L1AR145	2100 ms
S2MMM843	600 ms for AI mode, AO mode
	520 ms for DI mode, DO mode
S2MDV843	520 ms

The fault reaction time for the fault in communication between CPU module and output module is shown in the following formulas:

- Tr = 1 s (Tscan =< 250 ms)
- Tr = Tscan x 2 + 0.5 s (Tscan > 250 ms)

After the time (Tr above) passed since the faults, the output module outputs the Output value at fault.

- For failures involving a field device or wiring
  You need to enter the values specified in following table in the (fault detection time) of the previously mentioned formula only when calculating the fault reaction time for the following types of faults. Both are maximum values.

Table B4-5 Fault detection time of field wiring and devices

Type of Fault	Module	Fault detection time (Maximum)
Short circuit between channels	SDV144, SDV521, SDV531, SDV541, SDV53A, L1DV144, L1DV521, L1DV531, L1DV541, and L1DV53A	1.46 s (*1)
	SAI533, L1AI533	0.6 s
Short circuit in output wiring (while outputting OFF signals)	SDV531, SDV541, L1DV531, L1DV541	1.46 s (*1)
	SDV521, L1DV521	10 s (*1) (*2)
	SDV53A, L1DV53A	10 s (*1) (*3)
	DO mode of S2MMM843, S2MDV843	1.6 s(*4)
Open circuit	SAT145, SAR145, L1AT145, L1AR145	1.5 s(*5)
	DO mode of S2MMM843, S2MDV843	1.6 s(*6)
Inputting the signal out of the range	SDV144, L1AV144	1.02 s (*7)
	DI mode of S2MMM843, S2MDV843	1.02 s (*7)
Open circuit or short circuit with the power supply line (while sending OFF signal)	SDV526, L1DV526	302 s
Overload of field device	SDV526, L1DV526	1.5 s

*1: Can be detected only when the pulse test is enabled.
*2: Value for style S3 and above.

*3: Value for style S2 and above.
*4: Can be detected only when low voltage pulse test (on) is enabled.
*5: Can be detected only when burnout detection is enabled.
*6: Can be detected only when detect disconnection and low voltage pulse test (on) is enabled.
*7: This value applies when the modules are in dual redundant configuration. The value for non-redundant configuration is 520 ms as noted in the above explanation.

- Inter-SCS safety communication
  The reaction time while using inter-SCS safety communication is the timeout period that is specified in the FB for inter-SCS safety communication.

  Tr = OUTT + DLYT

  - OUTT: Reception Interval Timeout value
  - DLYT: Transmission Delay Timeout Value

- SCS link transmission safety communication
  The reaction time while using SCS link transmission safety communication is the timeout period that is specified for the receiver SCS.

  Tr = OUTT + DLYT

  - OUTT: Reception Interval Timeout value
  - DLYT: Transmission Delay Timeout Value

- Fire and gas communication
  The fault reaction time when fire and gas communication is being used is the total value of the following items (1) through (3):

Table B4-6 Fault reaction time when fire and gas communication is being used

Item	Description
(1) PROFIsafeWatchDogTime with communication immediately prior to the gas concentration being reflected onto the output value of GS01	30 to 60 s
(2) PROFIsafeWatchDogTime with communication after the gas concentration being reflected onto the output value of GS01	30 to 60 s
(3) SCS reaction time	SCS reaction time = Tscan x 2 + Input processing time + Output processing time - Idle time Input processing time = 100 ms (for S2LP131) Idle time = Tscan - Application logic execution time

SEE ALSO For more information about setting OUTT and DLYT, refer to:

- "● Inter-SCS safety communication timeout settings" in "■ Precaution for engineering" in A7., "Inter-SCS safety communication" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)
- "■ Definition of receive data" in A6.2, "Data structure and definition of the SCS link transmission" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Example of calculating the Fault Reaction Time (Tr)

Conditions:

Scan period of application logic: 200 ms

Idle time: 30%

DO module: SDV531 (output response time = 30 ms)

- Case 1 (Fault with the DI module)
  Tr (max.) = 520 ms + 200 ms x 2 + 30 ms – (200 ms x 0.3) = 890 ms
- Case 2 (Communication fault between the CPU module and the output module)
  Tr (max.) = 1 s (because Tscan < 250 ms)

- Case 3 (Short circuit fault between DI channels)
  Tr (max.) = 1460 ms + 200 ms x 2 + 30 ms – (200 ms x 0.3) = 1830 ms

PFD calculation

The average PFD (System PFDavg) of a system is calculated with the model in the following figure.

System PFDavg = Sensors PFDavg + Controller PFDavg + Valves PFDavg

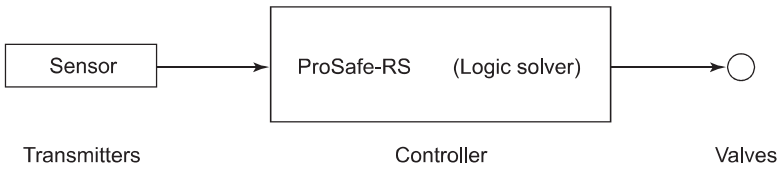


Figure B4-3 PFD calculation model

For ProSafe-RS (SIL 3), when the interval between proof tests is 10 years and the DIO module is used, the Controller PFDavg is indicated as follows.

Controller PFDavg = 6.63×10^{-6}

Further information about PFD calculation is available on request.

C. Basics of creating applications

This part describes the preparations common to all engineering methods of ProSafe-RS, the procedures for creating applications for each engineering method, precautions, analysis tools, and test methods in the following order:

1. Preparing the project
   This section describes how to prepare the AD Server to create a new project for SCS engineering and register the project in the AD Server.
2. Work flow for creating applications
   The work flow to define I/O and creating applications differs depending on the engineering method used. This section describes the work flow and main points of creating applications for each engineering method.
3. Precautions when creating applications
   This section describes the precautions when creating applications.
4. Procedures for generating a database
   After creating the application, generate a database. This section describes the method and precautions for generating a database.
5. Testing with the Safety Analyzer
   After generating the database, test the application by using the Safety Analyzer. This section describes the Safety Analyzer.
6. Simulation tests
   Run tests using simulators if necessary. This section describes simulation tests.
7. Offline download to the system
   Offline download the created application to SCS. This section describes the offline download.
8. Output enable operation
   After performing the output enable operation, values from the application are sent from the output module. This section describes the enable output operation.
9. Target tests
   The created application must undergo target testing. This section describes target tests.

C1. Preparing the project

After the preparation for the AD Server is complete, prepare the project. This section explains the type of projects that need to be prepared and how to prepare them.

C1.1 Type of project

ProSafe-RS has the following types of projects:

- AD project
  It is a project for managing multiple RS projects in the AD Server.
- RS project
  It is a project for managing multiple SCS projects. You can view the status of SCS projects which are included in the same RS project by using the SCS Maintenance Support Tool.
- SCS project
  It is a project that corresponds to a single SCS and is the smallest project unit.

The following figure shows the relationship between the actual SCS and each project type.

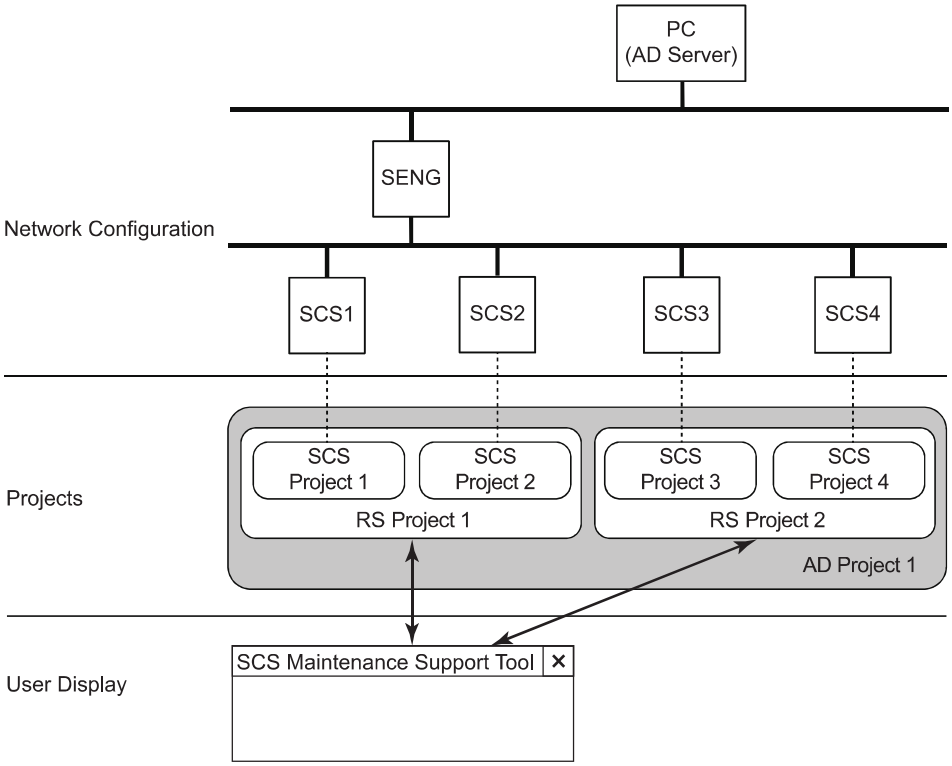


Figure C1.1-1 Relationship between the actual SCS and each project type

For integration with a CENTUM system, a definition to associate the CENTUM Project with SCS Project is required.

In addition to these projects, there are library projects where the engineering data can be used as a library. You can also register library projects in AD projects.

Relationship between SCS project and RS project

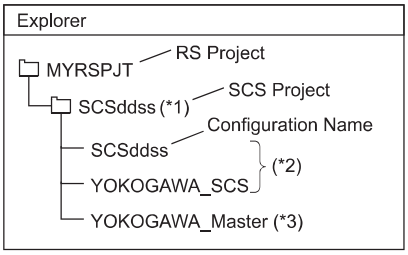
An SCS project is included in an RS project. One SCS project, which is always included in one RS project, is not shared with another RS project. In addition, an RS project is not included in another RS project.

Folder configuration of SCS project and RS project

The SCS projects that constitute an RS project are specified by the folder configuration.

- RS Project
  A folder created in Windows Explorer

- SCS Project
  A folder created by using the SCS Manager under an RS project folder. It is placed as one folder.



*1: The folder name must be identical to the SCS project name. (dd: Domain number, ss: Station number)
*2: This is a work database.
*3: This is a master database.

Figure C1.1-2 Folder configuration of SCS project and RS project

C1.1.1 AD project

It is a project for managing multiple RS projects. The engineering data of AD Suite is managed per AD project.

I/O licenses are counted for all SCSs contained in the RS projects that are registered in one AD project.

The following figure shows the relationship between the ProSafe-RS license project and the AD project.

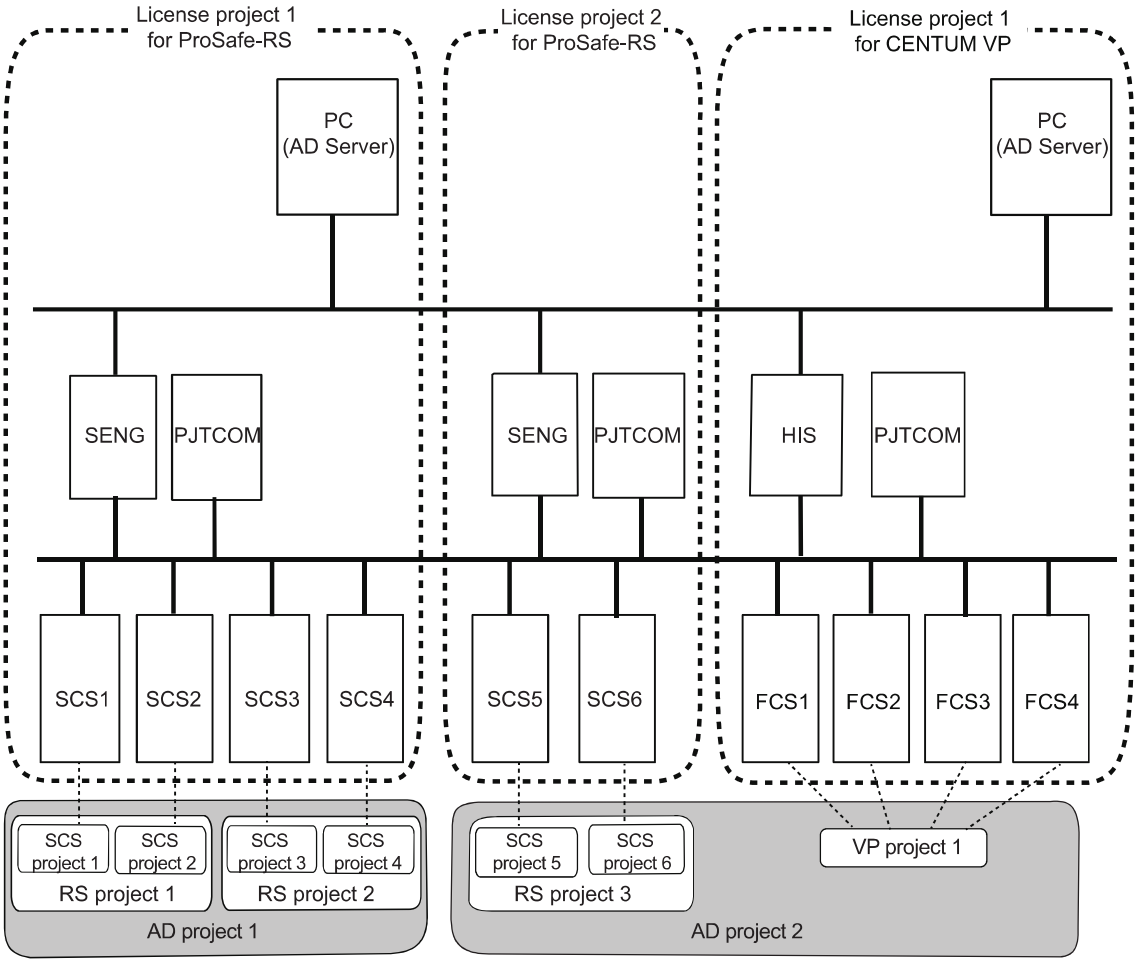


Figure C1.1.1-1 Relationship between the ProSafe-RS license project and the AD project

If the number of I/O points exceed the number of licenses, you will not be able to download SCS projects to the SCS. Use the SCS information display function to check the number of licenses.

SEE ALSO

For more information about the SCS information display function, refer to:

"■ Checking the usage status of I/O licenses" in F1., "Display SCS information" in Engineer's Reference Manual (IM 32P04B10-01EN)

C1.1.2 RS project

An RS project is a combination of several SCS projects in order to bundle engineering data of SCS projects. Defining an RS project permits the collective monitoring of the status of the constituent SCSs by using the SCS Maintenance Support Function.

You must register all RS projects that involve the SCSs to which a license of the same license project is assigned in a single AD project.

C1.1.3 SCS projects

You need to define one SCS project for each SCS. An SCS has an attribute and contains the following databases:

- Work database (SCS database and source files)
- Master database (running SCS database and source files)

■ SCS project attribute

An SCS project will be defined with the following three attributes.

The attributes of a project determine whether it can be downloaded to actual SCS and whether it can be tested by SCS simulation. However, a logic simulation test can be preformed for any project regardless of its attribute.

● Default project

A new project created in the SCS Manager will be the default project. The default project should be a project that has not been downloaded to the actual SCS. Engineering works for a new project are always carried out on the default project.

Downloading to the actual SCS: Always use offline download

Testing by SCS simulation test: Available

After offline download to the actual SCS has been completed successfully, the attribute of the project will change from Default Project to Current Project automatically.

● Current project

If the offline download to the actual SCS is completed successfully at least once, the attribute of the project will change to Current Project.

Downloading to the actual SCS: Available

Testing by SCS simulation test: Unavailable

● User-defined project

The attribute of a project created by using the Test Project Creation Tool is User-Defined Project.

SCS simulation tests cannot be run on the current project. To check the changes made to the application through the SCS simulation test, copy the current project by using the Test Project Creation Tool and test the changes using the copied project. Based on the scale of the changes made, decide whether to make a copy after modifying the current project or modify the project after copying.

Downloading to the actual SCS: Unavailable

Testing by SCS simulation test: Available

SEE ALSO For more information about reflecting the changes made to a user-defined project in the current project, refer to:

"■ Operations required after SCS simulation tests (user-defined project)" in 3.1.2, "Engineering procedure after SCS simulation tests" in Test Function Guide (IM 32P04B30-01EN)

■ Configuration and functions of SCS project database

In ProSafe-RS, one SCS project is defined and managed for each SCS. The following data are stored in each SCS project folder.

- Work database

- Master database

The following shows the components and related functions of an SCS project.

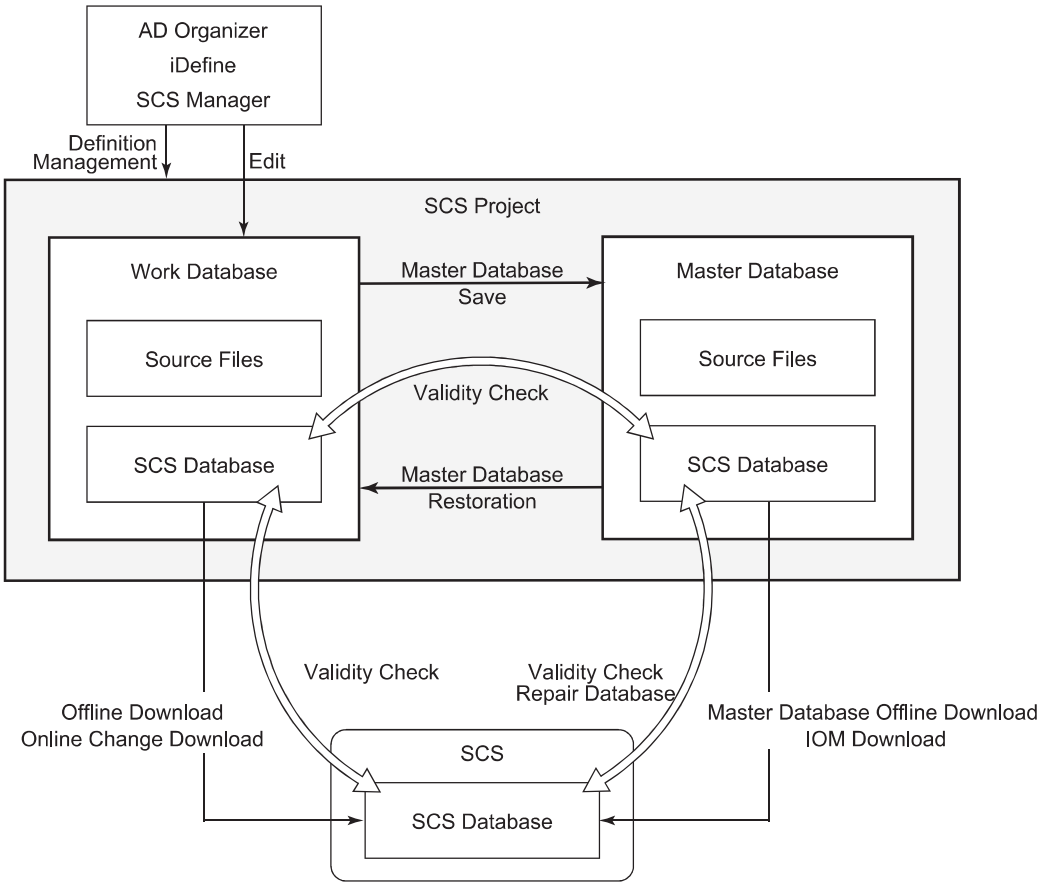


Figure C1.1.3-1 Configuration of SCS project

Work database

The SCS database with the edited content reflected on it and its source files are called work database.

After applications are edited using SCS Manager, Multi-Language Editor, or Builders, the source files will be created.

When performing I/O list engineering, the results are reflected in the work database when the data is edited in AD Organizer and the reflection process is run. You can edit by using iDefine in addition to AD Organizer.

The SCS database is created if you run RS generation from AD Organizer or if you build from SCS Manager.

Master database

The master database refers to the running SCS database and a group of its base source file group at the time when the SCS database is downloaded to the SCS via offline download or online change download.

The master database is also used both online change download and to detect differences from the work database by Cross Reference Analyzer.

IMPORTANT

Do not edit the master database using Windows explorer.

Master database saving function

This function automatically saves the contents of the work database to the master database when the SCS database is downloaded to the SCS via offline download or online change download, and retains it at all times in SCS projects. Therefore you do not need to upload the database from the SCS to SENG.

Master database restoring function

The Master Database Restoring function is provided as a function to delete the work database that is being edited and restore the contents of the master database as the work database.

Database validity check tool function

You can check the validity among the master database, work database, and the SCS database that is downloaded to the SCS. You can also eliminate any inconsistencies in the databases. This function is provided as the Database Validity Check Tool.

Editing rules and purpose of SCS project database

The rules to follow when editing SCS projects are as follows:

- You cannot open multiple SCS Managers on one SENG at the same time.
- You can use one SENG to edit the SCS projects that are stored on another SENG. However, you cannot operate the same SCS project from several SENGs at the same time.

The master database and the work database are separated, so the following is possible:

- The user can perform monitoring based on the master database running on an SCS regardless of whether the work database is being modified or not.
- Even if an SCS hardware failure occurs and a CPU module and/or input/output module require replacement, the user can restore the SCS application by master database offline download and IOM download.
- The user can restore the work database from the master database in order to cancel changes made to the SCS project.

SEE ALSO For more information about the function for downloading the master database onto SCS, refer to:

- I4.4, “Master database offline download” on page I4-76
- F4., “Master Database Restoring Function” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about precautions for restoring an SCS project that was generated by RS generation with AD Organizer of a revision earlier than R4.03.10, refer to:

“■ Precautions for restoring an SCS project that was generated by RS generation with AD Organizer of a revision earlier than R4.03.10” on page C3-2

C1.1.4 Library project

A library project is a project database that can be used as a library independent of the specific SCS. Library projects can be used for creating application logics and can be debugged only by a logic simulation test. (An individual library project cannot be tested by SCS simulation test or by target test for debugging.)

The functions and function blocks that are used among two or more SCSs can be created as library projects and be copied to each SCS project.

When engineering by using iDefine, library projects cannot be used.

C1.2 Procedures for creating projects

Follow these steps to prepare the project data. Use the same steps for both the RS original engineering method and the I/O list engineering method.

1. Set the location of ADMDB by using the ADS Administration Tool.
2. Create an AD project by using the ADS Administration Tool.
3. Configure the user management and access control by using the ADS Administration Tool.
4. Connect to the AD project by using the ADS Administration Tool.
5. Create an RS project folder by using Windows Explorer.
6. Register the RS project to the AD project by using AD Organizer.

TIP

Even if you have selected RS original engineering, register RS projects to AD projects. You can also register RS projects that include SCS projects that were created before introducing AD Suite.

7. Call SCS Manager from AD Organizer and create an SCS project.

TIP

When creating an SCS project, you select a station type and an engineering method. You cannot change the engineering method later.

SEE ALSO

For more information about ADMDB location configuration, refer to:

C1.1.4, “Setting the location of the ADMDB” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about creating AD projects, refer to:

C1.2.1, “Creating and deleting AD projects” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about configuring user management and access control, refer to:

C1.2.2, “Controlling access to AD projects” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about procedures to connect AD projects to the AD Server, refer to:

C1.2.1, “Connecting to AD projects” on page C1-11

For more information about creating RS projects, refer to:

C1.2.2, “Creating RS projects” on page C1-12

For more information about procedures for registering RS projects in an AD project, refer to:

C1.2.3, “Registering RS projects in the AD project” on page C1-13

For more information about SCS project creation procedure, refer to:

C1.2.4, “Creating SCS projects” on page C1-15

C1.2.1 Connecting to AD projects

After you complete the project registration, user management, and definition of access control on the AD Server, you must configure the settings for connection from AD Organizer to the AD project.

You need to perform the following procedure for setting:

1. Start AD Organizer.
   When AD Organizer is started for the first time, the Select AD Project dialog box appears.
2. When AD Organizer is not started for the first time, select [File] > [Change AD Project] from the menu bar on AD Organizer.
   The Select AD Project dialog box appears.
3. Enter the computer name or IP address of the AD Server, and then click [Connect].
   A connection is established to the specified AD Server and a list of AD projects that are found on the corresponding AD Server is displayed.
4. Select the target AD projects, and then click [Save Settings].
   If a logged-in user of AD Organizer is registered in the target project, the connection request succeeds, the Select AD Project dialog box closes, and the project information is displayed in AD Organizer.

SEE ALSO

For more information about project registration with AD Server, refer to:

“● Project registration” in “■ Server processing and status of the ADMDB at the time of the ADMDB location setting” in C1.1.3, “ADMDB location setting” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about defining user management and access control with AD Server, refer to:

C1.2.2, “Controlling access to AD projects” in Engineer's Reference Manual (IM 32P04B10-01EN)

C1.2.2 Creating RS projects

When you install ProSafe-RS software, a folder for an RS project is automatically created. You can also create another RS project.

You need to set the folder of the RS project as a shared folder.

Initial status of RS projects

When you install ProSafe-RS software, one RS project is automatically created as the `C:\RS-Projects\MYRSPJT` folder. When this folder is used as is, you do not need to create a new RS project.

Operations when sharing an RS project

You need to set the automatically created RS-Projects folder of `C:\RS-Projects` as a shared folder, or create an RS project under a shared folder.

Creation of new RS projects

It is possible to create new RS projects in addition to the RS project created at the installation. In this case, use Windows Explorer to create a folder with the name of new RS project. The folder name is used as the name of the RS project. The following restrictions apply to the folder name.

- Folder name: Up to 8 single-byte characters, starting with an upper case alphabet character
- Characters that can be used: Single-byte alphabet characters in upper case, numerals, underscore and hyphen
- Absolute path of the folder: The path to the RS project folder cannot contain the following characters:
  Single-byte space, `\, /, :, ;, *, ?, ", <, >, |, .`

TIP

Keep the absolute path of the folder as short as possible. If an error occurs due to a restriction in the file name length of Windows, review the length of the following names as well:

- Length of the absolute path of RS projects
- Length of the library project name
- Length of the library project configuration name
- Length of the library project resource name

C1.2.3 Registering RS projects in the AD project

After creating a folder of RS projects, you can use AD Organizer to register RS projects in the AD project.

You must register all RS projects that involve SCSs to which a license of the same license project is assigned in the same AD project. This registration enables you to correctly count the number of I/Os in the scope of the ProSafe-RS license project. After registering the RS project to an AD project, do not copy, move, or delete the RS project using Windows Explorer. In addition, make sure to use AD Organizer when you create a backup of the RS project.

You need to perform the following procedure to register RS projects in the AD project:

1. Start AD Organizer.
2. On the System Structure Navigator, select [Register System Project] from the sub menu. The System Project Registration dialog box appears.

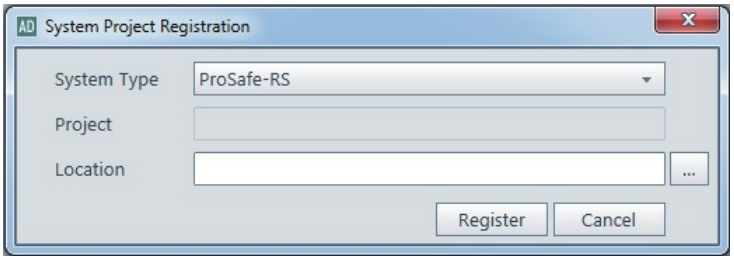


Figure C1.2.3-1 Project registration screen

3. Configure the settings as follows:

System type	Select ProSafe-RS.
Project	A folder that is created for RS projects is displayed. You cannot configure the settings.
Location	Set the location of RS projects.

4. Click the [Register] button.

Editing RS project properties

You need to perform the following procedure to edit the properties of the RS project:

1. Select the RS project displayed on the System Structure Navigator and select [Properties] in context menu.
   The Properties tab appears.
2. Edit items.
3. Click the [OK] button.

Unregistering RS projects

You need to perform the following procedure to unregister RS projects:

1. In the System Structure Navigator, select the RS project.
2. From the sub menu, select [Unregister System Project].
   The RS project in the AD project is unregistered.

Reflecting the changes in RS projects to the data in AD Organizer

The settings such as RS project definition and station are edited in SCS Manager and saved in ADMDB and RS project database. After registering or unregistering an RS project or editing

its properties, you need to perform the following operation to update the system information of System Structure Navigator in AD Organizer.

- From the menu bar of AD Organizer, select [View] > [Refresh].

C1.2.4 Creating SCS projects

You need to start SCS Manager from the System Configuration Navigator of AD Organizer and use the new SCS project creation function to create a new SCS Project.

The generated information is stored in the RS project database and ADMDB. In AD Organizer, when the update is done by using the System Structure Navigator, the latest status appears.

SCS project creation procedure

This section describes the procedures to create an SCS project.
To create a new SCS project, launch SCS Manager from AD Organizer and configure the following settings:

Do not use Windows Explorer functions to copy or move the SCS projects that you have created.

1. Setting an SCS project folder
   Set a folder in which to store the SCS project data.
2. Setting SCS project items
   Set Domain number and Station number etc. of the SCS project. Some of the items can only be specified in the process of creating a new SCS project and others can be changed later.
3. Setting a resource
   A resource refers to a set of SCS application logics. In this step, the resource name and resource number are specified. In ProSafe-RS, one resource can be set for one SCS.
4. Setting a configuration
   A configuration refers to a software object corresponding to one SCS. The configuration name is specified in this step. In ProSafe-RS, one configuration can be set for one SCS. A configuration includes a resource.
5. Setting an IP address
   Specify an address related to TCP/IP communication of the SCS.
6. Setting SCS constants
   Specify SCS constants.

Setting an SCS project folder

Follow these steps to create an SCS project:

1. From AD Organizer, start SCS Manager and select [File] > [New Project/Library] from the menu bar.
   The New dialog box appears.
2. Enter the following details:

Destination folder:	Folder where the SCS project is saved
Name:	SCS project name `SCSddss` dd denotes Domain number, and ss denotes Station number.
Comment:	64 characters or less
Template:	`SCS_Default_Target`

Create SCS project folders directly under RS project folder.

SEE ALSO For more information about details on SCS project folder settings, refer to:

"Working with projects" in "Workbench" in the Workbench User's Guide

Setting SCS project items

When the SCS project folder has been configured, the SCS Project Properties dialog box appears. Configure the settings related to the SCS and project on the [SCS] tab and the [Project] tab of this dialog box.
In the SCS Project Properties dialog box, the [I/O List Engineering] check box appears. This check box becomes available when you select a Station Type to which I/O list engineering is applicable. If you select the check box, the I/O list engineering is applied. If you create an SCS with this check box clear, RS original engineering is applied. You cannot change the engineering method later.

SCSP3/SCSL2/SCSP2/SCSP1/SCSU1can be a target of I/O list engineering.

When the system is integrated with CENTUM, specify a CENTUM project folder on the [Project] tab.

SEE ALSO For more information about details on SCS Project Properties dialog box, refer to:

C1.2.5, “SCS Project Properties dialog box” on page C1-18

Setting a resource

A resource refers to a set of application logics created by the user. Multiple programs can be run in one resource. Only one resource can be run in one SCS.
Right click the resource on Link Architecture View and then choose [Properties] from the pop-up menu so as to display the Resource Properties dialog box. The resource name and the resource number can be defined on the General tab. Specify "SCSddss" for the resource name and "ddss" (dd: domain number, ss: station number) for the resource number.

SEE ALSO For more information about details on resource settings, refer to:

"Resources" in "Link architecture view" in "Workbench" in the Workbench User's Guide

Setting a configuration

In order to execute an application logic set, it is necessary to specify the hardware configuration of each SCS.
Right click the configuration on Hardware Architecture View and then choose [Properties] from the pop-up menu so as to display the Configuration Properties dialog box. The configuration name can be defined on General tab.

Specify "SCSddss" (dd: domain number, ss: station number) for the configuration name.

SEE ALSO For more information about details on configuration settings, refer to:

"Configuration properties" in "Hardware Architecture View" in "Workbench" in the Workbench User's Guide

Setting an IP address

The IP address can be defined on Hardware Architecture View. Double click "Connection" so as to display Connection - Properties dialog box. The IP address needs to be set for "Value" item.
In the standard, the IP address sets "172.16.dd.ss" (dd: domain number, ss: station number).

SEE ALSO For more information about details on IP address settings, refer to:

"Connections" in "Hardware Architecture View" in "Workbench" in the Workbench User's Guide

Setting SCS constants

Specify constant values for SCS and parameters for communicating with external systems in SCS Constants Builder.

SEE ALSO For more information about details on SCS Constants Builder, refer to:

C1.2.6, “SCS Constants Builder” on page C1-21

C1.2.5 SCS Project Properties dialog box

The SCS Project Properties dialog box is used to make various basic settings for an SCS, including domain number and station number.

Calling the SCS Project Properties dialog box

The SCS Project Properties dialog box appears if you perform the following operations in SCS Manager.

- When a new SCS project is created
  The SCS Project Properties dialog box appears automatically when the SCS project folder settings are completed.
- When a menu is selected from the Engineering launcher menu of SCS Manager
  To edit an SCS project after it is created, select [Engineering] from the [Tools] menu of SCS Manager. The Engineering launcher menu appears; select [SCS Project Properties].

Components of the SCS Project Properties dialog box

The SCS Project Properties dialog box has the following components.

SCS tab

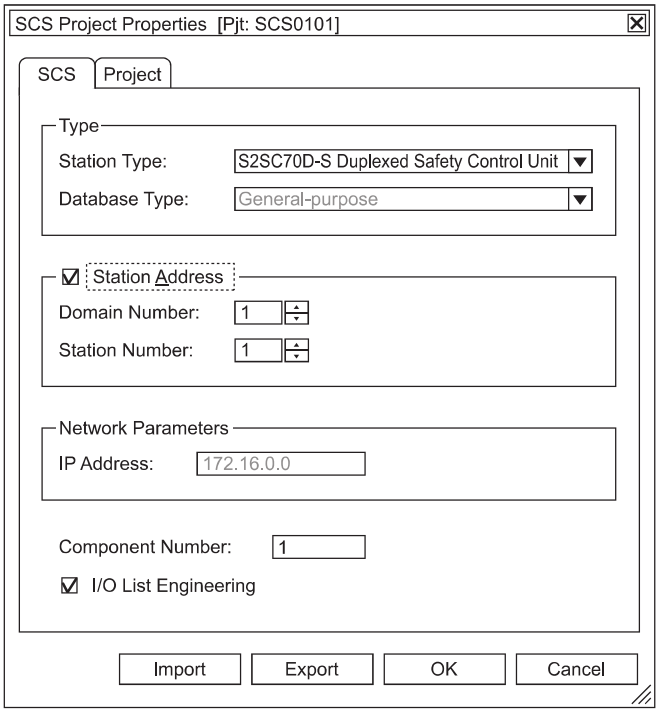


Figure C1.2.5-1 SCS tab

The table below shows the components of the "SCS" tab.

Table C1.2.5-1 Setting items in the "SCS" tab

Item	Setting (*1)	Description
Station Type	Only possible when a new project is created	Specify the model of the SCS station.
Database Type	Display only	Database type is displayed.

Continues on the next page

Table C1.2.5-1 Setting items in the "SCS" tab (Table continued)

Item	Setting (*1)	Description
Station Address	Yes	Select the check box to allow setting the domain number and station number. The check box is selected by default when a new project is created. The check box is not selected by default when this dialog box is opened from the Engineering launcher menu.
Domain Number	Yes	Specify the domain number. Select a value using the spin box or enter a character string directly. A value in the range from 1 to 31 can be specified.
Station Number	Yes	Specify the station number. Select a value using the spin box or enter a character string directly. A value in the range from 1 to 64 can be specified.
IP Address	Display only	The IP address set in Hardware Architecture View is displayed.
Component Number	Yes	Enter the component number. (*2) Up to 4 characters, which can be any alphanumeric characters, can be entered.
I/O List Engineering	You can configure the settings only when creating a new project.	Specify whether to use the I/O list engineering method

*1: Yes: Setting possible
*2: This is a number assigned to identify the devices belonging to an RS project. It is assigned when installing an SCS in a cabinet, etc., and used to show the connection origin and destination of each cable when wiring cables.

IMPORTANT

- Make sure to specify the station type and engineering method when creating a new SCS project. They cannot be changed later.
- After you have defined the station address (domain number and station number), try not to change it if possible. Changing the station address deletes the master database.

Project tab

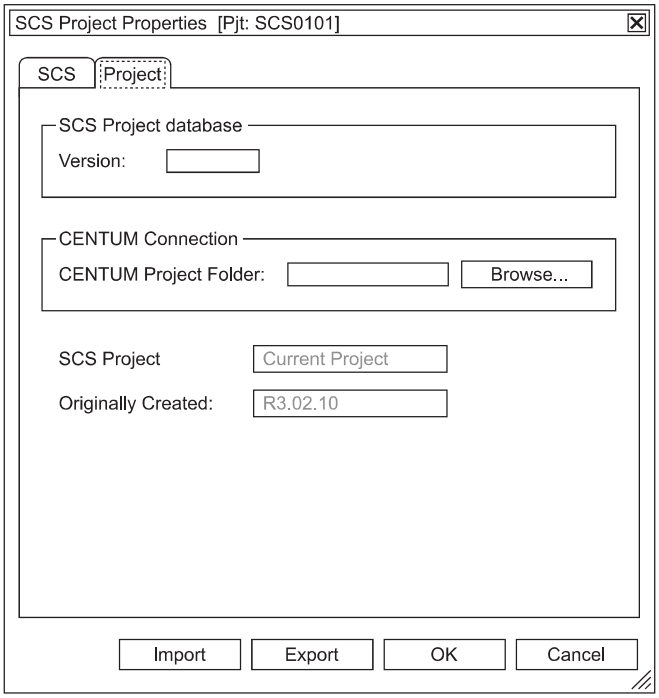


Figure C1.2.5-2 Project tab

The table below shows the components of the "Projects" tab.

Table C1.2.5-2 Setting items in the projects tab

Item	Setting (*1)	Description
Version	Display only	The version number is displayed if the versions of the project data are maintained. The field is blank in the case of an SCS project that has never been checked in with Version Control Tool.
CENTUM Project Folder	Yes	Specify the top folder of the CENTUM project. Enter the path directly or specify the path from the Folder Selection dialog box that is displayed by clicking [Browse]. (*2) (*3) This is valid only when a license for the CENTUM VP Integration Package has been assigned to the PC.
SCS Project	Display only	Displays SCS project attribute. Project Attribute: Default Project, Current Project, User-Defined Project
Originally Created	Display only (*4)	Displays the software revision number of the SENG that the project was created from.

*1: Yes: Setting possible
*2: If the entire length of the specified path cannot be displayed in the text edit box, the middle part of the path is omitted and displayed as [...].
*3: A path specified in the local drives format is automatically converted to a path in UNC format.
*4: If the project was created in SENG with a software revision number prior to R1.03, the software revision number cannot be displayed.

TIP

SCS Project Properties dialog box is available for both SCS project and Library project. It differs in the SCS project properties dialog box of Library project as follows:

- This dialog box will not automatically start when the project is newly created.
- When started from SCS Manager, only "Project" tab will be displayed.
- There is no need to specify [CENTUM Project Folder].
- [Default Project] will be displayed as SCS Project.

C1.2.6 SCS Constants Builder

SCS Constants Builder is used to specify constant values for SCS and parameters for communicating with external systems.

Calling SCS Constants Builder

Select [Engineering] from [Tools] menu of SCS Manager. When the Engineering launcher menu appears, select [SCS Constants Builder]. The SCS Constants Builder starts.

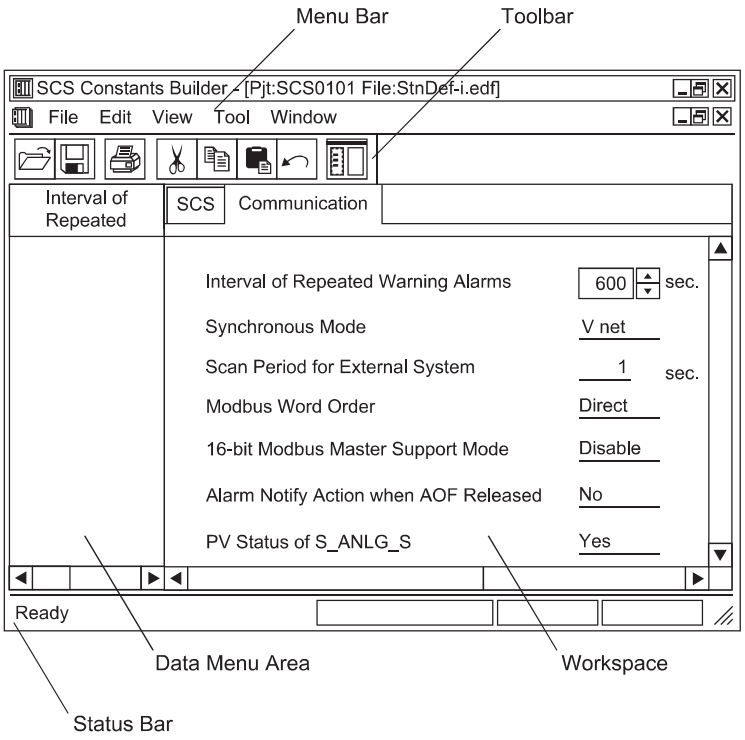


Figure C1.2.6-1 Communication tab of SCS Constants Builder window

SCS Constants Builder contains the following tab sheets:

- SCS tab
  For common setting parameters related to SCS
- Communication tab
  For setting parameters related to communication with external systems

SEE ALSO For more information about menu bar, toolbar, data menu area, and message display area, refer to:

A4.1, “Window components common to builders” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

SCS tab

On the SCS tab, you can set the following items:

Optical ESB Bus Repeater: SCSV1/SCSP1

Select [Yes] if you use the Optical ESB Bus Repeater. [No] if not. The initial setting is [No].

Maximum Extension Distance: SCSV1/SCSP1

Set the Maximum Extension Distance for the Optical ESB Bus Repeater.

If Optical ESB Bus Repeater is set to [Yes] for SCSP1, the maximum distance can be set within the range from 5 to 50 km in 5 km units. If Optical ESB Bus Repeater is set to [Yes] for SCSV1, [5 km] can be set. The initial setting is 5 km.

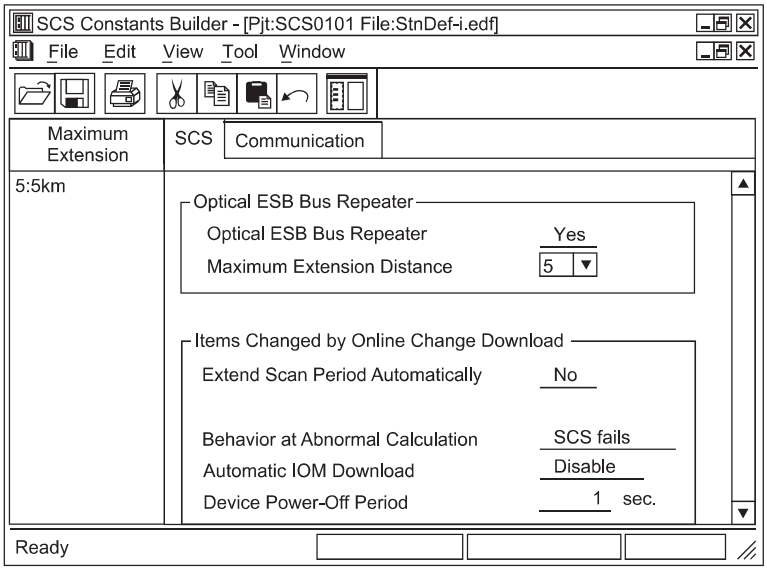


Figure C1.2.6-2 SCS tab of SCS Constants Builder

SEE ALSO For more information about specifying the SCSP1 node extension distance, refer to:

Appendix 1.1, “Setting items for nodes” on page App.1-2

Extend Scan Period Automatically

Select [Yes] or [No] to set whether to adjust the scan period of the application logic automatically. The default setting is [No]. If set to [Yes], the scan period will be extended automatically when the execution time of the application logic has extended the scan period specified on the SENG for some reasons. This prevents the communication performed by the SCS, for example, inter-SCS safety communication, from being discontinued. This setting is changeable by online change download.

SEE ALSO For more information about details on setting and checking the scan period of the application logic, refer to:

A7.2, “Automatic extension function for scan period of the application logic execution function” on page A7-5

Behavior at Abnormal Calculation

Select [SCS fails] or [SCS continues] to set the behavior of the SCS when an abnormal calculation has occurred in the application logic. The default setting is [SCS fails]. This setting is changeable by online change download.

SEE ALSO For more information about details on specifying the behavior at abnormal calculation, refer to:

G2.1.3, “Behavior at abnormal calculation” on page G2-7

Locking of Internal Variables: SCSP3/SCSL2/SCSP2

You can select [Enable] or [Disable] to set whether to lock the internal variables that are used in the application logic. This setting is displayed only when the SCS type is SCSP3, SCSL2, or SCSP2 and [Extend Scan Period Automatically] is set to [Yes]. By default, it is set to [Disable]. You can change this setting by online change download.

SEE ALSO For more information about details on locking internal variables, refer to:

"■ Locking internal variables" in F8.1, "Variable locking" in Engineer's Reference Manual (IM 32P04B10-01EN)

Automatic IOM Download

Select [Enable] or [Disable] to set whether to enable automatic IOM download. The default setting is [Disable]. This setting is changeable by online change download.

SEE ALSO For more information about Automatic IOM download details, refer to:

"■ Automatic execution of IOM download" on page I4-81

Device Power-Off Period

This item is used to reset the Smoke and Heat Detector.

You can set the number of seconds until the power ON command is output from when the function block HSDTR outputs a power OFF command. This is the number of seconds for which the Smoke and Heat Detector is power OFF. This setting is changeable by online change download.

- Setting range: 1 to 10 (seconds) (default: 1)

TIP This setting is displayed when using an SCS project newly created with a version of SENG that is R4.03.00 or later. However, this is not displayed with SCSV1. When importing an SCS project created with a version of SENG that is earlier than R4.03.00, an import error will occur with this item and the value will be set to 1.

Device Startup Waiting Period

This item is used to reset the Smoke and Heat Detector.

You can set the number of seconds until startup is completed from when the power of the Smoke and Heat Detector is turned ON. When there are multiple types of devices and equipment in the station, enter the maximum number of seconds. This setting is changeable by online change download.

- Setting range: 0 to 60 (seconds) (default: 0)

TIP This setting is displayed when using an SCS project newly created with a version of SENG that is R4.03.00 or later. However, this is not displayed with SCSV1. When an SCS project created with a version of SENG that is earlier than R4.03.00 is imported, this value is set to 0.

Alarm Suppression During Device Reset

This item is used to suppress the alarm during the reset status of the Smoke and Heat Detector.

You can set whether or not to suppress the display of system alarms and process alarms while the Smoke and Heat Detector is in the reset status. Set the value to [Enable] to suppress the display of system alarms and process alarms, or set the value to [Disable] to not suppress the display. This item cannot be changed by online change download.

TIP This setting is displayed when using an SCS project newly created with a version of SENG that is R4.03.00 or later. However, this is not displayed with SCSV1 and SCSU1. When an SCS project created with a version of SENG that is earlier than R4.03.00 is imported, this value is set to [Disable].

SEE ALSO For more information about engineering for resetting the Smoke and Heat Detector, refer to:

A3.4.4, “Engineering regarding the device reset function and alarm suppression during device reset” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Command Line

TIP Specify the command line with no more than 256 single-byte characters. If the command line is not set, the default value is used for each applicable item. The format is as follows:

Item name = Data value, Item name = Data value, ...

- PSINITIM (Fire and gas communication startup time)
  This item is the time required to initialize fire and gas communication during the SCS start-up processing. Before the initialization of fire and gas communication is completed, the data status of the data obtained by the communication is BAD. Therefore, specify this time to delay the completion of the startup of SCS. This setting is applicable to SCS in which one or more S2LP131 are defined.

  The number entered here is the communication cycle for GS01. The conversion from the GS01 communication cycle to the fire and gas communication startup time is implemented internally within the SCS.

  The formula is as follows:

  Fire and gas communication startup time (s) = 20 + (GS01 communication cycle + 8) x 4

  When the GS01 communication cycle is 12 seconds, the fire and gas communication startup time is 100 seconds.

  - Format
    PSINITIM=12
  - Parameter
    The configurable range is 8 to 30 seconds. The default value is 12 seconds.

Settings with the Communication Tab

On the Communication tab, you can set the following items:

Interval of Repeated Warning Alarms

This item should be set in the case of a CENTUM integration structure.

Set the time from the occurrence of a process alarm to the next occurrence of the same alarm. Repeated warning alarms are intended to notify the engineer that serious process alarms are existing continuously.

If the cause of an alarm still persists after a certain time has elapsed from the occurrence of the alarm, the process alarm message is sent again, regardless of whether or not the alarm is acknowledged.

The interval of repeated warning alarms can be specified in the range from 0 to 3600 seconds. The initial setting is 600 seconds.

If 0 is specified for the interval of repeated warning alarms, repeated warning alarms are disabled.

Synchronous Mode

This item allows specifying the method of synchronizing system time. The time of the SCS is used for the time stamps of messages recorded in SOERs.

For SCSV1, two options [IRIG-B] and [V net] are provided for time synchronization. The default is [V net].

For SCSP3/SCSL2/SCSP2/SCSP1, it is Vnet/IP time synchronization.

Table C1.2.6-1 Time Synchronous Mode

Method	Description
IRIG-B time synchronization	The time information is acquired from the externally installed GPS clock through IRIG-B and set to the CPU and I/O module. The GPS clock and CPU nodes of all SCSs are connected by IRIG-B. Specify this option when highly accurate synchronization is required for discrete input module time between different SCSs.
V net time synchronization	This method sets Vnet time to the CPU and I/O module. The Vnet time is also recorded in SOER.
Vnet/IP	This method sets Vnet/IP time to the CPU and I/O module. The Vnet/IP time is also recorded in SOER. If the SNTP server is connected to Vnet/IP network, the Vnet/IP time synchronizes with the SNTP server time.

Scan Period for External System

Specify the scan period used when connecting to external systems such as CENTUM. The scan period for external system setting refers to the operating period at which the connection function is executed.
Select either 1 second or 2 seconds. Default: 1 second.

Modbus Word Order

When establishing a connection with an external system and acquiring 32-bit data from the external system, the order of the most significant word and least significant word can be changed. Select either the order of the most significant word and then the least significant word, or the reverse order. The reverse order is used generally in Modbus. [Direct] is selected by default.

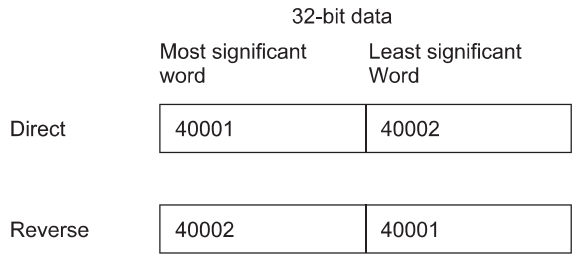


Figure C1.2.6-3 Modbus Word Order

16-bit Modbus Master Support Mode

This item specifies whether to allow the following accesses by the external Modbus master in Modbus slave communications.

These accesses are allowed when 16-bit Modbus master support mode is set to [Enable]. By default, it is set to [Disable].

- Write to a single holding register
  Function code is 06.
- Read 16-bit data
  Function codes are 03 and 04.
- Write 16-bit data
  Function code is 16.

Alarm Notify Action when AOF Released

This item should be set in the case of a CENTUM integration structure.
Specify to (or not to) output the suppressed messages when AOF is deactivated.

When you output the suppressed process alarm message, you need to set this setting to [Yes], otherwise, you can set this setting to [No]. By default, this setting is [No].

SEE ALSO For more information about activating/deactivating alarm suppression, refer to:

B8.2.4, “Alarm inhibition (AOF)” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

● PV Status of S_ANLG_S

This setting item is used for a CENTUM integration structure.
With this setting, whether to keep the PV status on the mapping block (S_ANLG_S) of ANLG_S (Analog Input Block with Data Status) can be defined. If you want to have BAD data status on the mapping block S_ANLG_S when the data status of IN terminal of ANLG_S block is BAD, you need to set this setting to [Yes], otherwise, you can set this setting to [No]. By default, this setting is [Yes].

● The first number of annunciator messages with tag name

You can specify the first number of annunciator messages with tag name (%AN).

The numbers from the specified number up to the maximum number of annunciator messages are used for annunciator messages with tag name.

However, if you specify 0 as the first number, all the numbers are used for annunciator messages instead of annunciator messages with tag name.

- For SCSP1/SCSU1: 0 to 1000
- For SCSP3/SCSL2/SCSP2: 0 to 2000

The initial setting is 0. It is not displayed in SCSV1.

● DNP3 Slave Function

When you use the DNP3 slave function, you need to set it to Enable, otherwise, you can set it to Disable. By default, it is set to Disable.

TIP This setting is displayed only for the SCS projects of SCSU1 that are created by the software version R3.02.20 or later. When the SCS projects that are created by the software prior to R3.02.20 are imported, this setting is set to Disable.

● Skip password dialog box for manual operation FB

This setting determines whether to skip the Password Input dialog box in HIS for MOA/MOB_11/MOB_21 FB when an empty string constant (′′) (two apostrophes) is specified in an input terminal (PSWD) that is used to set the password.

Set [No] if you do not want to skip the Password Input dialog box and [Yes] if you do. The initial value is [No] and the input dialog box is displayed even if the password is an empty string constant.

You can change this setting by online change download. This is not displayed for SCSV1 and SCSU1.

■ Change process alarm name of Analog Input Block with Data Status

The alarm name of the ANLG_S (Analog Input Block with Data Status) can be changed so as to match the alarm name on the diagnosis information window and SOE Viewer with the alarm name of CENTUM.

Before changing the alarm name, the CENTUM process alarm text strings need to be modified first. For more information about defining the process alarm text strings, please contact Yokogawa agents.

IMPORTANT

When applying this feature, if the SCS project to be monitored on CENTUM contains both ANLGI and ANLG_S blocks, the ANLGI blocks should be changed to ANLG_S blocks.

C2. Work flow of creating applications for each engineering method

After preparing the project, create applications by using the engineering functions.

The procedures for creating applications differ for each engineering method.

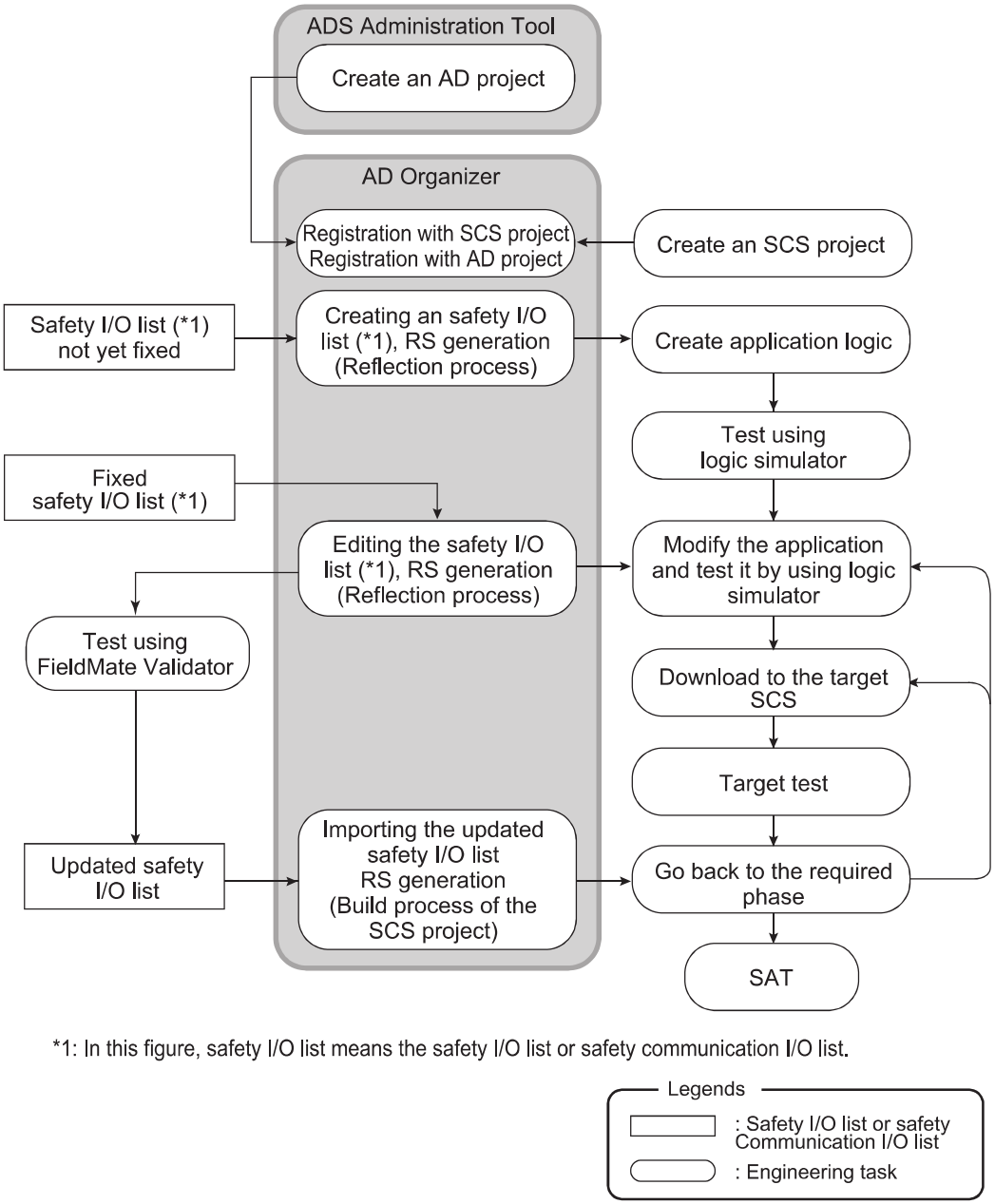
This chapter explains the engineering procedures and main points for each engineering method.

For modifying the application, it is necessary to analyze any effects caused by the modifications in advance and take the required measures against the effects.

C2.1 Work flow of I/O list engineering

This chapter explains the engineering flow of the I/O list engineering method. I/O list engineering is used even when you use iDefine as an engineering tool. Read the following section if you are using iDefine.

The following figure shows the engineering flow when using the AD Suite, SCS Manager, and FieldMate Validator. This flow describes only the differences from the flow of RS original engineering. By using FieldMate Validator, you can configure and adjust the I/O channels of universal type I/O modules without using the SCU.



*1: In this figure, safety I/O list means the safety I/O list or safety communication I/O list.

Figure C2.1-1 Engineering flow in AD Suite

SEE ALSO For more information about steps for I/O list engineering, refer to:

D., “Procedures to create applications using the I/O list engineering method” on page D-1

For more information about operations that are necessary when using iDefine, refer to:

C2.2, “Work flow of I/O list engineering with iDefine” on page C2-11

Engineering using a safety I/O list and safety communication I/O list

The safety application is a function element that can operate and control the plant in a safe manner, and is built mostly by using application logics based on input/out variables.

You can start building an application logic with the I/O variables being reflected onto Dictionary View from a safety I/O list and safety communication I/O list as long as you do not use iDefine as the engineering tool.

Handling of the safety I/O list and safety communication I/O list

The user can use the safety I/O list or safety communication I/O list to make definitions based on the P&ID tag name in the application, and proceed to build the application without having to wait for the detailed design of I/O modules or data communication.

The required information varies depending on whether the I/O addresses are set in the safety I/O list or safety communication I/O list.

When the I/O address is not set, the following information is required to create an application logic by using the safety I/O list or safety communication I/O list.

- Information required for the safety I/O list
  - P&ID tag name
  - I/O type (AI, AO, DI, DO)
  - I/O Tag
  - Signal Type
  - P&ID Group

  Information required to reflect variables onto Dictionary View is as follows:
  - P&ID tag name
  - I/O type (AI, AO, DI, DO)
  - I/O Tag
  - Data Type
  - P&ID Group
- Information required for the safety communication I/O list
  - P&ID tag name
  - I/O type (AI, AO, DI, DO)
  - Signal Protocol
  - I/O Tag
  - P&ID Group

  Information required to reflect variables onto Dictionary View is as follows:
  - P&ID tag name
  - I/O type (AI, AO, DI, DO)

    - Data Type
    - Signal Protocol
    - P&ID Group

  The type of the FB is decided as soon as the following information is decided:

    - I/O type (AI, AO, DI, DO)
    - Signal Protocol
    - Data Type

The P&ID tag name and the I/O type are mandatory to save the safety I/O list and safety communication I/O list.

When a safety I/O list or safety communication I/O list that contains I/O addresses is read by AD Organizer, IOM definitions are created by operating Create Node & IOM in IOM Definition Editor. The required information is as follows:

- Information required for the safety I/O list
    - SCS project name
    - RS project name
    - Node type
    - Node number
    - IOM category
    - IOM type
    - Unit number
    - Slot number
    - Terminal number
    - Signal type
- Information required for the safety communication I/O list
    - SCS project name
    - RS project name
    - Node type
    - Node number
    - IOM category
    - IOM type
    - Slot number

TIP

Even in a situation where the IOM definitions are not yet complete, the user can perform the reflection process in order to be able to define variables of safety I/O in POUs in the SCS project.

IMPORTANT

When using S2MMM843 or S2MDV843 in an explosion protection system, refer to the following document without fail because the approved values of the explosion protection parameters are different depending on the signal type.

ProSafe-RS/ProSafe-RS Lite Explosion Protection (TI 32S01J30-01E)

P&ID tag and P&ID group

The P&ID tag is a name that identifies an I/O point. The I/O points are identified by using the P&ID tag as the key while defining the I/O information for each line in the safety I/O list. The P&ID tag needs to be uniquely defined in the P&ID group.

The P&ID group is the label name required for identifying the safety I/O list or safety communication I/O list. The P&ID group name is used as the file name that is created under the I/O-List folder of the system configuration navigator of AD Organizer.

I/O Tag

The I/O Tag is a name that identifies an I/O point. The I/O Tag needs to be uniquely defined.

Engineering procedures for SCS I/O

This section describes the work flow for engineering regarding inputs/outputs.

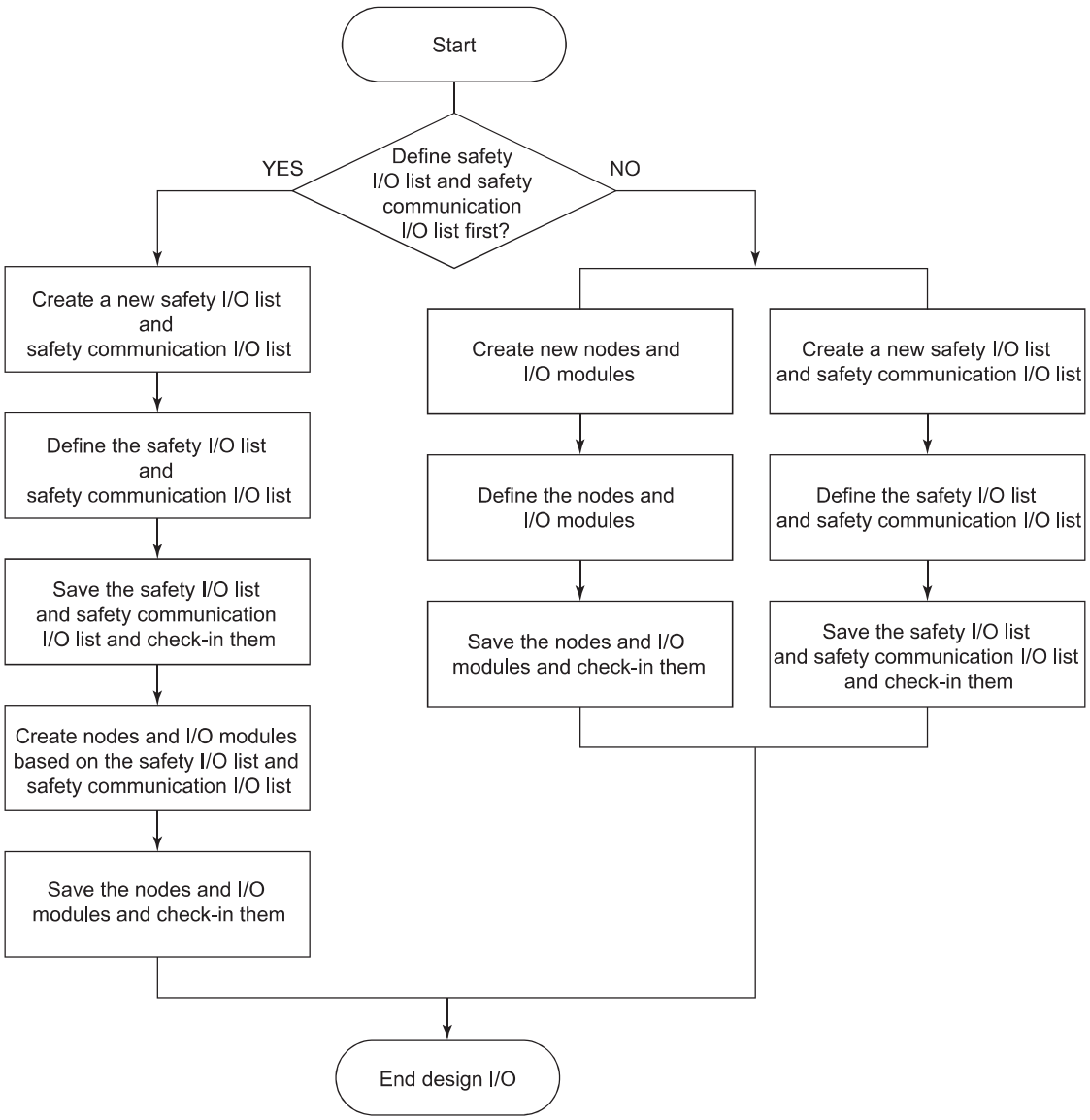


Figure C2.1-2 Work flow for engineering regarding inputs/outputs

The safety I/O list and safety communication I/O list can be created before or at the same time as an I/O module. By creating the safety I/O list and safety communication I/O list in advance, an application can be built alongside an I/O design.

Editor and tools that are used for I/O list engineering

The following table shows the editors and tools used when performing I/O list engineering.

You can start the SCS Manager from the System Structure Navigator in AD Organizer.

Table C2.1-1 Editor and tools that are used in I/O list engineering

Category	Operation	Means to operate editors and tools SCS Manager/AD Organizer	Editor or tool name	Remarks
Safety application	Safety logic definition	SCS Manager	Multi-Language Editor (*1)	-
	Variables and parameters definition	SCS Manager	Dictionary View (*1)	I/O variables are automatically created from the safety I/O list. Instances of subsystem communication I/O FB, PROFINET communication input FB, and fire and gas communication input FB are automatically generated from the safety communication I/O list. Internal variables and FB instances can be defined by iDefine.
I/O	I/O list definition	AD Organizer	Safety I/O Editor Safety Communication I/O Editor	The following information is generated: • Dictionary View • I/O Wiring View • I/O Parameter Builder • Communication I/O Builder
	Node/IOM detailed definition	AD Organizer	IOM Definition Editor	The information for the following is created: • I/O Wiring View • I/O Parameter Builder
System	Creation of SCS projects	SCS Manager	SCS Manager	The contents will be reflected in the AD Organizer.
	SCS project attribute	SCS Manager	SCS Project Properties	
	SCS constant definition	SCS Manager	SCS Constants Builder	-
	SCS parameter setting	SCS Manager	Hardware Architecture View	-
	POU definition	SCS Manager	Link Architecture View (*1)	-
	Safety communication association	SCS Manager	Binding List View	-
	SCS Link transmission data definition	SCS Manager	SCS Link Transmission Builder	-

Continues on the next page

Table C2.1-1 Editor and tools that are used in I/O list engineering (Table continued)

Category	Operation	Means to operate editors and tools SCS Manager/AD Organizer	Editor or tool name	Remarks
RS generation	Database generation	AD Organizer	RS Generation Manager	-
	Authorize	SCS Manager	Integrity Analyzer	-
		SCS Manager	Cross Reference Analyzer	-
Test	Start test function	SCS Manager	SCS Manager (*1)	-
Download	Offline download	SCS Manager	SCS Manager	-
	Online download	SCS Manager	SCS Manager	-
CENTUM integration	Tag and annunciator definition	SCS Manager	Tag Name Builder (*1)	-
	Alarm definition	SCS Manager	ProSafe-RS Alarm Priority Builder / Alarm Processing Table Builder	-
MODBUS communication	Definition of addresses of Modbus devices	SCS Manager	Modbus Address Builder	-
Subsystem communication	Communication I/O data definition	AD Organizer	Safety Communication I/O Editor	-
Safety subsystem communication	Communication I/O data definition	AD Organizer	Safety Communication I/O Editor	-
DNP3 communication	DNP3 slave definition	SCS Manager	DNP3 Communication Builder	-

*1: iDefine can be used as well.

Procedure for I/O list engineering without iDefine

The procedure for I/O list engineering without using iDefine is described as follows. The AD project is defined as a prerequisite.

1. Configure the I/O modules and I/O variables.
   Import the safety I/O list or safety communication I/O list and then add or modify I/O variables by using AD Organizer. Define the I/O modules and I/O parameters as well.
2. When using the fire and gas communication function, define fire and gas communication modules and fire and gas communication.
3. Select an SCS project and run Reflection.
4. Use the Multi-Language Editor and Link Architecture View of SCS Manager to create and modify POUs for the safety application.
5. Create applications other than the application logic and generate the databases to download to SCS.
6. Examine the created application by using Safety Analyzer.

SEE ALSO For more information about details on how to create an application logic, refer to:

A., “Configuring application” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Creating a communication I/O list for a subsystem communication module

For SCS projects created in R4.01 to R4.03.00, you must enable the setting items of the subsystem communication modules to be handled in a safety communication I/O list.

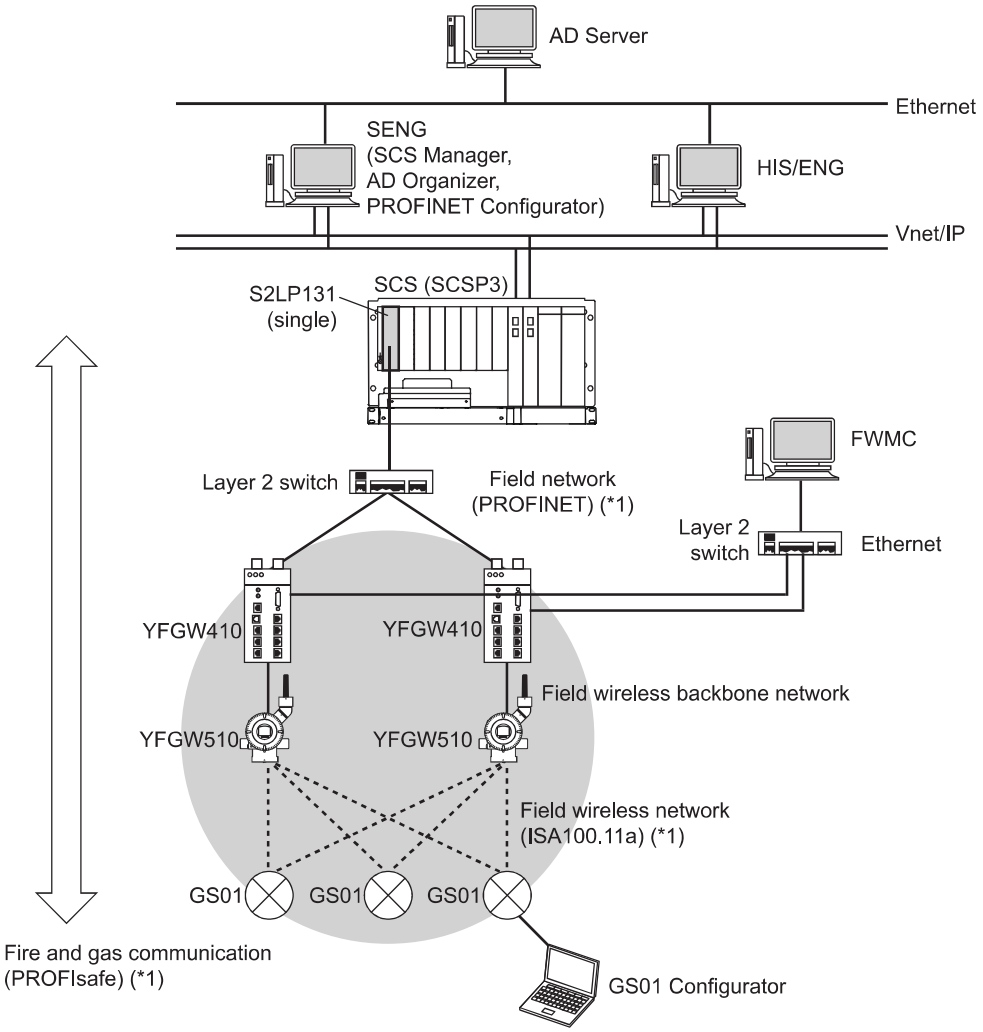
SEE ALSO For more information about how to create a safety communication I/O list, refer to:

“■ Communication I/O List Output Tool” on page App.3-16

Engineering for fire and gas communication modules

Engineering for fire and gas communication modules can be implemented with I/O list engineering only.

Fire and gas communication modules are used for safety communication with Gas Detector GS01 from GasSecure AS. The following figure shows an example of device configuration.



*1: For fire and gas communication, PROFINET is used as the field network between SCS and YFGW410 and ISA100.11.a as the field wireless network. In addition, the PROFIsafe protocol is used for the safety layer of fire and gas communication.

Figure C2.1-3 Example of system configuration using fire and gas communication modules

Fire and gas communication modules can be defined with Safety Communication I/O Editor and used in SCS projects of SCSP3.

Overall flow of engineering for fire and gas communication

The following figure shows the flow of engineering for fire and gas communication.

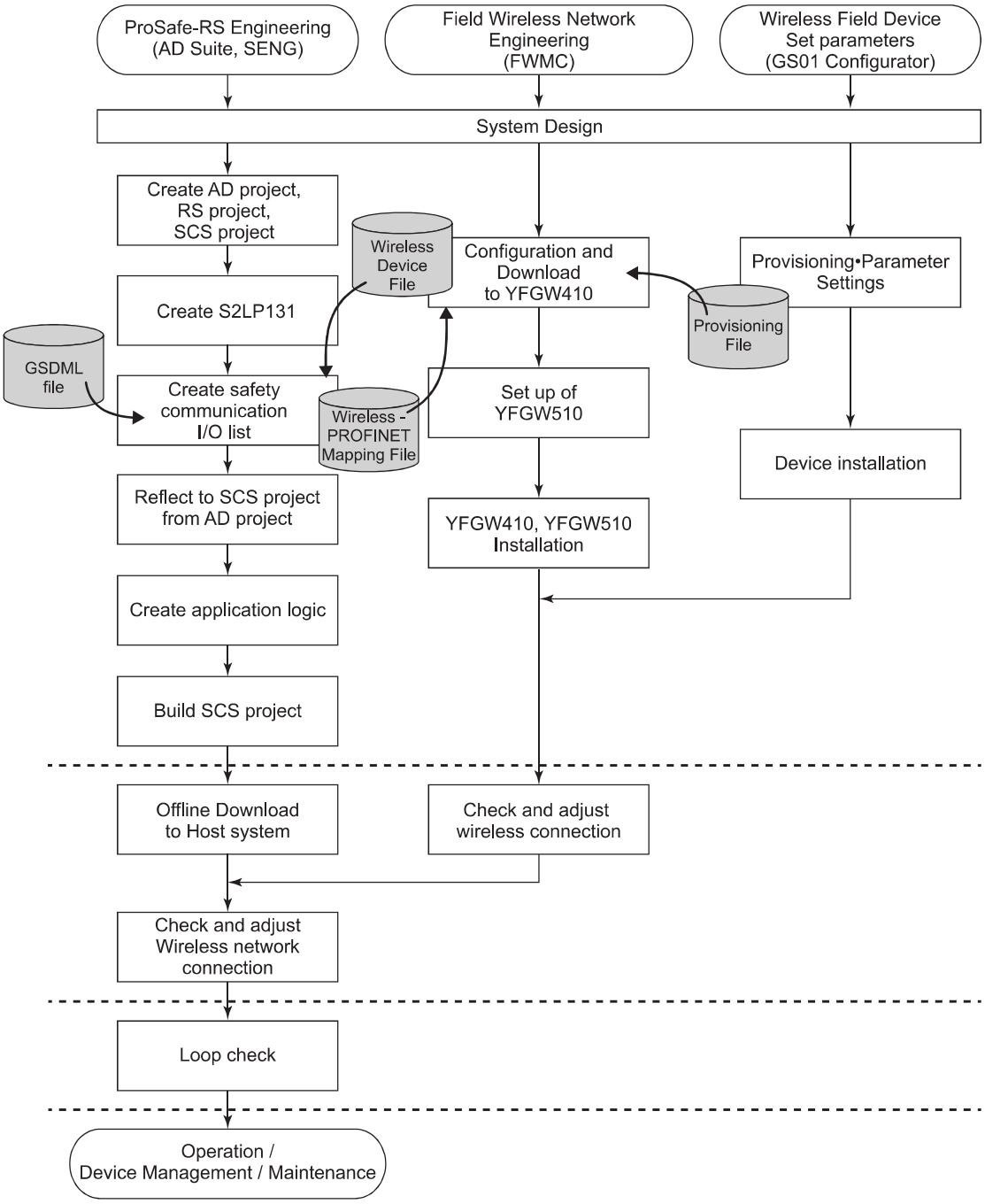


Figure C2.1-4 Flow of engineering for fire and gas communication

The following engineering is required to build a system for fire and gas communication:

- Engineering for SCS
- Engineering for a field wireless network
- Engineering for wireless field devices

SEE ALSO For more information about details of ProSafe-RS engineering, refer to:

E1.5, “Engineering for fire and gas communication” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

C2.2 Work flow of I/O list engineering with iDefine

In the case of I/O list engineering, you can use iDefine for part of the engineering and testing process. This section explains the following important points for using iDefine:

- System configurations of ProSafe-RS and iDefine
- ProSafe-RS engineering functions and iDefine interface
- Engineering flow when using iDefine

IMPORTANT

When using ProSafe-RS and iDefine, use ProSafe-RS R4.02 to R4.08.

If you want to use SENG to edit engineering data created with iDefine, contact YOKOGAWA.

C2.2.1 System configuration when using iDefine

When using iDefine in ProSafe-RS, you can install ProSafe-RS (AD Organizer and SENG) and iDefine on the same computer or on separate computers.

The following figure shows an example of the system configurations when ProSafe-RS and iDefine are installed on the same computer.

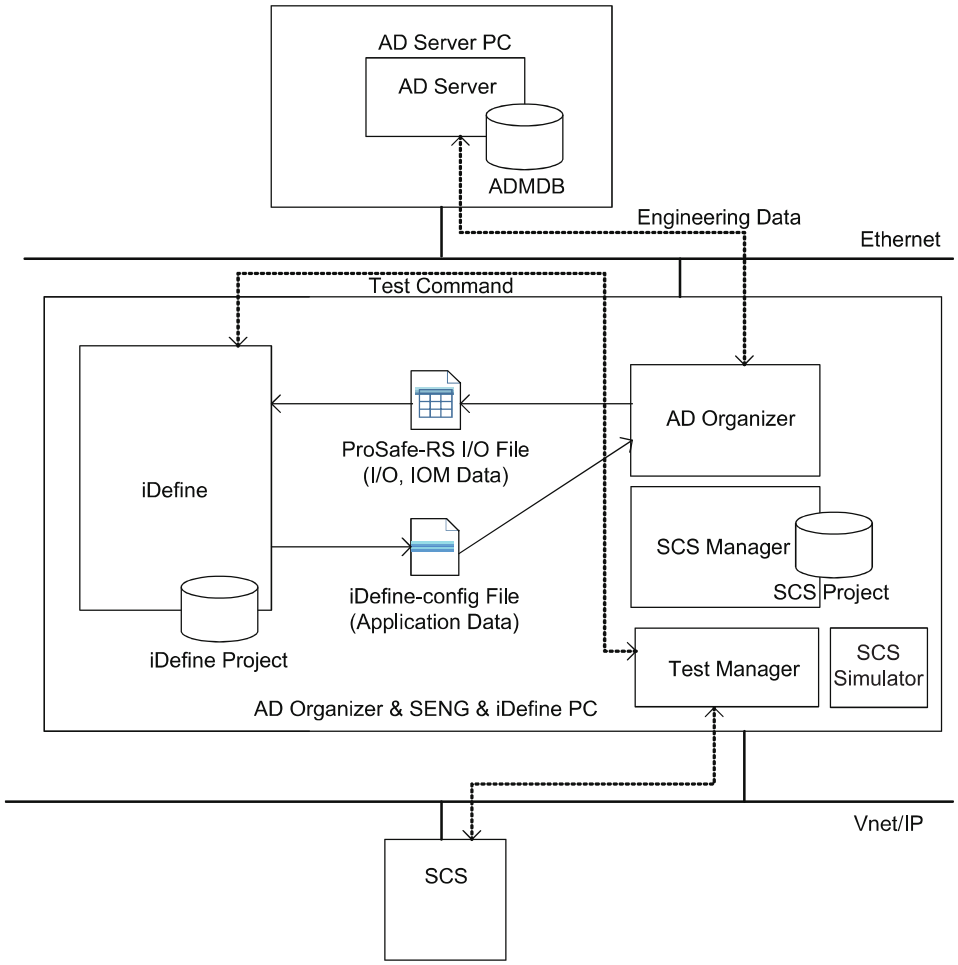


Figure C2.2.1-1 System configurations of ProSafe-RS and iDefine

C2.2.2 Relationship between ProSafe-RS engineering functions and iDefine

The following describes the relationship between ProSafe-RS engineering functions and iDefine when using iDefine.

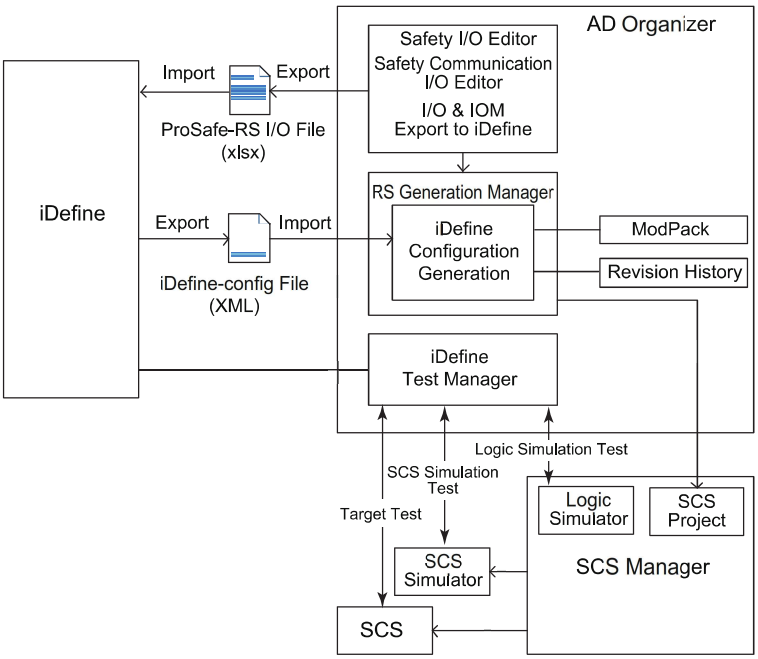


Figure C2.2.2-1 Relationship between ProSafe-RS engineering functions and iDefine

iDefine is used in the following ways in the application creation phase:

- iDefine can manage the data from multiple SCS projects. The engineer should decide how best to manage and associate iDefine projects with ProSafe-RS projects.
- The IOM definition, safety I/O list, and safety communication I/O list are managed in AD Suite and exported for iDefine as a ProSafe-RS I/O file in the xlsx format.
- The user creates an application in iDefine. Using information on the I/O of SCS, the ProSafe-RS I/O file that was generated from AD Organizer is imported and put to use. Engineering results are written as iDefine-config files in XML format for each SCS.
- The iDefine-config files that were generated are imported to AD Suite and reflected in SCS projects.

IMPORTANT

When starting iDefine from AD Organizer, there is no need to export the ProSafe-RS I/O file manually. You can import the I/O and IOM definitions of AD Organizer directly in iDefine. The iDefine-config file is imported directly from iDefine to AD Organizer.

- Data created by using iDefine such as POU and variables become read-only after it is reflected in SCS Manager.
- The run sequence of the POUs that were created by using the Multi-Language Editor can be changed in the Multi-Language Editor. The run sequence of the POUs that were created by using iDefine can be changed in iDefine.
- iDefine-config files can be assigned to ModPack in AD Suite. The history of iDefine-config files is also managed.

Logic simulation tests, SCS simulation tests, and target tests can be run from the iDefine test function.

- Launch iDefine Test Manager in AD Suite.
- iDefine can be connected with the logic simulator and SCS simulator of SCS Manager, and the actual SCS through iDefine Test Manager.
- Tests can be run using the iDefine test function.

Interface between ProSafe-RS and iDefine

ProSafe-RS I/O file and iDefine-config file serve as the interface between ProSafe-RS and iDefine.

- ProSafe-RS I/O file
  It includes information on the safety I/O list, safety communication I/O list, and I/O modules that are saved in ADMDB.

  The following items must be configured in the safety I/O list:

  - P&ID Tag
  - I/O Type (AI, AO, DI, DO)
  - I/O Tag
  - Signal Type
  - P&ID Group

  The following items must be configured in the safety communication I/O list:

  - P&ID Tag
  - I/O Type (AI, AO, DI, DO)
  - Signal Protocol
  - I/O Tag
  - P&ID Group

  If a value has been entered in the column for iDefine reference, such as Typical, in Safety I/O Editor and Safety Communication I/O Editor, you can view the value for reference purposes in iDefine.

  The safety I/O parameter profile defined in AD Organizer can be used as the I/O Parameter Profile of iDefine.

  Data that is checked-in to the AD Server is exported.

  The file is in the xlsx format with five worksheets.

  The following table shows the relationship between each worksheet and each iDefine editor.

Table C2.2.2-1 Relationship between the worksheets in ProSafe-RS I/O file and iDefine editors

Worksheet	iDefine editor
CIO worksheet	Client IO Table
IO worksheet	Client IO Table
IO Parameter worksheet	ProSafe-RS IO Parameter
Node worksheet	ProSafe-RS IO Node
IOM worksheet	ProSafe-RS IO Module

The content defined with Safety I/O Editor is not exported to the CIO worksheet.

The content defined with Safety Communication I/O Editor is not exported to the IO worksheet and the IO Parameter worksheet.

The following table shows the conditions for reflecting the data that is managed in AD Suite in each worksheet in the ProSafe-RS I/O file based on the rules for assigning information.

Table C2.2.2-2 Conditions for definitions of Safety I/O Editor being reflected onto the ProSafe-RS I/O file

Definition status of the I/O signal	Worksheet in the ProSafe-RS I/O file	Are definitions reflected onto the worksheet?
The I/O module to which the I/O signal is to be assigned is determined and the node to which the I/O module is to be assigned is already defined in IOM Definition Editor. However, the I/O module is not defined in IOM Definition Editor.	IO worksheet	Yes
	IO Parameter worksheet	Yes
	Node worksheet	Yes
	IOM worksheet	No
The I/O module to which the I/O signal is to be assigned is determined. However, the node to which the I/O module is to be assigned is not defined in IOM Definition Editor.	IO worksheet	Yes
	IO Parameter worksheet	Yes
	Node worksheet	No
	IOM worksheet	No
The I/O module to which the I/O signal is to be assigned is not determined yet. For example, one of the following columns in Safety I/O Editor is empty: • RS Project • SCS • Node Type • Node • IOM Category • IOM Type • Unit (For N-IO) • Slot • Terminal	IO worksheet	Yes
	IO Parameter worksheet	Yes (*1)
	Node worksheet	No
	IOM worksheet	No
The I/O Tag is not defined in the I/O signal.	IO worksheet	No
	IO Parameter worksheet	No
	Node worksheet	No
	IOM worksheet	No

*1: When a value has been entered for IOM Type

Table C2.2.2-3 Conditions for definitions of Safety Communication I/O Editor being reflected onto the ProSafe-RS I/O file

Definition status of the I/O signal	Corresponding worksheet	I/O signal definitions reflected?
The communication I/O module to which the communication I/O signal is to be assigned is determined and the node to which the communication module is to be assigned is already defined in IOM Definition Editor. However, the communication module is not defined in IOM Definition Editor.	CIO worksheet	Yes
	Node worksheet	Yes
	IOM worksheet	No

Continues on the next page

Table C2.2.2-3 Conditions for definitions of Safety Communication I/O Editor being reflected onto the ProSafe-RS I/O file (Table continued)

Definition status of the I/O signal	Corresponding worksheet	I/O signal definitions reflected?
The I/O Tag is defined in the communication I/O signal and the communication module to which the communication I/O signal is to be assigned is determined. However, the node to which the communication module is to be assigned is not defined in IOM Definition Editor.	CIO worksheet	Yes
	Node worksheet	No
	IOM worksheet	No
The I/O Tag is not defined in the communication I/O signal.	CIO worksheet	No
	Node worksheet	No
	IOM worksheet	No

- iDefine-config file
  This includes the POU, defined words, internal variables, FB instances, tag names, and parameters that were created by using iDefine.

  The file is in XML format.

SEE ALSO For more information about columns for iDefine reference, refer to:

"■ Setting items of the Safety I/O Editor" on page D1-7

■ Data from iDefine that is reflected in SCS Manager

When you import the iDefine-config file exported from iDefine into AD Organizer and run Reflection from RS Generation Manager, the data is reflected in the SCS Manager view and builders.

Table C2.2.2-4 Where data included in the iDefine-config file is reflected

Data in the iDefine-config file	Destination
POU	Link Architecture View
Internal variables and user defined FB instances (*1)	Dictionary View
Defined words	Dictionary View
Tag names and parameter	Tag Name Builder (*2)

*1: I/O variables and communication FB instances are not generated by iDefine. These are generated based on definitions of AD Organizer. The variables for instances of subsystem communication I/O FB can be defined with Safety Communication I/O Editor.
*2: It is reflected only when the CENTUM VP Integration Package or the CI Server Integration Package is enabled.

■ Selecting a FB with an instance name

From the function blocks that were defined in the POU that was created by using iDefine, you can select according to the type, the function blocks with instance name after imported to the SCS project. Select a function block with an instance name before you run Build All in iDefine. If you are starting iDefine directly, you can also select a function block with an instance name when importing the iDefine-config file to AD Organizer.

C2.2.3 Engineering by using iDefine

Applications can be created in iDefine by using the I/O list engineering method. The following methods are available for engineering by using iDefine depending on how iDefine is started:

- Starting iDefine from AD Organizer
- Starting iDefine directly

If you start iDefine from AD Organizer, operations between AD Organizer and iDefine are automated, and you can operate with reduced steps, for example, you do not have to start or switch tools, or check in.

If you start iDefine directly, you must import, export, and check in files, as well as start and switch tools.

This section describes the operation flow depending on how iDefine is started and details on the engineering method for iDefine, including AD Suite.

Refer to the following if you want to confirm the operation flow depending on how iDefine is started:

- Operation flow when starting iDefine from AD Organizer
- Operation flow when starting iDefine directly

Refer to the following if you want to confirm the details on the engineering method for iDefine, including AD Suite:

- Engineering flow when using iDefine

SEE ALSO For more information about the details of engineering using iDefine, refer to:

- iDefine User Guide (PR03076-MAN-970_01)
- iDefine User Guide (Yokogawa Extensions) (PR12002-MAN-980_01)

Operation flow when starting iDefine from AD Organizer

If AD Organizer and iDefine have been installed on the same computer, you can start iDefine from AD Organizer.

The following figure shows the operation flow when starting iDefine from AD Organizer.

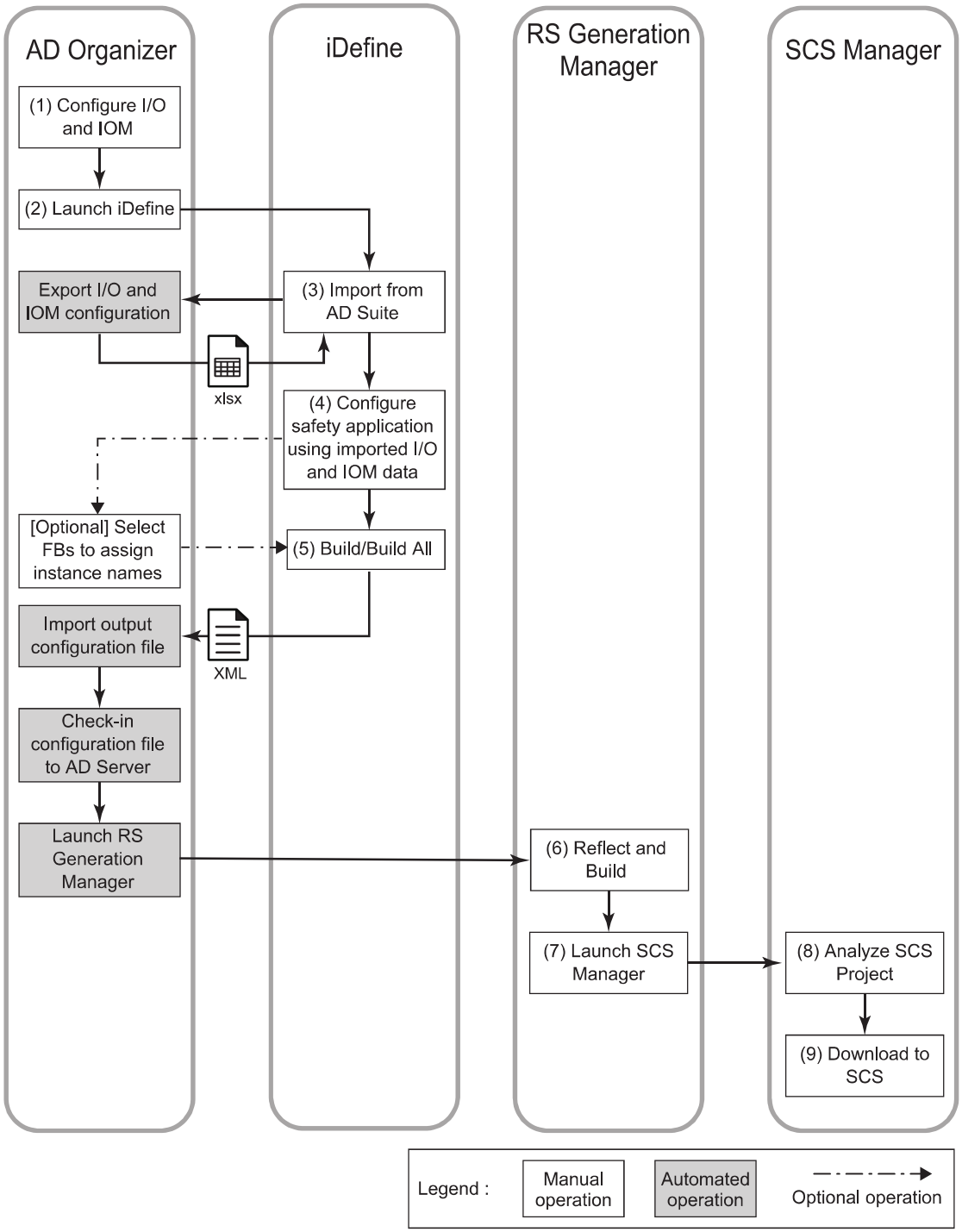


Figure C2.2.3-1 Operation flow when starting iDefine from AD Organizer

SEE ALSO

For more information about engineering steps when starting iDefine from AD Organizer, refer to:

D5.1, “Engineering steps when starting iDefine from AD Organizer” on page D5-2

For more information about I/O settings, refer to:

- D1., “Engineering based on the safety I/O list” on page D1-1
- D2., “Engineering based on the safety communication I/O list” on page D2-1

For more information about IOM settings, refer to:

D3., “Input/output module configuration definition” on page D3-1

For more information about the start of iDefine and selection of FB to generate instances with names, refer to:

D5.1.1, “Operations in AD Organizer” on page D5-3

For more information about importing from AD Suite, refer to:

D5.1.2, “Operations in iDefine” on page D5-5

For more information about specific operations in iDefine, refer to:

- iDefine User Guide (PR03076-MAN-970_01)
- iDefine User Guide (Yokogawa Extensions) (PR12002-MAN-980_01)

For more information about the reflect, build and start of SCS Manager, refer to:

D5.1.3, “Operations in RS Generation Manager” on page D5-7

For more information about the analysis of SCS projects, refer to:

C5., “Testing with the Safety Analyzers” on page C5-1

For more information about download to the SCS, refer to:

C7., “Offline download to the target SCS” on page C7-1

Operation flow when starting iDefine directly

The following figure shows the operation flow when starting iDefine directly.

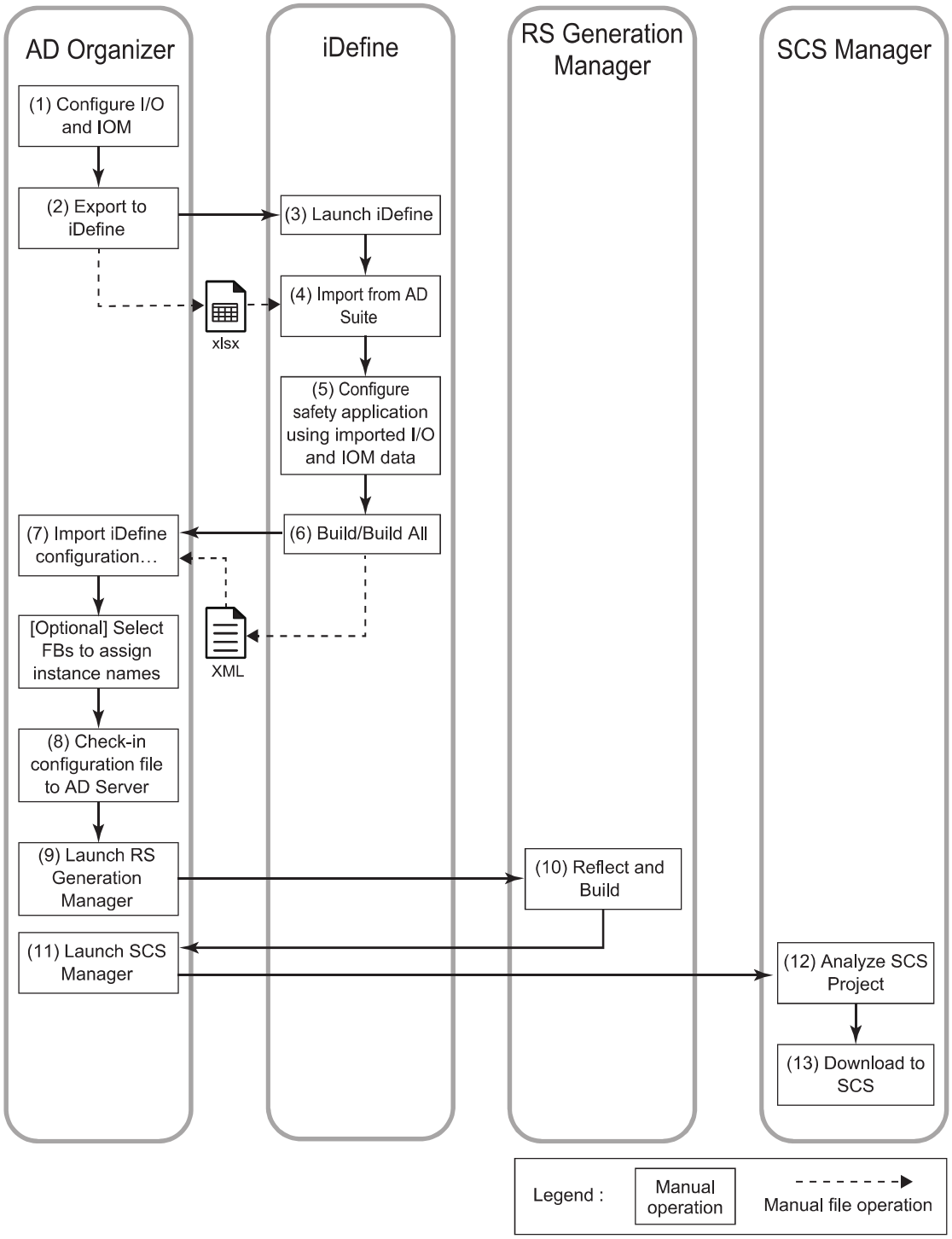


Figure C2.2.3-2 Operation flow when starting iDefine directly

SEE ALSO For more information about engineering steps when starting iDefine directly, refer to:

D5.2, “Engineering steps when starting iDefine directly” on page D5-8

For more information about I/O settings, refer to:

- D1., “Engineering based on the safety I/O list” on page D1-1
- D2., “Engineering based on the safety communication I/O list” on page D2-1

For more information about IOM settings, refer to:

D3., “Input/output module configuration definition” on page D3-1

For more information about exporting to iDefine, refer to:

D5.2.1, “Exporting the ProSafe-RS I/O file from AD Organizer” on page D5-9

For more information about the start of iDefine, refer to:

D5.2.2, “Operations in iDefine” on page D5-10

For more information about specific operations in iDefine, refer to:

- iDefine User Guide (PR03076-MAN-970_01)
- iDefine User Guide (Yokogawa Extensions) (PR12002-MAN-980_01)

For more information about the import of iDefine configurations and selection of FB to generate instances with names, refer to:

D5.2.3, “Import the iDefine-config file by using AD Organizer” on page D5-11

For more information about the reflect, build, and start of RS Generation Manager, refer to:

D4.4, “Operating procedure of RS generation” on page D4-8

For more information about starting SCS Manager, refer to:

A10.2, “SCS Manager” on page A10-3

For more information about the analysis of SCS projects, refer to:

C5., “Testing with the Safety Analyzers” on page C5-1

For more information about download to the SCS, refer to:

C7., “Offline download to the target SCS” on page C7-1

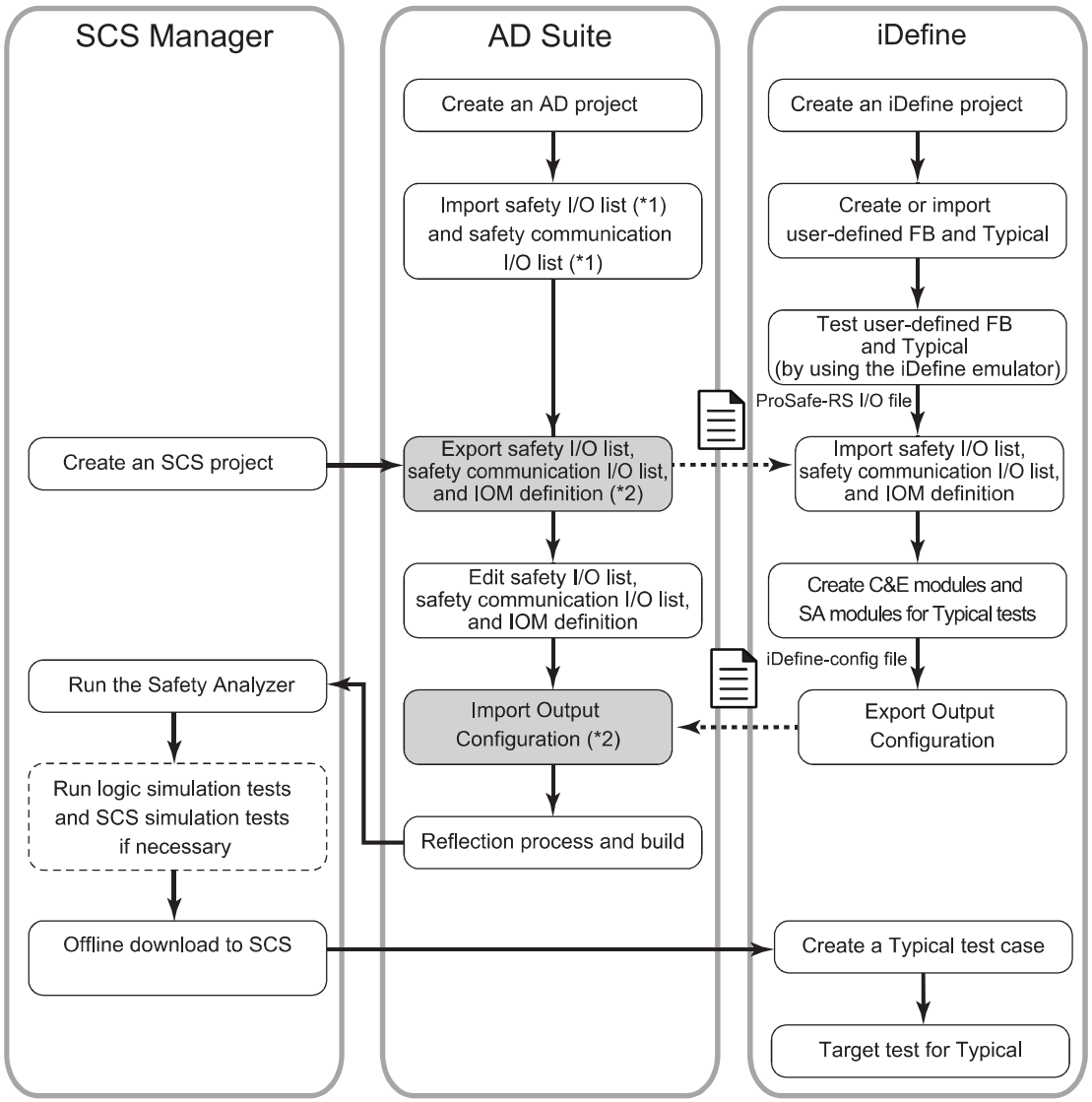
Engineering flow when using iDefine

The engineering flows when using iDefine are described in each of the following flows:

- Work flow from the start of engineering until the end of Typical test
- Work flow for engineering and testing the POU and I/O data of the SCS

Work flow from the start of engineering until the end of Typical test

iDefine breaks into parts the typical logic, such as the common input and output processes of application logics, and registers them as a template in Typical. Unit tests can be run on registered Typicals by using the emulator on iDefine, but sometimes the test function in SCS Manager is also used for testing to prevent engineering regression. However, it is possible that the specification for the application logic and I/O definition have not been finalized at this stage. In such a case, you need to configure a dummy I/O and logic, which is the bare minimum required to run a Typical test. The following figure explains the tasks that need to be done in SCS Manager, AD Suite, and iDefine in order to run a Typical test by using SCS.



*1: Data that is required to test Typical is included, as well as a tentative safety I/O list
*2: Operations that run automatically if you install AD Suite and iDefine on the same computer and start iDefine from AD Organizer.

Figure C2.2.3-3 Work flow for running a Typical test

SEE ALSO

For more information about creating AD projects, refer to:

C1.2.1, “Creating and deleting AD projects” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about the import of the safety I/O list, refer to:

D1.4.2, “Importing the I/O information list” on page D1-16

For more information about the import of the safety communication I/O list, refer to:

D2.6, “Importing I/O information into the safety communication I/O list” on page D2-30

For more information about the creation of SCS projects, refer to:

C1.2.4, “Creating SCS projects” on page C1-15

For more information about the export of the safety I/O list, refer to:

D1.4.5, “Exporting the I/O information in the safety I/O list” on page D1-23

For more information about the export of the safety communication I/O list, refer to:

D2.7, “Exporting the I/O information in the safety communication I/O list” on page D2-33

For more information about the export of IOM definitions, refer to:

D3.7, “Exporting information from IOM Definition Editor” on page D3-12

For more information about specific operations in iDefine, refer to:

- iDefine User Guide (PR03076-MAN-970_01)
- iDefine User Guide (Yokogawa Extensions) (PR12002-MAN-980_01)

For more information about editing the safety I/O list, refer to:

D1.4.4, “Editing a safety I/O list” on page D1-21

For more information about editing the safety communication I/O list, refer to:

D2.4, “Entering I/O information in the signal definition list” on page D2-17

For more information about editing IOM definitions, refer to:

D3.5, “Editing the setting items of the node and I/O module” on page D3-10

For more information about the import of output configurations, refer to:

D5.2.3, “Import the iDefine-config file by using AD Organizer” on page D5-11

For more information about the reflection process and build, refer to:

D4.4, “Operating procedure of RS generation” on page D4-8

For more information about the implementation of Safety Analyzer, refer to:

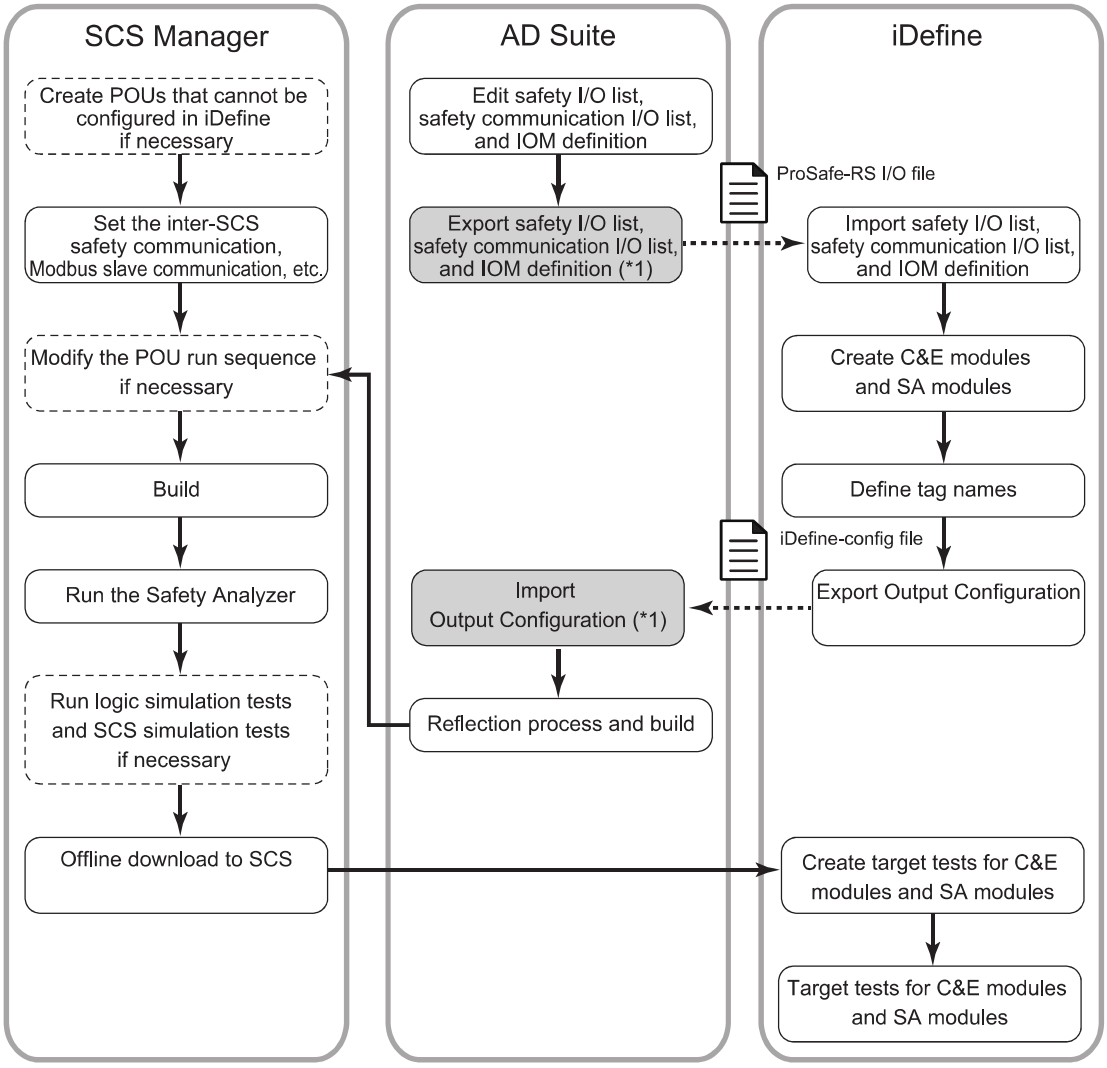
C5., “Testing with the Safety Analyzers” on page C5-1

For more information about offline download to the SCS, refer to:

C7., “Offline download to the target SCS” on page C7-1

Work flow for engineering and testing the POU and I/O data of the SCS

After you have completed the Typical test, engineer using the safety I/O list or safety communication I/O list after the specifications have been defined and run a target test by using SCS.



*1: Operations that run automatically if you install AD Suite and iDefine on the same computer and start iDefine from AD Organizer.

Figure C2.2.3-4 Work flow for running a target test

SEE ALSO

For more information about POUs that can be created in iDefine, refer to:

"■ Functions and function blocks" on page D5-14

For more information about editing the safety I/O list, refer to:

D1.4.4, "Editing a safety I/O list" on page D1-21

For more information about editing the safety communication I/O list, refer to:

D2.4, "Entering I/O information in the signal definition list" on page D2-17

For more information about editing IOM definitions, refer to:

D3.5, "Editing the setting items of the node and I/O module" on page D3-10

For more information about the export of the safety I/O list, refer to:

D1.4.5, "Exporting the I/O information in the safety I/O list" on page D1-23

For more information about the export of the safety communication I/O list, refer to:

D2.7, "Exporting the I/O information in the safety communication I/O list" on page D2-33

For more information about the export of IOM definitions, refer to:

D3.7, "Exporting information from IOM Definition Editor" on page D3-12

For more information about specific operations in iDefine, refer to:

- iDefine User Guide (PR03076-MAN-970_01)
- iDefine User Guide (Yokogawa Extensions) (PR12002-MAN-980_01)

For more information about the import of output configurations, refer to:

D5.2.3, “Import the iDefine-config file by using AD Organizer” on page D5-11

For more information about the reflection process and build, refer to:

D4.4, “Operating procedure of RS generation” on page D4-8

For more information about building in SCS Manager, refer to:

C4., “Procedures for generating a database” on page C4-1

For more information about the implementation of Safety Analyzer, refer to:

C5., “Testing with the Safety Analyzers” on page C5-1

For more information about offline download to the SCS, refer to:

C7., “Offline download to the target SCS” on page C7-1

C2.3 Work flow for RS original engineering

The following figure shows the engineering flow from the creation of an RS project and SCS project to the backing up of the projects (check-in) after completion in RS original engineering.

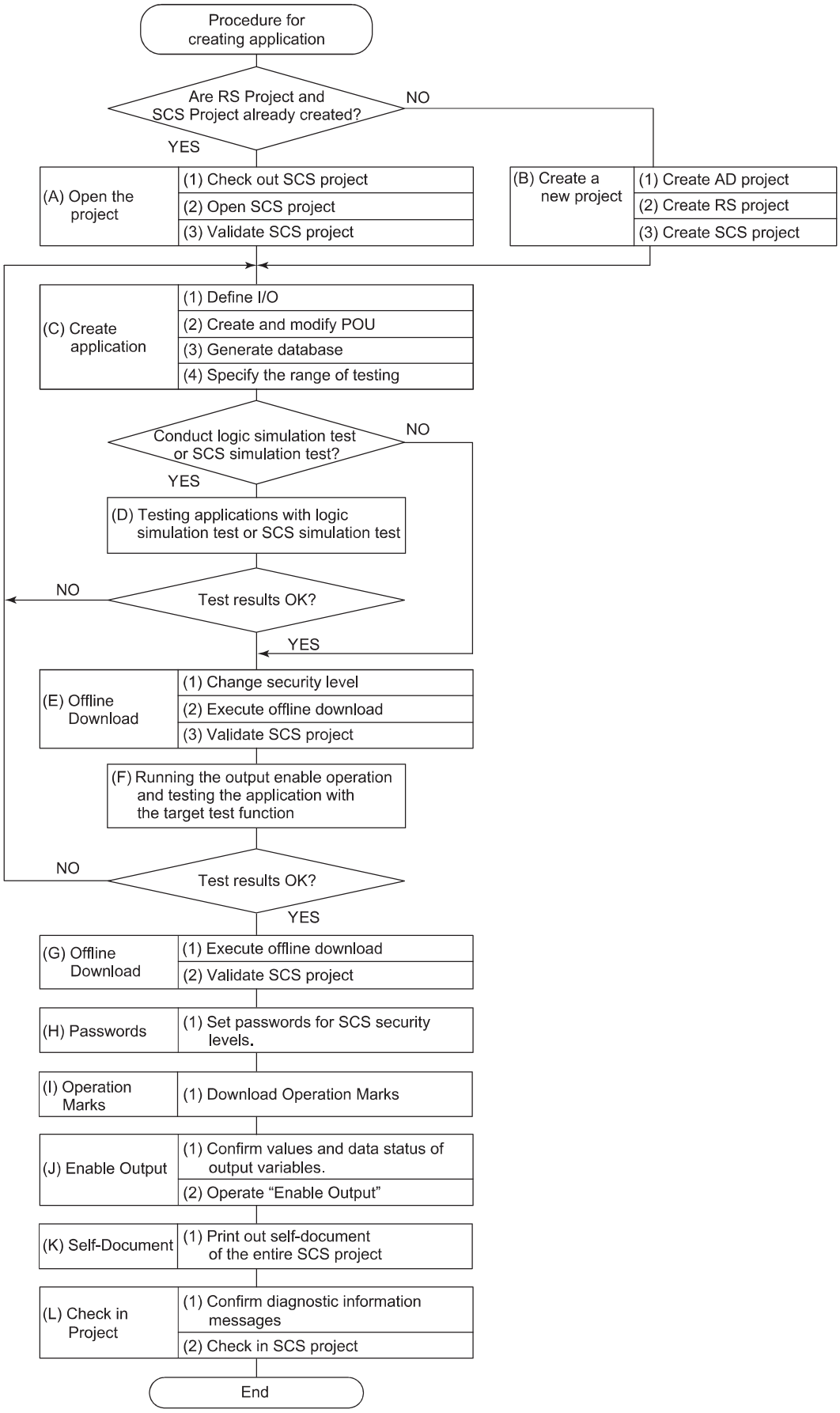


Figure C2.3-1 Procedure of creating an application

Detailed procedure for creating a new application

(A) Opening the project

Table C2.3-1 Procedure for opening the project

Item	Description
(1) Check out SCS project	• When check-in is performed by temporarily discontinuing on-going creation of an application, you can check out the created SCS project by using the Version Control Tool.
(2) Open SCS project	• Launch the SCS Manager. • Open the SCS project. • Enter the password for the SCS project.
(3) Validate SCS project	• Run the Database Validity Check Tool and check that the CRC codes and generation times of the databases are consistent between the SCS and SCS project. • Repair a database if there is a discrepancy in the database.

(B) Creating a new project

Table C2.3-2 Procedure for creating a new project

Items	Description
(1) Create an AD project	Perform the following tasks by using the ADS Administration Tool: • Set the ADMDB location • Create an AD project
(2) Create an RS project	• Only one folder of RS project is automatically created when the engineering function is installed. You need to set the folder of the RS project as a shared folder. • Then you can use AD Organizer to register the RS project in the AD project.
(3) Create an SCS project	To create a new SCS project, you need to configure the following settings by using SCS Manager: • Folder for SCS project • Properties of SCS project • Resource • Configuration • IP address

(C) Creating an application

Table C2.3-3 Procedure for creating an application

Items	Description
(1) Define Input/Output	• Define I/O variables.(Dictionary View) • Define I/O modules.(I/O Wiring View) • Perform wiring of channels and I/O variables (I/O Wiring View). • Set parameters for nodes, I/O modules and channels.(I/O Parameter Builder)
(2) Create and modify POU	• Open POU which you want to create and modify. • Edit POU. • Save POU. • Print POU. • Confirm that the logic entered in Multi-Language Editor is the same as the logic printed by using the self-document function. • Confirm that the execution order of FB/FU is correct.
(3) Generate database	• Perform build. • Analyze and confirm that the safety applications such as FU/FB are correct in terms of safety by using the Integrity Analyzer.

Continues on the next page

Table C2.3-3 Procedure for creating an application (Table continued)

Items	Description
(4) Specify the range of testing	• Run the Cross Reference Analyzer to check the changed Program Organization Unit (POU) and the affected POU and then authorize them. Then, visually check the following setting items, which are critical for safety, to be sure that there are no unintended changes, because changes in these items cannot be detected by the Cross Reference Analyzer. [Cycle Timing] in Resource Properties of SCS Manager Items in SCS Constants Builder: • [Optical ESB Bus Repeater] (for SCSP1/SCSV1) • [Maximum Extension Distance] (for SCSP1/SCSV1) • [Extend Scan Period Automatically] • [Behavior at Abnormal Calculation] • [Automatic IOM Download] • [Locking of Internal Variables] (for SCSP3/SCSL2/SCSP2) • [Device Power-Off Period] (for SCSP3/SCSL2/SCSP2/SCSP1/SCSU1) • [Device Startup Waiting Period] (for SCSP3/SCSL2/SCSP2/SCSP1/SCSU1) • [Skip Password Dialog Box for Manual Operation FB] (for SCSP3/SCSL2/SCSP2/SCSP1)

SEE ALSO For more information about Integrity Analyzer, refer to:

C5.1, “Integrity Analyzer” on page C5-2

For more information about Cross Reference Analyzer details, refer to:

C5.2, “Cross Reference Analyzer” on page C5-19

(D) Testing the application with the SCS simulation test or Logic simulation test function

Test the user application by using the SCS simulation test or logic simulation test.

SEE ALSO For more information about details of SCS simulation test and logic simulation test, refer to:

C6., “Simulation tests” on page C6-1

(E) Offline download

Table C2.3-4 Procedure for offline download

Items	Description
(1) Change Security Level	• Start the SCS Maintenance Support Tool which monitors the SCS from the SCS Manager. • Set the SCS security level to 0. Entering a password is required. • Confirm that the SCS Security Level is 0 on the SCS State Management window of the SCS Maintenance Support Tool. • Confirm the diagnostic information message indicating the security level at 0 with the SCS Maintenance Support Tool.
(2) Execute Offline Download	• Execute offline download. • When integrated with CENTUM, choosing offline downloading menu will pop up a dialog box to prompt for saving the operation marks. The operation marks may be saved as necessary. • Confirm that SCS has started normally on the SCS State Management window of the SCS Maintenance Support Tool.
(3) Validate SCS project	• Start the Database Validity Check Tool to check that CRC and generation time of four kinds of databases for SCS and SCS project are correct. • Repair a database if there is a discrepancy in the database.

SEE ALSO For more information about offline download operations, refer to:

"■ Procedure for offline download" on page C7-2

For more information about repairing a database, refer to:

"■ Repair database" in F3., "Database Validity Check Tool" in Engineer's Reference Manual (IM 32P04B10-01EN)

(F) Target tests

Perform the output enable operation and test the user application on the target SCS.

SEE ALSO For more information about details of target test, refer to:

C9., "Target tests" on page C9-1

(G) Offline download

Table C2.3-5 Procedure for offline download

Items	Description
(1) Execute Clean Project and Build	• Before you execute offline download, you should perform Clean Project. Then perform build to create the database for downloading.
(2) Execute Offline Download	• Execute offline download. • When integrated with CENTUM, choosing offline downloading menu will pop up a dialog box to prompt for saving the operation marks. Save the operation marks as necessary. • Confirm that SCS has started normally on the SCS State Management window of SCS Maintenance Support Tool.
(3) Validate SCS project	• Run the Database Validity Check Tool and check that the CRC codes and generation times of the databases are consistent between the SCS and SCS project. • Repair a database if there is a discrepancy in the database.

SEE ALSO For more information about clean project, refer to:

Cleaning Projects" in "Build" in "Code Generator" in "Workbench" in the Workbench User's Guide

(H) Setting passwords

Table C2.3-6 Procedure for setting passwords

Items	Description
Set passwords for Security Levels	• Set passwords for security levels 1 and 0 from the SCS Manager. • Confirm the diagnostic information message from SCS for which passwords for the security levels have been set with the SCS Maintenance Support Tool.

(I) Download operation marks

Table C2.3-7 Procedure for downloading operation marks

Items	Description
Download Operation Marks	• In the case of the CENTUM integration structure, the operation marks saved in advance are downloaded to the SCS.

(J) Enabling output

Table C2.3-8 Procedure for enabling output

Items	Description
(1) Confirm values and data status of output variables	• Confirm which output channels are disabled on the SCS State Management window of SCS Maintenance Support Tool. • Start the I/O Lock Window.(This can be performed at security level 2.) • Confirm that values and statuses of logical data and physical data for output variables are correct.
(2) Operate “Enable Output”	• Perform the Output Enable Operation for output modules on the SCS State Management window of SCS Maintenance Support Tool. • Confirm that the diagnostic information message on the Output Enable Operation for output modules is displayed. • Confirm that Output Channels are enabled on the SCS State Management window. • Confirm that the SCS operating mode is "Running" on the SCS State Management window.

SEE ALSO For more information about Output enable operation details, refer to:

“■ Enable Output operation” on page C8-2

(K) Self-document

Table C2.3-9 Procedure for self-document

Items	Description
(1) Print out whole SCS project using self-document	• In preparation for the desk check performed at application software changes in the future, print out the latest SCS project database as self-documents.

(L) Checking in project

Table C2.3-10 Procedure for checking in a project

Items	Description
(1) Confirm the diagnostic information message	• Confirm whether any diagnostic information messages you have not confirmed are displayed or not with the SCS Maintenance Support Tool.
(2) Check in SCS project	• Close the SCS Manager. • Check in the SCS project with the Version Control Tool.

SEE ALSO For more information about check-in operations, refer to:

F5.3, “Checking in project data” in Engineer's Reference Manual (IM 32P04B10-01EN)

C3. Precautions when creating applications

The tools and builders that can be used to define variables, POU, tag names are not the same due to differences in the engineering method. This section explains the precautions for handling them.

Precautions for handling variables in I/O list engineering

In the case of I/O list engineering, the variables can be defined by using Safety I/O Editor, Safety Communication I/O Editor, and SCS Manager. Variables defined by using other tools are read-only. iDefine can also be used to define variables if you are using the tool.

The differences are as follows:

- Safety I/O Editor
  This is used to define I/O variables.
- Safety Communication I/O Editor
  The following can be defined:
  - Instances of subsystem communication I/O FB
  - Instances of PROFINET communication FB
  - Instances of fire and gas communication FB

  In addition, the following variables can be assigned to the communication I/O data area:
  - FB instances defined with Safety Communication I/O Editor
  - Local FB instances defined with SCS Manager
  - FB instances of user defined FB parameters defined with SCS Manager or iDefine

  The communication I/O data area is shown in Communication I/O Builder on the Comm. I/O Wiring tab or Safety Comm. I/O Wiring tab.
- iDefine
  This is used to define internal variables and FB instances.
- SCS Manager
  This is used to define internal variables and FB instances.

Precautions for handling POU

- Handling POU when using iDefine
  You can create POU by using iDefine or the Multi-Language Editor. However, POUs that were created by using iDefine are read-only in Multi-Language Editor. POUs that were created by using the Multi-Language Editor can only be changed in the Multi-Language Editor. However, if you create a POU by using iDefine with the same name as a POU that is already registered in the Link Architecture View, you can overwrite the existing POU with confirmation when you run Reflection in RS Generation Manager.

Precautions for handling tag names

You can define tag names by using iDefine or the Tag Name Builder. Tag names that were defined by using iDefine are read-only in the Tag Name Builder. Tag names that were defined by using iDefine can only be changed in iDefine. Tag names that were defined by using the Tag Name Builder can only be changed in the Tag Name Builder.

Precautions on communication I/O definitions

When performing I/O list engineering with a version of SENG that is R4.03.10 or later, engineering for subsystem communication and safety subsystem communication is all implemented with Safety Communication I/O Editor and IOM Definition Editor of AD Organizer. Communication I/O Builder will be used as read-only. Engineering for Modbus slave communication and the DNP3 slave function is implemented with SCS Manager.

When reusing engineering data related to subsystem communication I/O created with version earlier than R4.03.10, convert the data into a safety communication I/O list by using Communication I/O List Output Tool.

SEE ALSO For more information about communication I/O List Output Tool, refer to:

"■ Communication I/O List Output Tool" on page App.3-16

Precautions for handling an SCS project that was checked in with Version Control Tool of a revision earlier than R4.03.10

When you check out an SCS project that was checked in with Version Control Tool of a revision earlier than R4.03.10 and is handled by I/O list engineering, perform the task of restoring the safety I/O list and IOM information within AD Organizer to the content labeled at the time of the previous download.

Precautions for restoring an SCS project that was generated by RS generation with AD Organizer of a revision earlier than R4.03.10

If you have used Master Database Restoring Function to restore an SCS project that was generated by RS generation with AD Organizer of a version earlier than R4.03.10 and downloaded to the SCS, you must also restore the safety I/O list and IOM information to the correct contents. By using AD Organizer, recover the safety I/O list and IOM information that are labeled at the time of downloading last time.

Precautions for managing SCS projects in AD Server

SCS projects are managed in an AD Server. The following describes the precautions for handling SCS projects:

- Creation of new SCS projects
  The selection of station type and I/O list engineering method should be determined at the time of SCS project creation, and cannot be changed afterwards.
- Deleting SCS projects
  To delete an SCS project, you must clear all items under the SCS project folder by using Windows Explorer. After that, delete the SCS project by using AD Organizer.
- Moving SCS projects
  For SCS projects registered in AD Server, you need to move the SCS projects by using the export/import function of AD Organizer. In the destination folder, do not duplicate the SCS project name and station address. Do not move the SCS project in Windows Explorer.
- Modification of SCS project names
  You need to use the SCS project export/import function of AD Organizer. You need to specify a new SCS project name at the time of importing. Do not rename the SCS project in Windows Explorer.
- Backup of SCS projects and RS projects
  You need to use the backup function of AD Organizer. You cannot run backup from Windows Explorer.

- Test Project Creating Tool
  In the case of SCS projects created with I/O list engineering, the safety I/O list, safety communication I/O list, and IOM information are registered in AD Organizer, while various setting files are included in SCS projects managed by SCS Manager.

  In case of creating a test project from the current project, you need to create a separate AD project for testing.

- License management
  You can check whether the I/O number has exceeded the number of I/O licenses by using the SCS information display function.

  If a module is added, you need to confirm the license count at the time of RS generation

C4. Procedures for generating a database

After creating the application, generate a database. This chapter describes the steps for generating a database.

Generating a database

After creating the application, build it and generate a database for SCS.

- Generating a database in I/O list engineering
  In the case of I/O list engineering, run RS generation from AD Organizer. The reflection process of RS generation reflects the engineering result of AD Organizer in SCS Manager. If you have specified the build, after the reflection process has been completed successfully, the application is built and the database is generated.

  When an SCS project for which I/O list engineering is selected has been built successfully, labels are set to the safety I/O list, safety communication I/O list, and IOM information of AD Suite. Label names are as follows:

  ```
  SCS project name-Build-Time
  ```

- Generating a database in I/O list engineering with iDefine
  Import the relevant SCS iDefine-config file that was generated from iDefine into AD Organizer and perform RS generation. To adjust the POU run sequence, run the reflection process only, change the sequence by using the Link Architecture View, and build by using SCS Manager. If you do not adjust the POU run sequence, run the build process for SCS projects by using RS Generation Manager.
- Generating a database from SCS Manager
  From the menu bar of SCS Manager, click [Project] > [Build Project], or run build project from the tool bar of SCS Manager. This method is used to build and generate a database in the case of RS original engineering. The message from database creation function appears in SCS Manager.

C5. Testing with the Safety Analyzers

The following tools are provided for the purpose of analyzing application logic.

- Integrity Analyzer
- Cross Reference Analyzer

Integrity Analyzer is used to analyze application logics and detect functions whose use is not permitted in terms of safety. If unauthorized functions are used, operations for acknowledging the use are required.

Cross Reference Analyzer is used to analyze areas affected by modifications and display the test area when the application logic is modified. It is required to perform acknowledgement operation for this test area.

IMPORTANT

Make sure to perform the acknowledgement operations for both analyzers before downloading the application logic to an SCS. If acknowledgement by both analyzers has not been completed, offline download and online change download to SCS cannot be performed.

It is recommended to perform the acknowledgement operation with Integrity Analyzer first and then with Cross Reference Analyzer.

C5.1 Integrity Analyzer

Integrity Analyzer analyzes application logics, detects "functions that are not allowed to be used" for the functions for safety and displays them in the window by highlighting for visual emphasis.

The user can check whether or not functions prohibited from use for safety applications are used. You can also print the analysis results.

If there is a program that intentionally makes use of functions prohibited from use for application, the user can acknowledge their use for each program upon examining the program based on the results of the analysis.

If functions prohibited from use for safety applications are used unintentionally, the application logic must be modified. Make changes to the application logic, perform a build operation and then analyze the application logic with Integrity Analyzer again.

IMPORTANT

- Before downloading application logic to SCS or before performing the SCS simulation test, run Integrity Analyzer and Cross Reference Analyzer, check and acknowledge the analysis results.
- It is possible to execute an application logic on a PC in logic simulation tests even if it has not been analyzed by both analyzers.
- Even when logic simulation tests are used, make sure to check that only functions whose use is permitted for safety applications and interference-free functions are used in an application logic by Integrity Analyzer at the appropriate time in order to detect errors in the application logic.

C5.1.1 Methods for checking analysis results

This section explains how to check results of analysis by Integrity Analyzer.

Starting Integrity Analyzer

1. After a build operation, select [Engineering] from the [Tools] menu of SCS Manager.
   The Engineering launcher menu appears.
2. Select [Integrity Analyzer] from the Engineering launcher menu.
   Integrity Analyzer starts up and analyzes the application logic in question.

IMPORTANT

- Start Integrity Analyzer after modifying and saving an application logic and performing a build operation. Integrity Analyzer analyzes the databases generated by the build operation.
- If Integrity Analyzer has already been started when you attempted to perform a build or download operation, a dialog box prompting to close Integrity Analyzer appears. In this case, neither the build nor the download operation is performed.

Procedure for using Integrity Analyzer

The procedure for using Integrity Analyzer is explained below.

1. Checking functions prohibited from use in terms of safety in Project Tree
   The results of analyzing the application logic with Integrity Analyzer are displayed in Project Tree. Check whether or not functions prohibited from use in terms of safety are used.
2. Checking with analysis result report
   Check the Integrity Analysis Report showing the analysis results, either directly in a window or by printing it out.
3. Acknowledgement of functions prohibited from use in terms of safety
   If there are programs that use interference-free functions intentionally, acknowledge the use of those functions for each program in the Acknowledge Non-Compliance dialog box upon examining the programs based on the analysis results.

   If interference-free functions are used unintentionally or prohibited functions are used, it is necessary to modify the application logic in question. Close Integrity Analyzer without approving the functions, modify the application logic, perform a build operation and then analyze the application logic by Integrity Analyzer again.
4. Saving and printing analysis results
   Save the analysis results and print them if necessary.

Checking functions prohibited from use in terms of safety in project tree

Project Tree allows checking whether or not functions that are prohibited from use in terms of safety exist in an application logic.

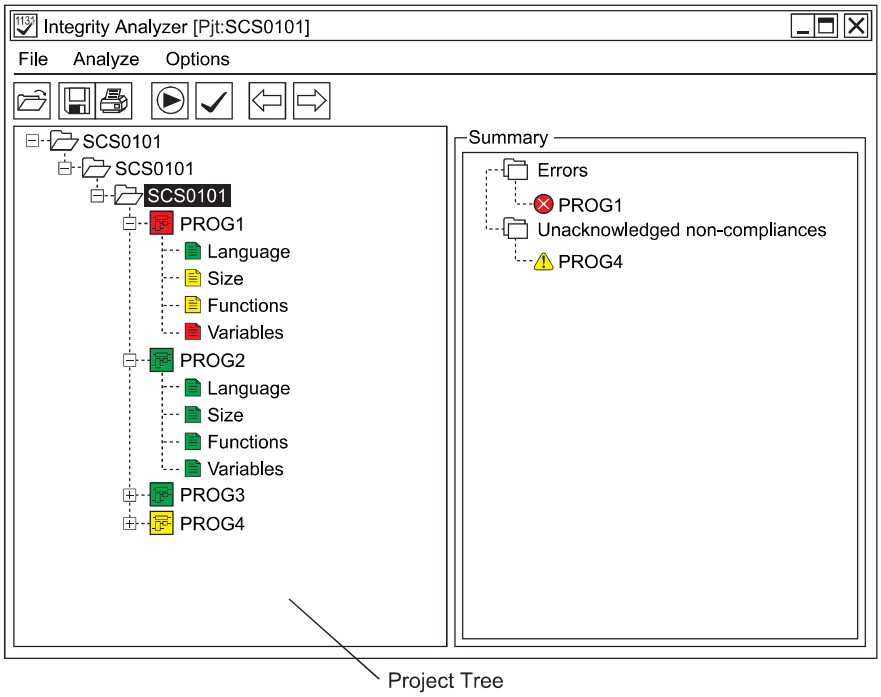


Figure C5.1.1-1 Project tree of Integrity Analyzer

The graphical analysis results can only be viewed in the window; it cannot be printed out.

How to understand icon colors

Project Tree displays SCS projects, configurations, resource and programs in a tree structure. Double-click a program icon to display icons for [Language], [Size], [Functions] and [Variables]. Analysis results are shown using colored icons placed to the left of the labels in the tree.

Table C5.1.1-1 Meaning of colors of icons on the left side of project tree

Icon color	Description
Red	Errors. Red icons indicate that prohibited functions are used. For example, using AND with 17 or more input parameters or using arrays in FBD or LD fall under this classification. It is necessary to modify programs for which red icons are displayed and remove the prohibited functions. It is not possible to download application logics to an SCS if they contain prohibited functions.
Yellow	Warnings. Yellow icons indicate that interference-free functions are used. For example, SIN and COS functions cannot be used in safety applications but can be used in other applications (control logics that do not influence safety). Check that the areas where the interference-free functions exist are outside the range of safety applications. Alternatively, check that there is no influence on safety applications. Once the use of interference-free functions is acknowledged, the applications can be downloaded to an SCS.
Green	No error. Green icons indicate that a program is created using only the functions for safety (safety applications are created). Though acknowledgement is not required, the acknowledgement status needs to be saved.

If you select an individual icon in Project Tree, detailed analysis information of items to be checked is displayed in the right pane of the window. The right pane shows analysis results of an item selected in Project Tree using one of the following icons.

Table C5.1.1-2 Meaning of icons in the right pane

Icon	Meaning
 (red)	Error. Prohibited functions are used.
 (yellow)	Warning. Interference-free functions are used.
 (green)	No error. A program is created using only the functions for safety.

SEE ALSO For more information about details on how to read the analysis results of the program in Project Tree, refer to:

C5.1.3, “Confirmation of analysis results by project tree” on page C5-12

Checking with Analysis report

The Integrity Analysis Report organizes and summarizes all the information in analysis results. It can be displayed in a window, printed or saved in a file (using RTF or TEXT format) as a report.

The Integrity Analysis Report is used mainly for the following two applications.

- It provides more detailed information than the information obtained by expanding Project Tree.
- The Integrity Analysis Report can be used as a part of operation records or application construction documentation, by printing it out or saving it to a file. The Integrity Analysis Report also includes information about whether or not acknowledgement is made in the Acknowledge Non-Compliance dialog box, along with comments. In order to record acknowledged items, print or save the report in a file after acknowledgement.

Application Logic Integrity Analysis Report

Project : SCS0101
Configuration : SCS0101
Resource : SCS0101 (101)
Project Build Date : 12/05/2007 10:45:30 AM
Project Analysis Date : 12/05/2007 10:54:53 AM
Report Date : 12/05/2007 10:55:24 AM
User : MATSUI

PROG1
Language Usage
Pass PROG1 FBD (Function Block Diagram)

Program Size
Pass PROG1 524 Limits 0..4000

Function Usage
Pass

Variable Usage
Pass

PROG2
Language Usage
Pass PROG2 LD (Ladder Diagram)

Program Size
Pass PROG2 1044 Limits 0..4000

Function Usage
Pass

Variable Usage
Pass

⋮

Acknowledgement Status

Program	Status	
PROG1	Pass	
PROG2	Pass	
PROG3	Pass	
PROG4	Pass	
PROG5	Warning	Acknowledged by MATSUI 12/05/2007 10:54:59 AM

Number of programs with integrity errors: 0
Number of programs requiring acknowledgement: 0

Figure C5.1.1-2 Example of Integrity Analysis report

Saving and displaying Analysis report

1. Select a resource in Project Tree and select [Save Analysis] from the [File] menu. Alternatively, click the [Save current analysis history] button in the toolbar.
   the analysis results are saved.
2. Select [Report] from the [Analyze] menu.
   The saved analysis results are displayed as an analysis report.

IMPORTANT

Make sure to save the analysis results before creating an analysis report.

If the current analysis results and acknowledgement history are not saved before creating an analysis report, a message prompting you to save the history is notified. If you click [Yes] button in the message box, the current analysis results and acknowledgement history are saved, overwriting the history saved before in the process, and an analysis report is created. An analysis report is not created if you click [No] button.

Acknowledgement of interference-free functions

If the analyzed application logic includes programs using interference-free functions, it is necessary to acknowledge such programs one by one in the Acknowledge Non-Compliance dialog box.

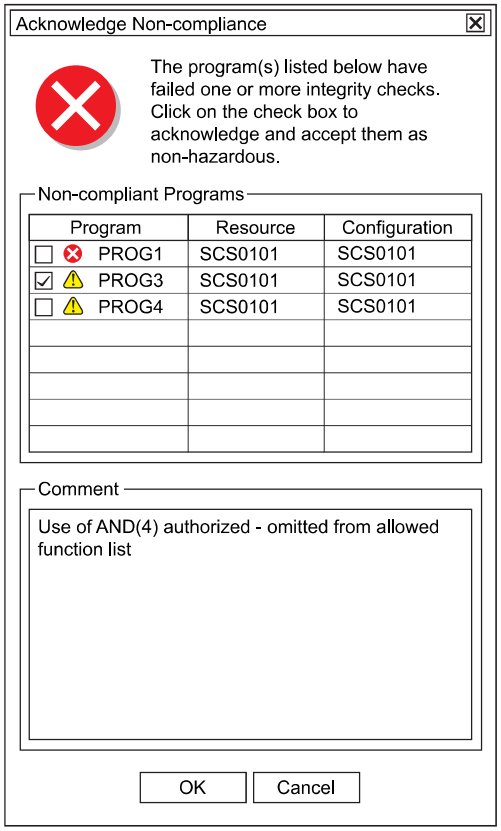


Figure C5.1.1-3 Acknowledge Non-compliance dialog box

Displaying the Acknowledge Non-compliance dialog box

Select [Authorize] in the [Analyze] menu. Alternatively, click "Display program non-compliance dialog" button in the toolbar. The Acknowledge Non-Compliance dialog box appears.

Acknowledgement of programs and displayed icons

This dialog box shows analysis results of each program with one of the following icons.

Table C5.1.1-3 Meaning of icons

Icon (color)	Description
 (red)	A program uses prohibited functions. This icon has the same meaning as the red program icon displayed in Project Tree. Modify the program and remove the prohibited functions. This program cannot be acknowledged.
 (yellow)	A program uses interference-free functions. This icon has the same meaning as the yellow program icon displayed in Project Tree. In order to download the programs to an SCS, it is necessary to check each check box of all the programs marked with this icon and acknowledge them.

Before approving, confirm that only the functions for safety are used in the safety application using Project Tree or by checking the Integrity Analysis Report.

The reasons why interference-free functions are used, results of analysis for the purpose of acknowledgement, etc., can be entered as comments. The Integrity Analysis Report includes information about whether or not acknowledgement was made along with any comments entered.

C5.1.2 Integrity Analyzer window structure

This section explains the window structure of Integrity Analyzer.

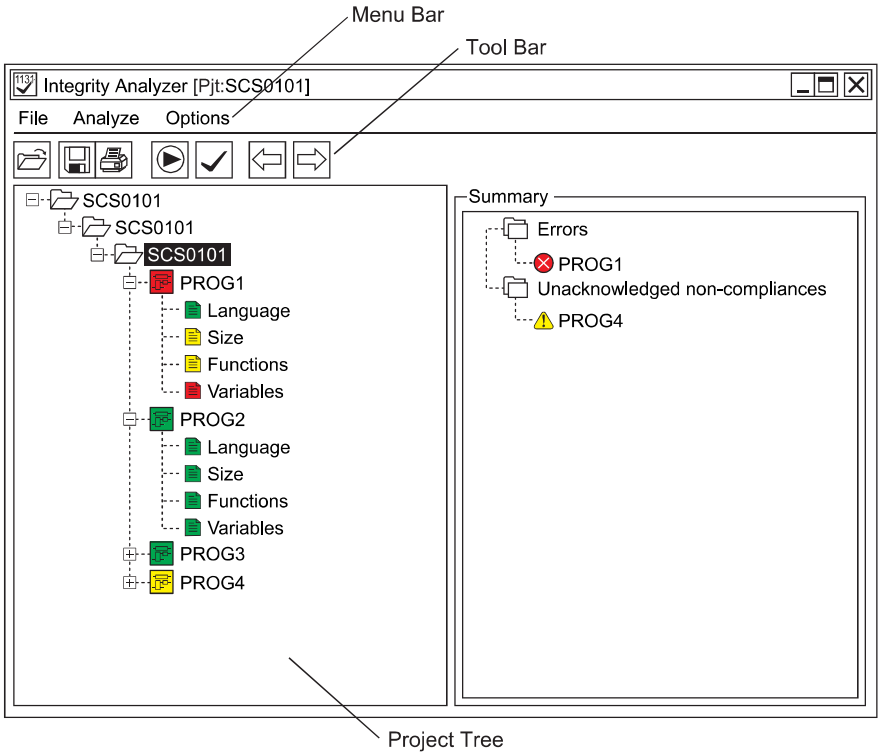


Figure C5.1.2-1 Integrity Analyzer window structure

Menu bar

The menu bar provides the following menus.

- [File] menu
- [Analyze] menu
- [Options] menu

The menu items of each menu are explained below.

Table C5.1.2-1 File menu

Menu item	Description
Print Report	Prints an analysis report saved by [Save Analysis]
Save Report	Creates an analysis report and saves it in a file (RTF or TEXT format)
Save Analysis	Saves analysis results and acknowledgement status.
Exit	Closes Integrity Analyzer

Table C5.1.2-2 Analyze menu

Menu item		Description
Start	With history	Performs analysis and compares with the results of previous warning acknowledgement and analysis. If the areas acknowledged in the previous analysis are not modified this time, it is regarded as if they have already been acknowledged.
	Without history	Performs analysis without comparing it with results of previous acknowledgement and analysis

Continues on the next page

Table C5.1.2-2 Analyze menu (Table continued)

Menu item	Description
Report	Creates and displays the analysis report in the Integrity Analysis Report window
Authorize	Displays the Acknowledge Non-Compliance dialog box.

Table C5.1.2-3 Options menu

Menu item	Description
Settings	Displays the Settings dialog box

IMPORTANT

Make sure to save the analysis results before creating an analysis report.

If the current analysis results and acknowledgement history are not saved before creating an analysis report, a message prompting you to save the history is notified. If you click [Yes] button in the message box, the current analysis results and acknowledgement history are saved, overwriting the history saved before in the process, and an analysis report is created. An analysis report is not created if you click [No] button.

Toolbar

The toolbar provides the following buttons.

Table C5.1.2-4 Toolbar buttons

Button	Name	Description
	Save current analysis history	Saves analysis results and acknowledgement status.
	Print report for a selected resource	Prints analysis reports.
	Display program non-compliance dialog	Displays the Acknowledge Non-Compliance dialog box.
	Previous non-compliance	Selects the icon of the previous interference-free element or element not allowed in terms of safety relative to the currently selected icon in Project Tree (the upward direction in the tree).
	Next non-compliance	Selects the icon of the next interference-free element or element not allowed in terms of safety in Project Tree relative to the currently selected icon (the downward direction in the tree).

Project tree

Project Tree is displayed on the left pane of the Integrity Analyzer window.

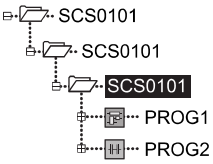


Figure C5.1.2-2 Project tree

Each level of Project Tree can be expanded or collapsed by double-clicking an icon or text label, or clicking the +/- button on the left edge.

Analysis results of an item selected in Project Tree are displayed in the right pane of the window.

The display arrangement of Project Tree can be defined in Settings dialog box.

Displaying the Settings dialog box

On the [Options] menu, click [Settings]. The Settings dialog box appears.

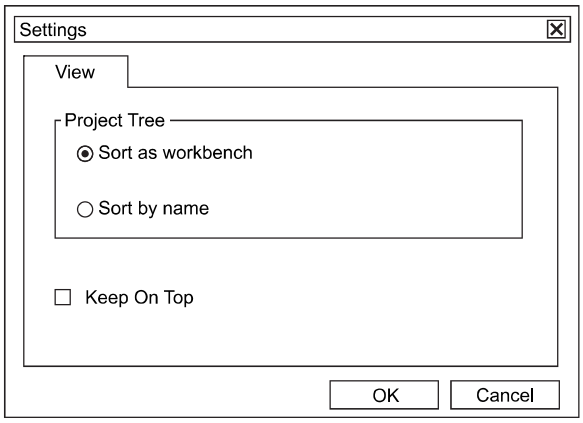


Figure C5.1.2-3 Settings dialog box

- Project Tree
  Sort as workbench: Contents displayed on Project Tree are sorted along with Workbench.

  Sort by name: Contents displayed on Project Tree are sorted by names alphabetically.
- Keep On Top
  Integrity Analyzer window is kept always on top.

C5.1.3 Confirmation of analysis results by project tree

This section explains how to understand the detailed information displayed when the following layers below the resource (the SCS project) are selected in Project Tree.

- Resource (list of program errors and unacknowledged warnings in a resource)
- Program (program classification and analysis results)
- Language (language usage information of a program)
- Size (size information of a program)
- Functions (results of analyzing program source code and object code)
- Variables (results of analyzing variables in a program)

Displaying analysis results of Functions and Function Blocks

Project Tree displays analysis results of FUs and FBs as part of the summary for the program that calls the FUs and FBs.

That is, if you expand an icon of a program name, not only the analysis results of the program itself, but also the analysis results for the FUs and FBs called by the program are displayed.

Checking resources

A list of analysis statuses of resources (SCS projects) is displayed in the right pane of the window. The list displays detected errors and unacknowledged warnings.

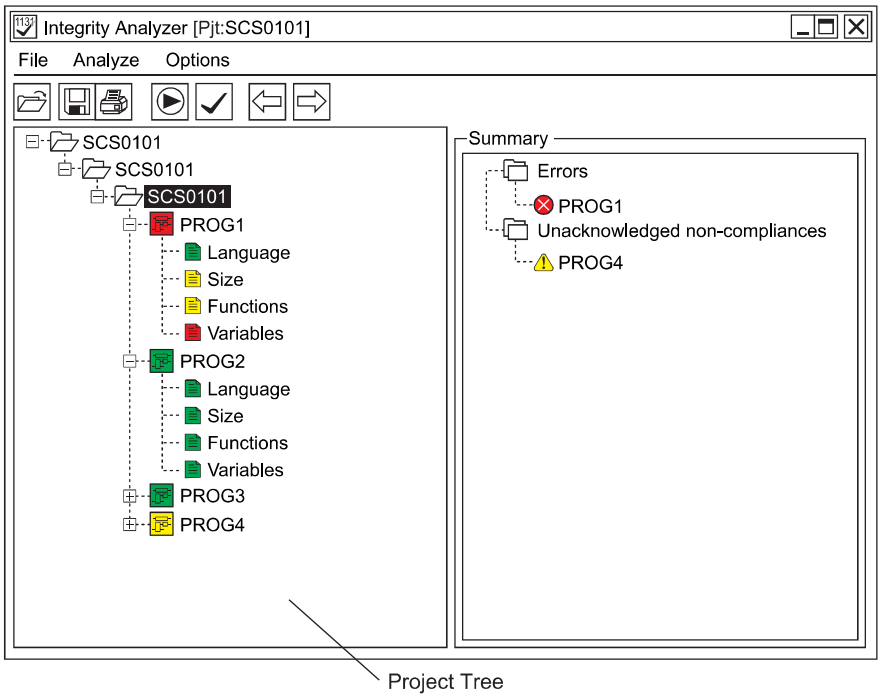


Figure C5.1.3-1 Analysis results of resource

The analysis results of the selected resource are classified into errors and unacknowledged warnings, and displayed in a tree structure in the right pane. Errors and unacknowledged warnings can be expanded or collapsed.

These graphical analysis results can only be viewed in the window; they cannot be printed out.

Checking programs

When you select a program name in Project Tree, a list of analysis results of the program is displayed in the right pane of the window. The classification of the program and the result of analysis (Pass, Fail, Warning) are displayed.

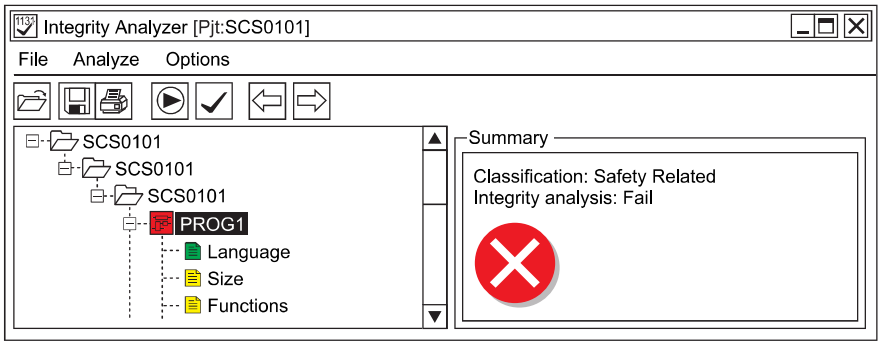


Figure C5.1.3-2 Analysis results of a program for which error occurred

These graphical analysis results can only be viewed in the window; they cannot be printed out.

Checking program languages

If you select [Language] in Project Tree, the language used for the program is displayed in the right pane of the window. If the program includes user-defined FUs or user-defined FBs, the languages used for them are shown as well.

Table C5.1.3-1 Icons displayed on the left side of program names and meaning

Icon (color)	Meaning
✓ (green)	POUs are created using permitted languages
✗ (red)	POUs are created using languages that are not allowed (*1)

*1: When using ST to write a program other than FU and FB, an error will occur.

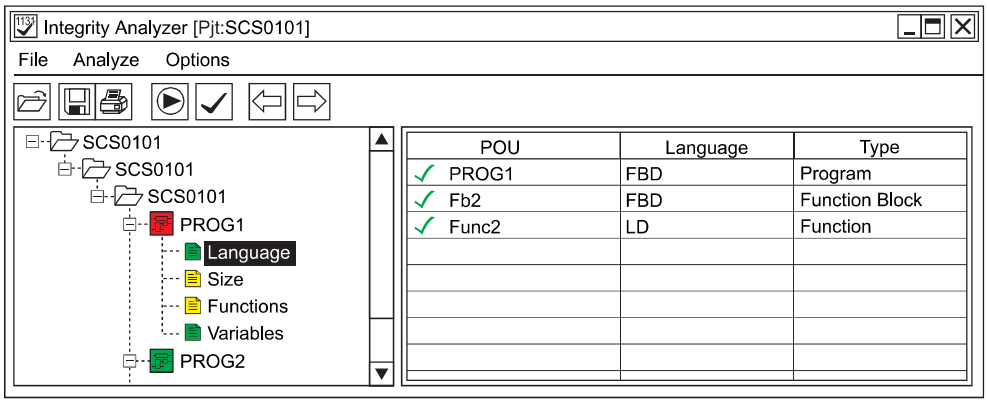


Figure C5.1.3-3 Results of checking languages used in programs

The screenshot example above shows the result of analyzing languages used in PROG1. PROG1 uses a function block called Fb2 and a function called Func2. PROG1, Fb2 and Func2 are written with permitted languages.

These graphical analysis results can only be viewed in the window; they cannot be printed out.

Checking program size

IMPORTANT

If the program size exceeds the specified limit, a warning is displayed. However, even if the warning is displayed, you can still use the program for a safety function after sufficiently confirming the validity of the program through some testing.

If you select [Size] in Project Tree, the size of the program and the specified upper limit size are displayed in the right pane of the window. If the program includes user-defined FUs or user-defined FBs, their program sizes are shown as well.

For the FB created with ST, the number of lines excluding the comment lines and blank lines as well as the maximum number of lines is displayed.

Table C5.1.3-2 Icon displayed on the left side of program names and meaning

Icon (color)	Meaning
⚠ (yellow)	The program size exceeded the warning range

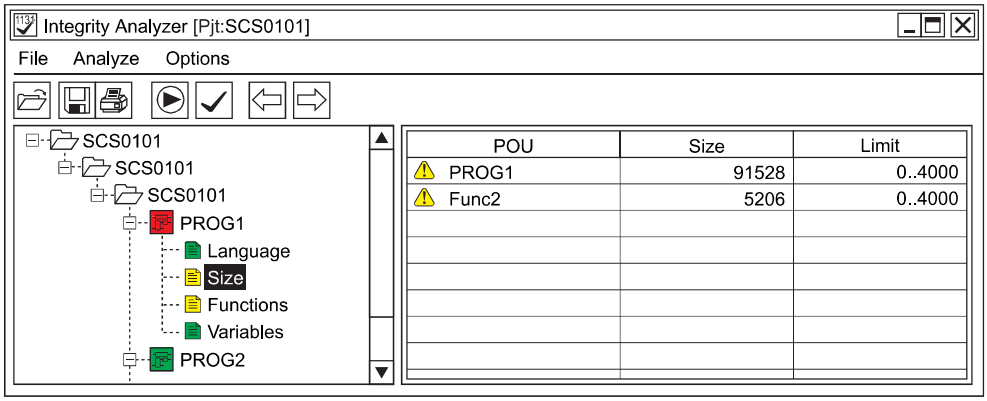


Figure C5.1.3-4 Program size information

These graphical analysis results can only be viewed in the window; they cannot be printed out.

Checking program source code and object code

If you select [Functions] in Project Tree, the results of analyzing the source code and object code of the program are displayed as a list of unauthorized FUs or FBs used in the right pane of the window.

An icon displayed to the left of a function name or function block name indicates that the FU or FB is not allowed in terms of safety.

Table C5.1.3-3 Icons displayed on the left side of Function names/Function Block names and meaning

Icon (color)	Meaning
⊗ (red)	The FU or FB in question is not classified as safe or interference-fee and its use caused an error
⚠ (yellow)	The FU or FB in question is classified as interference-free and its use in a safety program requires acknowledgement

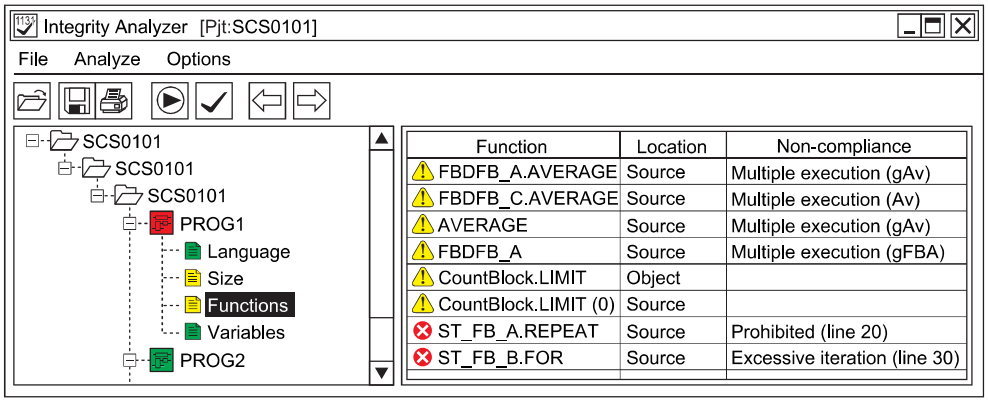


Figure C5.1.3-5 Information of Function usage in the program

Integrity Analyzer searches in one or multiple POUs for the functions calling the same FB instance and displays the functions as the analysis result. If the same FB instance in a POU is called by multiple functions from different locations, the related functions and POUs will be displayed with respective warning messages. The above figure illustrates the result of the analysis.

In the message displayed in the "Function" column of the preceding figure, FBDFB_A is the name of the POU and AVERAGE is the type of the FB. The instance name or parameter name is displayed in parentheses in the "Non-compliance" column.

In LD source code analysis, the existence and usage of EN inputs inside the program are also detected. An EN input refers to the first BOOL-type input that is automatically appended when the type of the first input for FUs or FBs is BOOL in LD.

If libraries are used, the source files of the libraries are also analyzed.

A number in ( ) following a function name or function block name indicates the number of inputs. However, EN inputs are not included in this number.

In case of a library, a function name is displayed as "library name.program name.function name" and a function block name is displayed as "library name.program name.function block name."

Note that the graphical view of the analysis results in the above figure is only available on the screen. The printout is text only.

If unrecognizable statements or scripts with incorrect syntax are found in ST, the following messages are displayed in the "Non-compliance" column.

Table C5.1.3-4 Non-compliance messages when error or warning occurs

Icon (color)	Message in Function(*1)	Message in Non-Compliance	Description
(red)	ST_FB.WHILE	Prohibited (line xx) (*2)	WHILE must not be used.
(red)	ST_FB.REPEAT	Prohibited (line xx) (*2)	REPEAT must not be used.
(red)	ST_FB.FOR	Loop nesting (line xx) (*2)	Nested loop in FOR loop must not be used.
(red)	ST_FB.FOR	Variable iteration count (line xx) (*2)	Initial value, end condition or step number in FOR loop must use a constant.
(red)	ST_FB.FOR	Iteration counter overflow (line xx) (*2)	FOR loop index counter range overflow.
(red)	ST_FB.EXIT	Outside loop (line xx) (*2)	EXIT must not be used outside FOR loop.

Continues on the next page

Table C5.1.3-4 Non-compliance messages when error or warning occurs (Table continued)

Icon (color)	Message in Function(*1)	Message in Non-Compliance	Description
(yellow)	ST_FB.RET	Interference Free (line xx) (*2)	Interference-free. Due to RETURN being used.
(yellow)	ST_FB.FOR	Excessive iterations (line xx) (*2)	Due to the number of iterations in FOR loop exceeding 500.
(yellow)	ST_FB.FBD_FB	Function Block Call (*3)	Due to ST calling FB.
(yellow)	ST_FB.FBD_FB	FB Parameter Access (*4)	Due to ST accessing FB parameter.
(yellow)	ST_FB.= FBD_FB.<>	Exact comparison (line xx) (*5)	Exact comparison should not be used to compare real numbers.

*1: The messages of ST_FB here are the examples of functions and function blocks. FBD_FB is a function block name example, not an instance name.
*2: xx in (line xx) will be replaced by the line number that are applicable to the message.
*3: The message will be displayed once even though the same FB is called many times by ST.
*4: The message will be displayed once even though same parameters in the same FB or different parameters in the same FB are accessed many times by ST.
*5: xx in (line xx) will be replaced by all the line numbers that are related to the ST message.

Even comparing the two real numbers using an equal operator or not equal operator in FBD or LD is classified as interference-free, and the message "Exact Comparison" will be displayed once per POU in the "Non-compliance" column.

SEE ALSO For more information about precautions on the structure when describing FU and FB with the ST language, refer to:

2., “Structured text” in POU Reference Manual (IM 32P03B20-01EN)

Checking analysis results of variables in programs

If you select [Variables] in the project tree, variables that do not satisfy the requirements of the program, such as naming rules and data type, are displayed in the right pane of the window.

The right pane displays names of variables that may cause errors or warnings and the programs, FUs or FBs to which those variables belong. Moreover, detailed information about errors and warnings is also displayed.

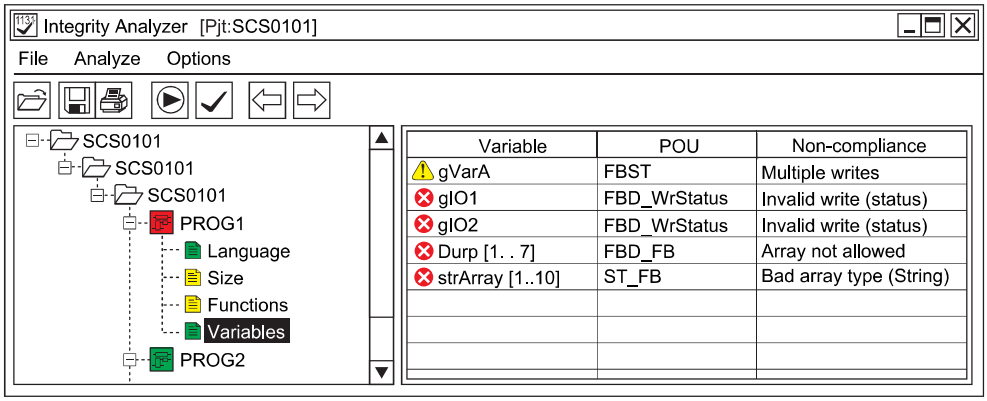


Figure C5.1.3-6 Example of variable analysis results

The Integrity Analyzer checks POUs to detect illegal writings: multiple writing to a variable, within a POU or by different POUs, and writing to output variable statuses. The preceding figure illustrates the result of the analysis. In the [POU] column, names of the POUs performing the illegal writing are displayed. If a POU contains multiple writing to the same variable, a warning message will be displayed for that POU. If multiple POUs are writing to the same variable, a warning message will be displayed for each of the POUs.

TIP

- Integrity Analyzer does not detect multiple writing to the same variable in ST objects. Such usage should be checked through a code review or unit test. However, multiple writing to the same variable by a certain ST object and other POU will be detected.
- Integrity Analyzer does not detect multiple writing to arrays or array elements.

Error messages will be displayed for the POUs that are writing to the status of output variables.

- Integrity Analyzer detects writing to the .status member of the IO_BOOL or IO_REAL variables having output attribute.

  For example, an error message is displayed in the following case: The value of internal variable bool1 (type BOOL) is written to the .status member of output variable DO010101 (type IO_BOOL).

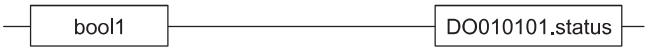


Figure C5.1.3-7 Example where error message is displayed for POU (1)

- Integrity Analyzer detects writing to the entire IO_BOOL or IO_REAL variables having output attribute. Integrity Analyzer also detects the cases where the output (type IO_BOOL or IO_REAL) of an function block, such as B_TO_IB, is connected to an output variable.

  For example, an error message is displayed in the following cases:

  The value of internal variable IO_BOOL1 (type IO_BOOL) is written to the .status member of output variable DO010102 (type IO_BOOL).



Figure C5.1.3-8 Example where error message is displayed for POU (2)

The value of Q (type IO_BOOL), which is the output of function block B_TO_IB, is written to the .status member of output variable DO010103 (type IO_BOOL).

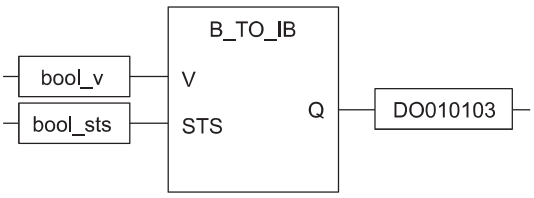


Figure C5.1.3-9 Example where error message is displayed for POU (3)

Table C5.1.3-5 Error messages displayed in Non-compliance column

Icon (color)	Indication in [Variable]	Message in Non-Compliance	Description
(yellow)	gVarA (*1)	Multiple writes	Multiple writing to this variable was detected.
(red)	gI01 (*2)	Invalid write(status) (*3)	Writing to the status of this output variable was detected.

*1: Variable name or FB instance name plus parameter name is displayed.
*2: Variable name is displayed.
*3: In parentheses ( ), the member name (i.e. status) or type name of the variable is displayed.

Note that the graphical view of the analysis results in the above figure is only available on the screen. The printout is text only.

If prohibited variables are used in ST, the following messages will be displayed as Non-Compliances.

Table C5.1.3-6 Error messages displayed in Non-compliance column

Icon (color)	Message in Variable	Message in Non-Compliance	Description
(red)	bArrayB[1..10000]	Array size	Number of array elements exceeds 500.
(red)	MultiArray[1..10][1..10]	Array dimensions	Multiple dimension arrays cannot be used.
(red)	bArrayC[10..20]	Array bounds	The array initial index must be 1.
(red)	strArray[1..10]	Bad array type({TYPE})	Array cannot contain prohibited data type (Detail is displayed in {TYPE}).
(red)	DO1	Bad type({TYPE})	Prohibited global variable cannot be used (Detail is displayed in {TYPE}).
(red)	COM_BOOL1	Bad local type({TYPE})	Prohibited local variable cannot be used (Detail is displayed in {TYPE}).
(red)	COM_BOOL2	Bad parameter type({TYPE})	Prohibited input/output parameter cannot be used (Detail is displayed in {TYPE}).
(red)	(*1)	Array check error	The analyzer detected a defect of a mechanism which checks the access outside the range of array.

*1: Message cannot be displayed.

If prohibited variables are used in FBD or LD, the following messages will be displayed as Non-Compliances.

Table C5.1.3-7 Error messages displayed in Non-compliance column

Icon (color)	Message in Variable	Message in Non-Compliance	Description
(red)	bArrayA[1..10]	Array not allowed	Array must not be used in FBD or LD.

These graphical analysis results can only be viewed in the window; it cannot be printed out.

C5.2 Cross Reference Analyzer

Cross Reference Analyzer displays the differences between the previously downloaded application (the application currently running in an SCS) and the application to be downloaded, and the extent to which the download will affect the operation in a window by highlighting them visually, in order to limit the range of retesting caused by changes in an application logic.

You can check programs that require retesting. You can also print the analysis results.

Cross Reference Analyzer detects programs that depend on the modified program. You should retest the detected programs. A list of programs requiring retesting is displayed; they can be acknowledged upon checking the analysis results of each program.

If unintended program changes and dependencies are detected, the application logic must be modified. Modify the application logic, perform a build operation and then analyze the application logic with Cross Reference Analyzer again.

If no program is found for retesting, retesting will not be performed. However, since the modifications on a certain items may not be discovered for retesting, these modified items need to be tested accordingly.

IMPORTANT

- Before downloading application logic to SCS, run Integrity Analyzer and Cross Reference Analyzer and acknowledge.
- Cross Reference Analyzer detects the differences between the application currently running in an SCS and the application to be downloaded.

  It does not detect differences with an application running in a virtual test.

  In a virtual test, it is possible to execute and test an application logic on a PC without having to perform analysis by both analyzers.

Cross Reference Analyzer also has the function to compare an SCS database with the master database of other SCS project with the same domain number and station number. Using this function, you can verify that a project created from an existing project is exactly the same in functionality as the original project. This eliminates the need to test all the POUs when you regenerate a project.

SEE ALSO For more information about the items that require retesting but not detected by Cross reference Analyzer, refer to:

C5.2.5, “Precautions on Cross Reference Analyzer” on page C5-46

C5.2.1 Methods for checking analysis results

This section explains how to check results of analysis by Cross Reference Analyzer.

Starting Cross Reference Analyzer

1. After a build operation, select [Engineering] from the [Tools] menu of SCS Manager.
   The Engineering launcher menu appears.
2. Select [Cross Reference Analyzer] from the Engineering launcher menu.
   Cross Reference Analyzer starts up, automatically analyzes the application logic in question and displays the analysis results.

TIP

Cross Reference Analyzer displays or prints the differences between the previously downloaded application logic and the application logic to be downloaded, and the extent of the differences. If an application logic has never been downloaded, there is no equivalent to a previously downloaded application logic. In this case, Cross Reference Analyzer displays all programs as new.

IMPORTANT

If Cross Reference Analyzer has already started when you attempted to perform a build or download operation, a dialog box prompting to close Cross Reference Analyzer appears. In this case, neither the build nor the download operation is performed.

Procedure for using Cross Reference Analyzer

The procedure for using Cross Reference Analyzer is explained below.

1. Checking programs in Dependency Tree
   Check the results of analysis by Cross Reference Analyzer in Dependency Tree to identify the programs requiring retesting. The programs requiring retesting are those with changes and those that depend on the changed programs.
2. Checking with analysis result report
   Check the Cross Reference Analysis Report showing the analysis results, either directly in a window or by printing it out.
3. Acknowledgement of differences between application logics and extent of influence
   A list of programs requiring retesting is displayed in the Acknowledge Dependencies dialog box; acknowledge them upon checking the analysis results of each program.

   If unintended changes and independencies are detected or the application requires modification, close Cross Reference Analyzer without approving the programs. Modify the application logic, perform a build operation and then analyze the application logic by Cross Reference Analyzer again.
4. Saving and printing analysis results
   Save the analysis results and print them if necessary.

Checking programs in Dependency tree

Dependency Tree allows checking the results of comparing the application logic running on an SCS and the application logic to be downloaded, as well as programs that depend on the changes. These programs are the ones that require retesting and review.

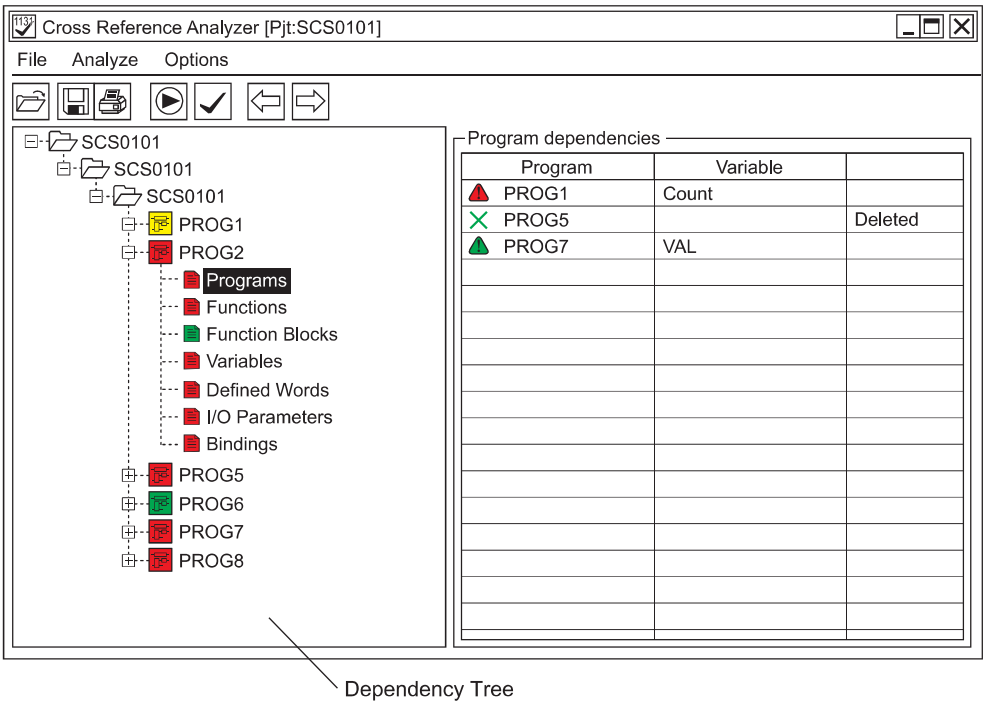


Figure C5.2.1-1 Example of program analysis result by Cross Reference Analyzer

These graphical analysis results can only be viewed in the window; they cannot be printed out.

How to understand icon colors

Dependency Tree displays SCS projects, configurations, resource and programs in a tree structure. Double-click a program icon to display icons for [Programs], [Functions], [Function Blocks], [Variables], [Defined Words], [I/O Parameters] and [Bindings]. Analysis results are shown using colored icons placed to the left of the labels in the tree.

Table C5.2.1-1 Meaning of colors of icons on the left side of Dependency tree

Icon color	Description
Red	Red icons indicate that programs or function blocks and functions used in the program have been changed.
Yellow	Yellow icons indicate dependencies on changed programs. Although the programs themselves have not been changed, it is necessary to retest or examine the code in order to check that it is not affected by changes made to the dependent programs. A yellow icon may also indicate that the program name was changed. Retesting is not required in this case.
Green	Green icons indicate that the changes do not affect other programs. Neither retesting nor review is required.

If you select an individual icon in Dependency Tree, detailed analysis information of the item to be checked is displayed on the right pane of the window. The right pane shows the status of changes of the item selected in Dependency Tree and the extent of influence of the changes.

If you select an individual icon below the program layer, the following colored icons are displayed next to the corresponding program components in the right pane of the window.

Table C5.2.1-2 Meaning of icons in the right pane of the window when an icon below the program icon is selected

Icon (color)	Meaning
 (green)	An item in the right pane is dependent on the program selected in Dependency Tree but not affected directly by the changes.
 (red)	An item in the right pane is dependent on the program selected in Dependency Tree and affected by the changes. In other words, the item was directly changed or newly created, or is dependent on the changed areas.
 (green)	An item in the right pane used to depend on the program selected in Dependency Tree but the dependency was eliminated by the change.

SEE ALSO For more information about details on how to read the analysis results of the program in Dependency Tree, refer to:

C5.2.3, “Confirmation of analysis results by Dependency tree” on page C5-30

Checking with Analysis report

The Cross Reference Analysis Report organizes and summarizes all the information in analysis results. It can be displayed in a window, printed or saved in a file (RTF or TEXT format) as a report.

The Cross Reference Analysis Report is used mainly for the following two applications.

- It provides more detailed information than the information obtained by expanding Dependency Tree.
- The Cross Reference Analysis Report can be used as a part of operation records or application construction documentation, by printing it out or saving it to a file. The Cross Reference Analysis Report also includes information about whether or not acknowledgement is made in the Acknowledge Dependencies dialog box, along with comments. In order to record acknowledged items, print or save the report in a file after acknowledgement.

Application Logic Cross Reference Analysis Report

Project : SCS0101
Configuration : SCS0101
Resource : SCS0101 (101)
Project Build Date : 12/05/2007 10:45:30 AM
Project Analysis Date : 12/05/2007 1:18:27 PM
Report Date : 12/05/2007 1:19:02 PM
User : MATSUI

Programs in previous version : 8
Programs in current version : 8
Variables in previous version : 66
Variables in current version : 66
Shared variables in previous version : 57
Shared variables in current version : 57

Modified Programs

Name	Change
PROG2	Modified
PROG3	Deleted
PROG5	I/O Changed
PROG7	Modified I/O Changed
PROG8	Function block modified, Variable changed, Defined Word changed
WASPROG4	Renamed

Modified Functions

Name	Change
Func4	Modified

Modified Function Blocks

Name	Change
Fb1	Modified

Modified Variables

Name	Change
IN1	Type Changed, Initial Changed
IN2	Scope Changed
OUT1	Type Changed

Modified Defined Words

defConst	Equivalent Changed

I/O Parameter Changes

Variable	Comment
AI001	1-3 SAV144[01] Channel
DI001	1-5 SDV144[01] Channel
DI002	1-5 SDV144[02] Channel
DI003	1-5 SDV144[03] Channel
DI007	1-5 SDV144[07] Channel

Dependency Cross Reference

Current Version Bound Variable Usage

Program	Bound variables
PROG1	C01001 C01002 C01003
PROG2	C01001 C01003 CONSU2 P02002
PROG5	C01001 P03001 P03002 P030003
PROG6	
PROG7	LP0001@PROG7
PROG8	
WASPROG4	

Current Version Bound Variable Cross Reference

Bound Variable	Used	
C01001	PROG1 PROG2 PROG5	
C01002	PROG1	
C01003	PROG1(2) PROG2	Unmatched name (P02005)
C0NSU2	PROG2	Unmatched name (P02006)
LP0001@PROG7	PROG7(3)	
P02002	PROG2	
P03001	PROG5	
P03002	PROG5	
P03003	PROG5	

Acknowledgement Status

Program	Status	
PROG1	Not Modified	Not acknowledged
PROG2	Modified	Not acknowledged
PROG5	IO Changed	Not acknowledged
PROG7	Modified IO Changed	Acknowledged by SUZUKI 12/05/2007 09:10:23
PROG8	Function block modified, Variable changed, Defined Word changed	

Not acknowledged

Number of programs requiring acknowledgement : 4

Figure C5.2.1-2 Example of Cross Reference report (RTF format file)

Displaying Analysis report

1. Select a resource in Dependency Tree and select [Save Analysis] in the [File] menu. Alternatively, click [Save current analysis history] button in the toolbar;
   the analysis results are saved.
2. Select [Report] from the [Analyze] menu.
   The saved analysis results are displayed as an analysis report.

IMPORTANT

Make sure to save the analysis results before creating an analysis report.

If the current analysis results and acknowledgement history are not saved before creating an analysis report, a message prompting you to save the history is notified. If you click [Yes] button in the message box, the current analysis results and acknowledgement history are saved, overwriting the history saved before in the process, and an analysis report is created. An analysis report is not created if you click [No] button.

Displaying previous Analysis report

By running [Previous Report] in the [Analyze] menu, you can display the report of the analysis result for the previously downloaded application. The report file is saved in .rtf format. The report date of the previous analysis report is the date that the analysis report was last saved before downloading.

Acknowledgement of program dependencies

If the analyzed application logic contains programs requiring retesting because they were changed or depend on the changed programs, it is necessary to acknowledge these programs one by one in the Acknowledge Dependencies dialog box.

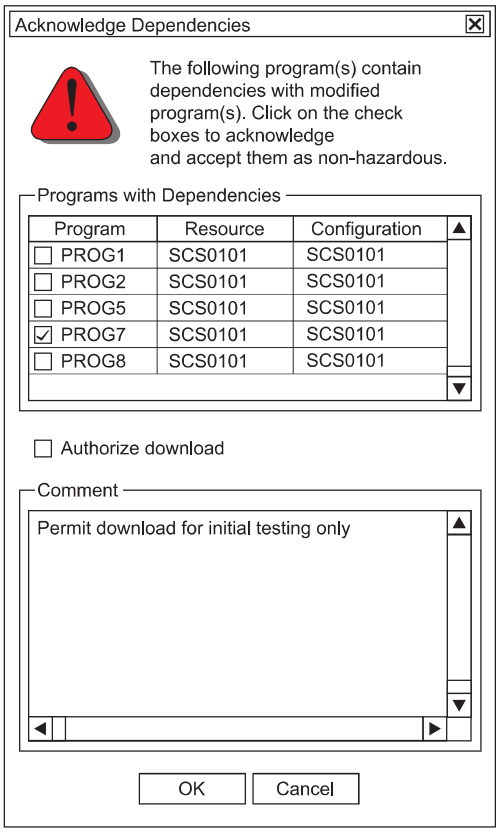


Figure C5.2.1-3 Acknowledge Dependencies dialog box

Displaying the Acknowledge Dependencies dialog box

Select [Authorize] in the [Analyze] menu. Alternatively, click "Display program dependency acknowledge dialog" button in the toolbar. The Acknowledge Dependencies dialog box appears.

Acknowledgement of programs with changes and dependencies

The Acknowledge Dependencies dialog box displays programs indicated with red or yellow icons in Dependency Tree. In order to download the application logic to an SCS, it is necessary to acknowledge all the programs displayed in the dialog box.

The user must confirm the following items and then check the check box for each program.

- Retesting and review must be planned and executed for programs indicated by red and yellow icons.
- No unintended modifications are included.
- No unintended dependencies (e.g., unintended sharing of global variables) are included.

Authorize download check box

Selecting this check box allows downloading the application logic to an SCS without acknowledging individual program dependencies.

IMPORTANT

- Use this check box only at the beginning of application development such as during debugging an application logic.
- While the SCS is in use for actual plant, acknowledge the dependencies of individual programs without selecting this check box.
- It is recommended to enter the reasons in the comment field when the Authorize Download check box is selected.

Comment

Memos related to changed areas, results of analysis for the purpose of acknowledgement, etc. can be entered as comments. The Cross Reference Analysis Report includes information about whether or not programs are acknowledged, along with comments.

C5.2.2 Cross Reference Analyzer window structure

This section explains the window structure of Cross Reference Analyzer.

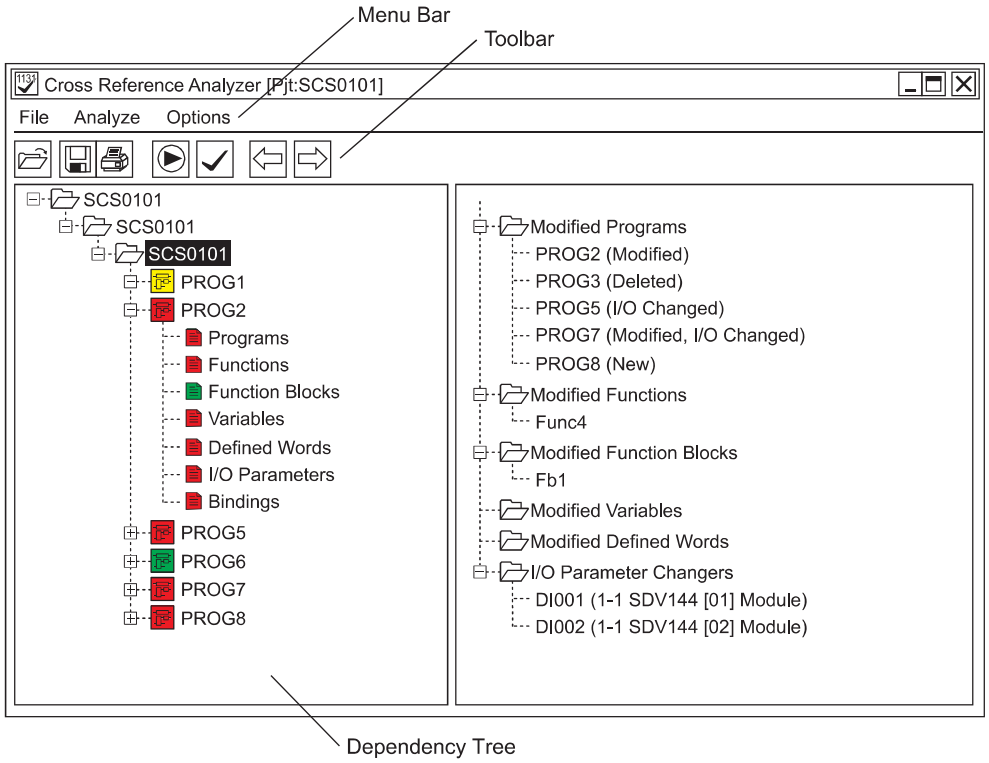


Figure C5.2.2-1 Cross Reference Analyzer window structure

Menu bar

The menu bar provides the following menus.

- [File] menu
- [Analyze] menu
- [Options] menu

The menu items of each menu are explained below.

Table C5.2.2-1 File menu

Menu item	Description
Print Report	Prints an analysis report saved by [Save Analysis]
Save Report	Creates an analysis report and saves it in a file (RTF or TEXT format)
Save Analysis	Saves analysis results and acknowledgement status.
Exit	Closes Cross Reference Analyzer

Table C5.2.2-2 Analyze menu

Menu item		Description
Start	With History	Performs analysis and compares it with the results of previous acknowledgement and analysis. If the areas acknowledged in the previous analysis are not modified this time, it is regarded as if they have already been acknowledged.
	Without History	Performs analysis without comparing it with results of previous acknowledgement and analysis
Report		Creates and displays the analysis report in the Cross Reference Analysis Report window
Previous Report		Displays previous analysis report.
Authorize		Displays the Acknowledge Dependencies dialog box.
Compare with Original Project		Compares a work database with the master database of another project

Table C5.2.2-3 Options menu

Menu item	Description
Settings	Displays the Settings dialog box

IMPORTANT

Make sure to save the analysis results before creating an analysis report.

If the current analysis results and acknowledgement history are not saved before creating an analysis report, a message prompting you to save the history is notified. If you click [Yes] button in the message box, the current analysis results and acknowledgement history are saved, overwriting the history saved before in the process, and an analysis report is created. An analysis report is not created if you click [No] button.

Toolbar

The toolbar provides the following buttons.

Table C5.2.2-4 Toolbar buttons

Button	Name	Description
	Save current analysis history	Saves analysis results and acknowledgement status.
	Print report for a selected resource	Prints analysis reports.
	Display program dependency acknowledgement dialog	Displays the Acknowledge Dependencies dialog box
	Previous dependency change	Selects the icon of the previous element that was changed or affected relative to the currently selected icon in Dependency Tree (the upward direction in the tree).
	Next dependency change	Selects the icon of the next element that was changed or affected relative to the currently selected icon in Dependency Tree (the downward direction in the tree).

Dependency tree

Dependency Tree is displayed on the left pane of the Cross Reference Analyzer window.

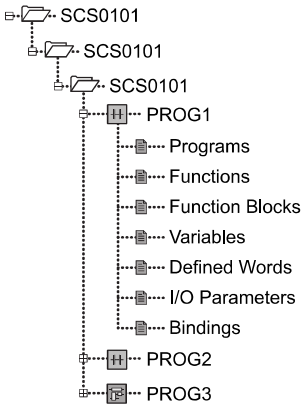


Figure C5.2.2-2 Displaying Dependency tree

Each level of Dependency Tree can be expanded or collapsed by double-clicking an icon, or text label, or clicking the +/- button on the left edge.

Analysis results of an item selected in Dependency Tree is displayed in the right pane.

The display arrangement of Dependency Tree can be defined in Settings dialog box.

Displaying the Settings dialog box

On the [Options] menu, click [Settings]. The Settings dialog box appears.

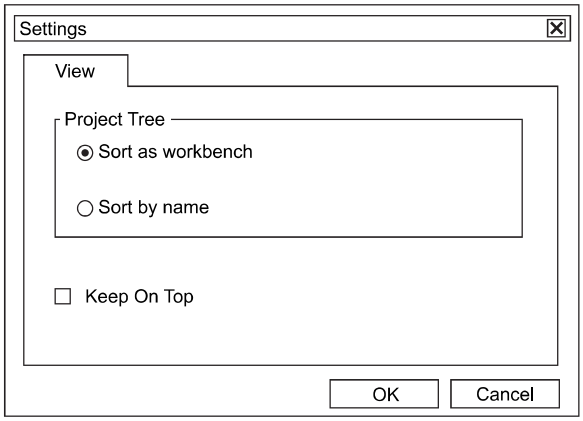


Figure C5.2.2-3 Settings dialog box

- Project Tree
  Sort as workbench: the Dependency Tree is displayed in the same order as the display with Workbench.

  Sort by name: Contents displayed on Dependency Tree are sorted by names alphabetically.
- Keep On Top
  Cross Reference Analyzer window is kept always on top.

C5.2.3 Confirmation of analysis results by Dependency tree

This section explains how to understand the detailed information displayed when layers below resources (SCS projects) are selected in Dependency Tree.

Checking resources

If you select a resource (SCS projects) in Dependency Tree, a list of analysis results of the resource is displayed in the right pane of the window. The list displays changes related to the selected SCS project.

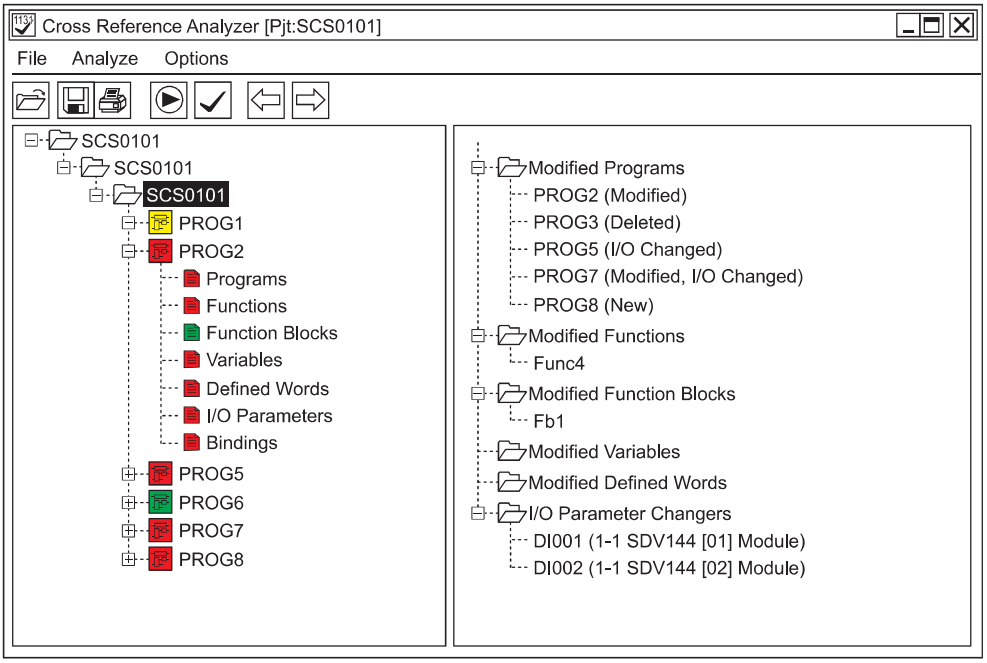


Figure C5.2.3-1 Dependency tree of Cross Reference Analyzer

The analysis results of the selected SCS project are displayed in a tree structure in the right pane. The modifications are displayed as classified groups of modified programs, modified functions, modified function blocks and input/output parameter changes.

Each category can be expanded and collapsed by clicking the +/- button to the left of the category.

Icon colors and classifications of program names

The following table explains icon colors of program names in Dependency Tree and classifications displayed to the right of program names in the "Modified Programs" tree.

Table C5.2.3-1 Icon colors and classifications of program names

Icon color of program name in Dependency Tree	Classification	Description	Display in the right pane (*1)
Red	Modified	The program itself has been changed.	Yes
	Instruction modified (*2)	The program itself has not been changed, but the database downloaded to SCS has been changed.	Yes
	Function modified	The program itself has not been changed, but dependent FUs have been changed. Or user-defined FB is changed to user-defined FU.	Yes
	Function block modified	The program itself has not been changed, but dependent FBs have been changed. Or user-defined FU is changed to user-defined FB.	Yes
	Variable changed	The settings of variable or function block instance used in the POU is changed.	Yes
	Defined Word changed	The value of Defined word used in the POU is changed.	Yes
	I/O changed	The program itself has not been changed, but a dependent input/output has been changed. Otherwise, information regarding a dependent subsystem communication I/O FB, information regarding a PROFINET communication input FB, information regarding a fire and gas communication input FB, or SCS link transmission I/O FB has been changed.	Yes
	New	The program itself has been newly added. Programs added by importing are also regarded as being newly added.	Yes
Yellow	Not modified	The program became dependent as it shares variables with a program requiring code review. The program itself, dependent functions, function blocks and inputs/outputs have not been changed.	No
	Renamed	The program name has been changed. No influence other than the name change. Program name change does not require acknowledgement on the Acknowledge Dialog box.	Yes
Green	(none)	The program is not affected by changes.	No
None (*3)	Deleted	The program has been deleted.	Yes

*1: Yes: Displayed in the right pane.
No: Not displayed in the right pane.
*2: When "Instruction modified" is displayed, please contact Yokogawa's service department.
*3: The program has been deleted and the program name is not displayed in Dependency Tree.

TIP

If the execution order of programs is changed, or a program is inserted or deleted, all the subsequent programs are regarded as being changed. Their icons therefore become red, and retesting of the programs is required.

Displaying analysis results of Functions and Function Blocks

Dependency Tree displays results of analyzing FUs and FBs as part of the summary for the program that calls the FUs and FBs.

- Dependency Tree displays only icons for program names. Icons for FUs and FBs are not displayed.
- If you expand an icon of a program name, the analysis results for the FUs and FBs called by the program are displayed, in addition to the analysis results of the program itself.
- If FUs and FBs have been changed, the icon of the program name that calls these FUs and FBs becomes red.

- If a program on which FUs and/or FBs are dependent has been changed, the icon of the program that calls the FUs and FBs becomes yellow even if no change has been made to the FUs and FBs themselves.
- If you select a resource (SCS project) in Dependency Tree, "Modified Functions" and "Modified Function Blocks" in the right pane display changed FUs and FBs, respectively.

Judging dependencies between POUs

Cross Reference Analyzer judges that there are dependencies between POUs in the following cases. If dependent POUs have been changed, retesting or review is required even if the program itself has not been changed.

Shared global variables

POUs that share global variables are dependent on each other. POUs are considered to be sharing global variables in the following cases.

- POUs are reading and writing directly to/from global variables.
- POUs are reading and writing to/from global variables within called FBs.

If multiple POUs satisfy one of the two conditions above for the same global variable, the POUs are dependent on each other.

The relationship between the global variables and program is displayed in the Current Version Shared Variable Changes Cross Reference item of the Cross Reference Analysis Report. If FBs read and write to/from the same global variables, only the name of the program that uses those FBs is displayed; the names of the FBs are not displayed.

Use of functions or Function Blocks

If a program calls FUs or FBs, there is a dependency between the calling side and the called side. For example, if A calls B and B calls C, not only A and B, and B and C that have direct calling relations, but also A and C, which only have an indirect calling relation, are considered to be dependent on each other.

Checking programs (POU)

When you select a program name in Dependency Tree, a list of program statuses is displayed in the right pane of the window. The list displays the cross reference status (e.g. New, Modified, Binding Error, Function modified, Function block modified) and acknowledgement status of the program.

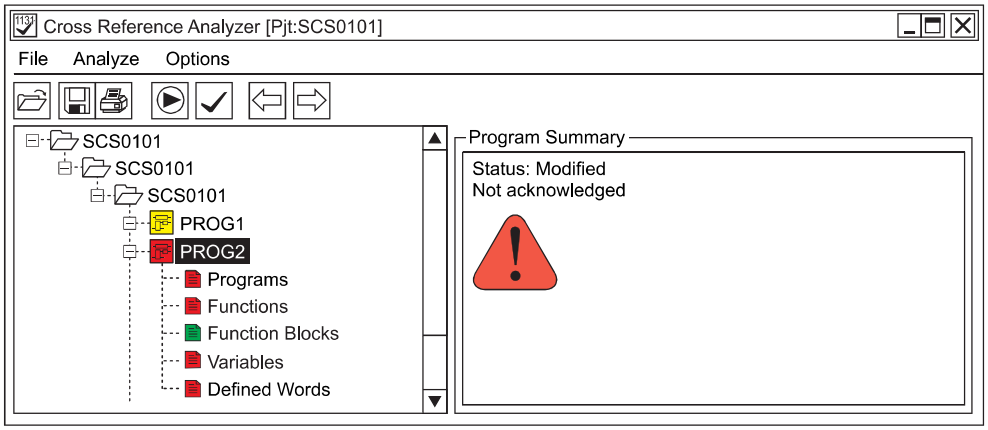


Figure C5.2.3-2 Analysis results of a programs (POU)

Table C5.2.3-2 Meaning of icons displayed on the left side of program names

Icon color	Meaning
Red	The program itself or items that are directly depending on it (FU, FB, input/output) have been changed.
Yellow	Dependencies requiring review are present in the program (the program has not been changed).
Green	The program has not been affected by changes.

Checking programs

If you select [Programs] in the Dependency Tree, programs dependent on the selected program are displayed in a column in the right pane of the window. If multiple variables are shared among programs, all the variables shared in the programs are displayed in the "Variable" column.

Check to see if there is any unintended dependencies. For example, if global variables are shared unintentionally, modify the program to eliminate the dependencies. The programs that have dependencies but not have been changed are displayed with green icons. It is necessary to check programs displayed with green icons as well.

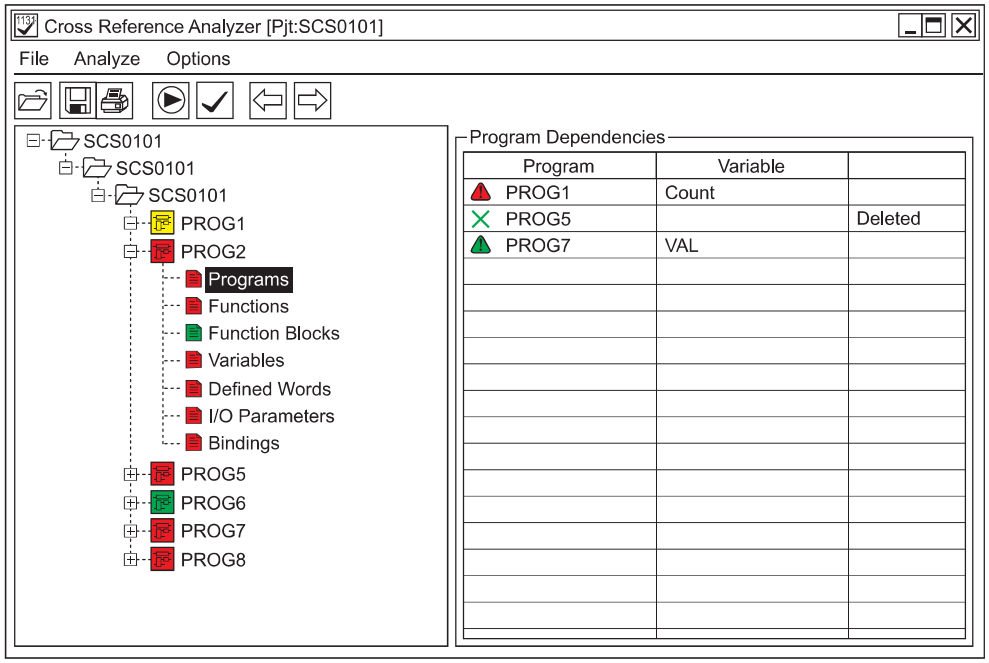


Figure C5.2.3-3 Analysis results of programs

In the preceding figure, PROG2 is selected in the Dependency Tree, and dependencies and changes related to PROG2 are displayed in the right pane of the window.

PROG2 has dependencies on PROG1 and PROG 7. PROG1 has been changed, while PROG7 has not been changed. Although PROG2 had a dependency on PROG5, the dependency on PROG5 is eliminated in the application to be downloaded.

Checking functions

If you select [Functions] in the Dependency Tree, FUs and library FUs directly changed or indirectly affected by changes are displayed in the right pane of the window.

Note that simply changing the order of FUs is irrelevant for the analysis.

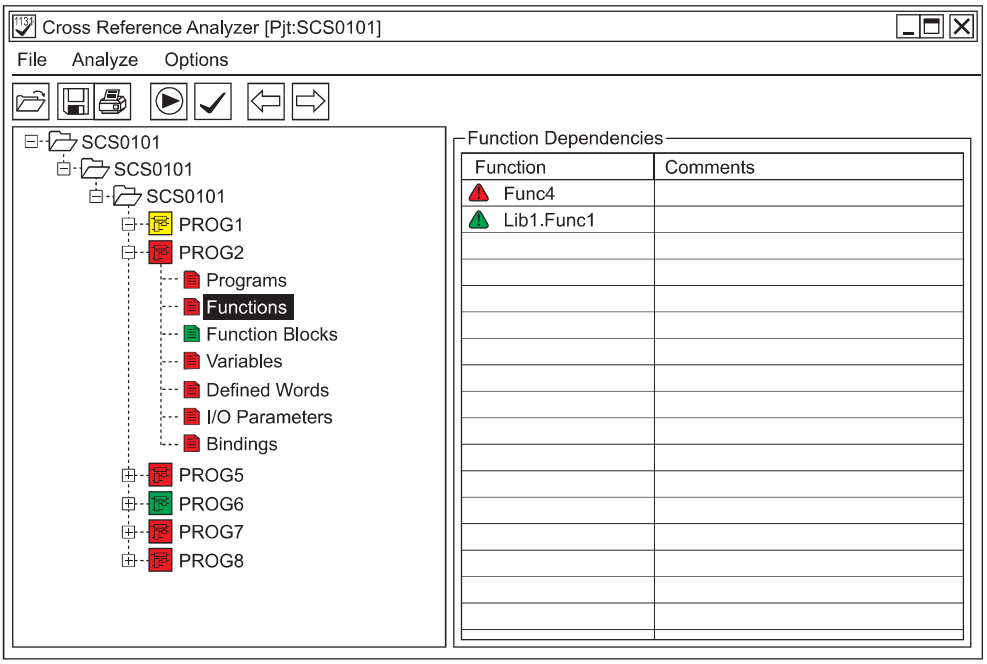


Figure C5.2.3-4 Results of analyzing functions

The preceding figure indicates that PROG2 uses Func4 and Func1 defined in library Lib1. Func4 has been changed, while Lib1.Func1 has not been changed.

TIP

FUs of libraries are displayed using the format "library name.function name."

Checking Function Blocks

If you select [Function Blocks] in the Dependency Tree, FBs and library FBs directly changed or indirectly affected by changes are displayed in the right pane of the window.

Note that simply changing the order of FBs is irrelevant for the analysis.

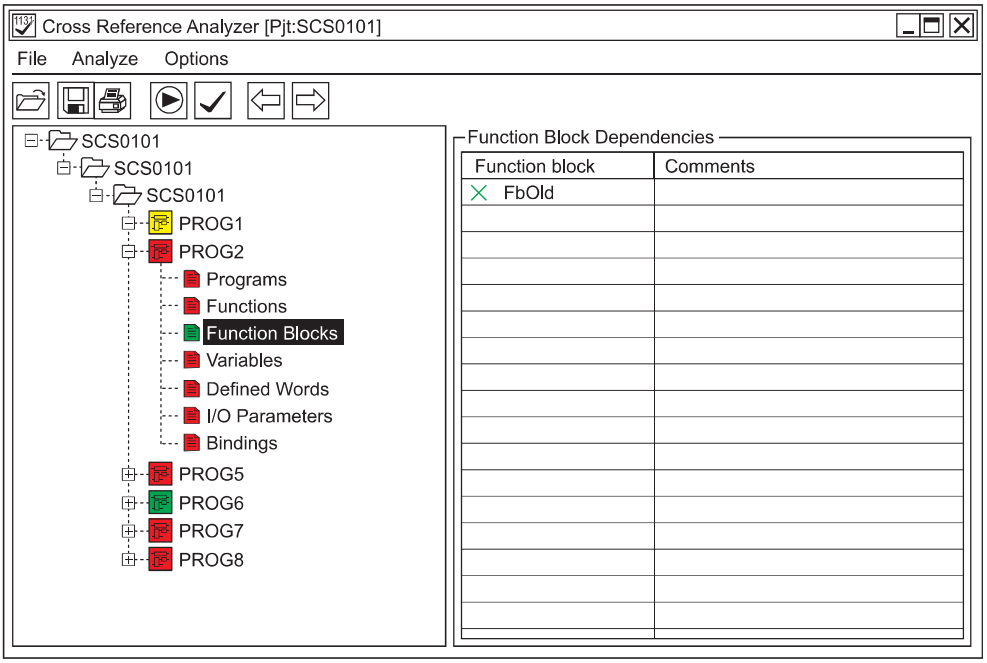


Figure C5.2.3-5 Results of analyzing Function Blocks

The preceding figure indicates that PROG2 used the FbOld function block before, but does not use it any longer.

TIP FBs of libraries are displayed using the format "library name.function block name."

Checking variables

When [Variables] is selected in the Dependency Tree, variables and FB instances whose settings have changed are displayed in the right pane of the window.

These variables and FB instances are used in the selected program (PROG2 in the following figure), or in FU or FB called by the program.

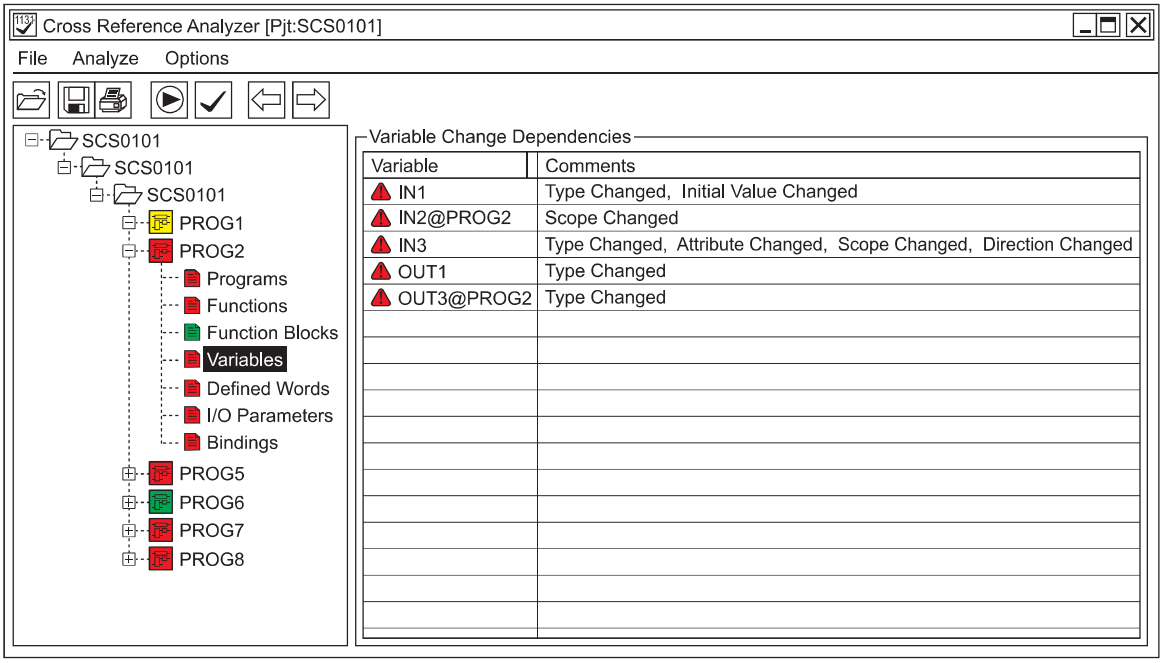


Figure C5.2.3-6 Result of analyzing variables

In the previous figure, IN1 indicates that Type and Initial value were changed.

The following table shows whether a change to the variable or FB instance is detected or not.

Table C5.2.3-3 Changes to variables or FB instances and detection

Item	Detected(*1)	Remarks
Name	No	Changed names are regarded as added variables.
Alias	No	-
Type	Yes	Changes to Type of FB instances included.
() [Specify the number of characters in a STRING variable]	Yes	STRING variables are not allowed to use.
Init. value	Yes	-
Dimension [The extent of index of array]	Yes	Arrays should not be used in FBD and LD.
Group	No	-
Attribute [Read/Write/Free]	Yes	-
Scope	Yes	-
Direction [Input/Output/Internal]	Yes	-

Continues on the next page

Table C5.2.3-3 Changes to variables or FB instances and detection (Table continued)

Item	Detected(*1)	Remarks
Retain [Yes/No]	No	-
Wiring	No	Changed wiring is categorized as "I/O changed."
Address	No	-
Comment	No	-

*1: Yes: Detected as change
No: Not detected as change

Checking defined word

If you select [Defined Words] in the Dependency Tree, the changed defined words are displayed in the right pane of the window.

These defined words are used in the selected program (PROG2 in the following figure), or in FUs or FBs called by the program.

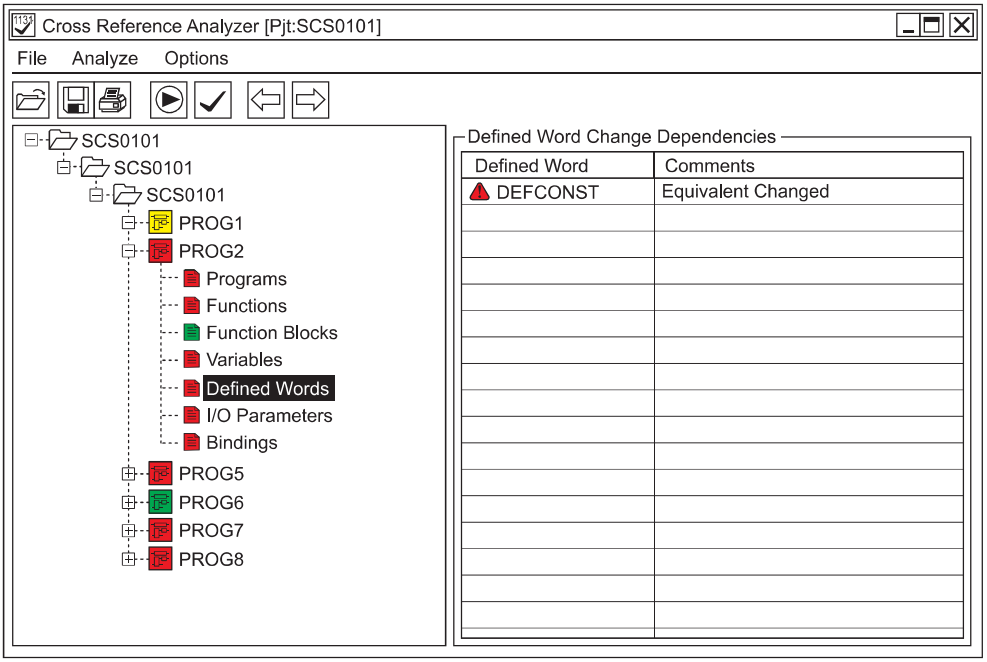


Figure C5.2.3-7 Result of analyzing defined words

The preceding figure shows that the value of DEFCONST was changed.

The following table shows whether a change to the Defined word is detected or not.

Table C5.2.3-4 Changes to defined word and detection

Item	Detected (*1)	Remarks
Word	No	Changed names are regarded as added Word.
Equivalent	Yes	-
Comment	No	-

*1: Yes: Detected as change
No: Not detected as change

Checking input/output parameters

If you select [I/O Parameters] in the Dependency Tree, a list of input/output variables with changed input/output module or input/output channel parameters is displayed in the right pane of the window.

These input/output variables are used in the selected program (PROG2 in the figure below) or FUs and FBs called by the program.

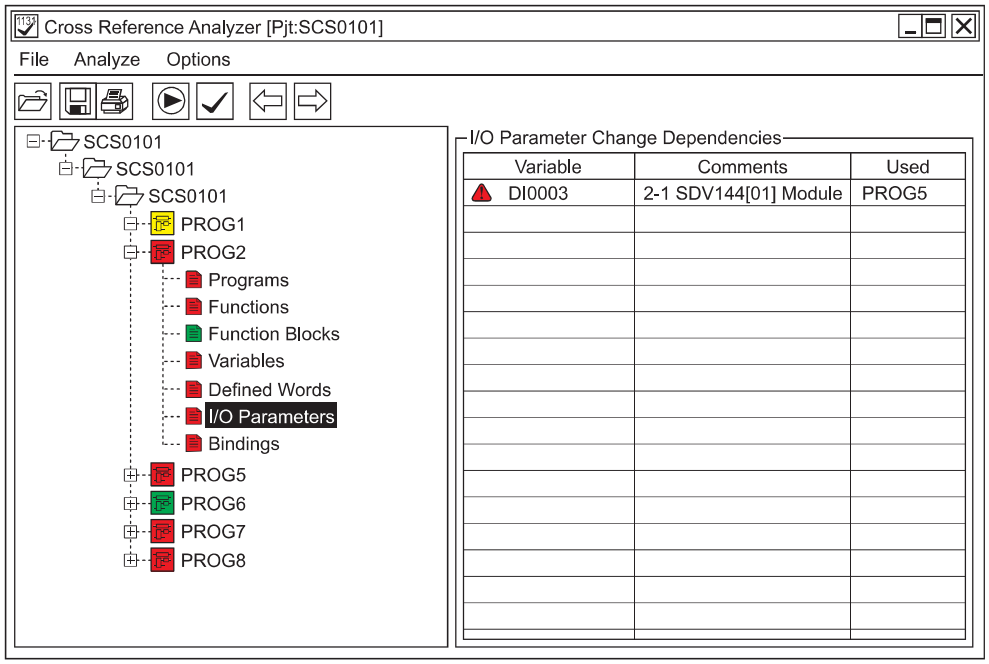


Figure C5.2.3-8 Results of analyzing input/output parameters

The preceding figure shows the following.

- PROG2 uses the variable DI0003.
- The input/output parameters related to DI0003 have been changed.

SEE ALSO For more information about details on how to check the input/output parameters, refer to:

"■ Checking when input/output parameters have been changed" on page C5-40

Explanation of entries in the Comments column

The format of the entries in the Comments column is explained below.

- For FIO
  <Node number>-<slot number><module model>[<channel number>]<wiring information><parameter information>
- For N-IO
  <Node number>-<unit number><slot number><module model>[<channel number>]<wiring information><parameter information>

Wiring information (omitted if there are no changes)

- New addition: Wiring-Added
- Change: Wiring-Changed

Parameter information (omitted if there are no changes)

- Parameters common to modules have been changed: Module
- Channel parameters have been changed: Channel
- Both are changed: Module Channel

Extent of influence of input/output parameter changes

The table below shows the influence that changes made to input/output parameters have on an application logic.

Table C5.2.3-5 Influence of I/O parameters

Classification	Example	Influence on application logic
Changes affecting data	Specification of Input Processing at Fault	Member v of the IO_BOOL and IO_REAL structure of input/output variables is influenced.
Changes affecting data status	Specification of disconnection detection specification of short-circuit detection	Member status of the IO_BOOL and IO_REAL structure of input/output variables, or the system FB notifying the status of an inputs and outputs is influenced.
Changes not affecting application logic	Comment	No influence on an application logic

SEE ALSO For more information about influence on system FBs notifying the status of inputs and outputs, refer to:

"■ Influence of input/output changes" on page C5-46

Changing Scan period

If you change the scan period of an application logic, the system automatically changes all internal parameters of the N-IO module common area of an SCS. As a result, the analysis results of Cross Reference Analyzer become as follows.

- The analysis results of all programs accessing the I/O variables that are wired to an N-IO module become "I/O Changed" and the color of the corresponding program icons becomes red.
- "I/O Parameter changes" in the right pane of the window and the "Current Version I/O Parameter Changes Cross Reference" item of the Cross Reference Analysis Report display "Module" indicating changes (I/O module common area) for all I/O variables that are wired to an N-IO module.

Checking binding variables

If you select [Bindings] in the Dependency Tree, binding variables depending on the selected program (PROG2 in the following figure) are displayed in the right pane of the window.

These binding variables are used by the program or FBs called by the program.

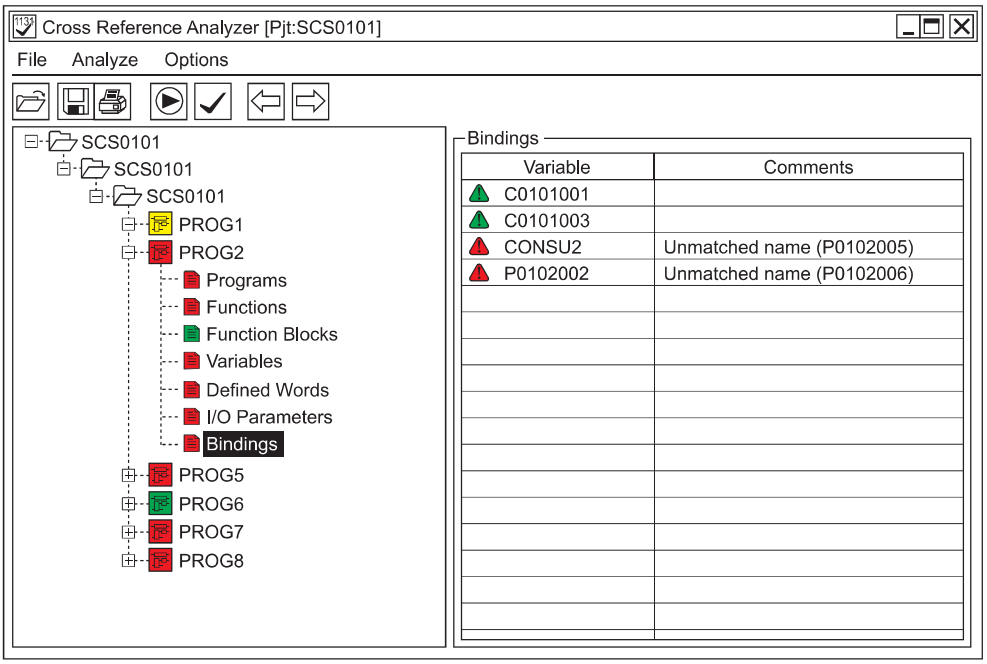


Figure C5.2.3-9 Results of analyzing bindings

The preceding figure shows the following.

- Four variables are used in PROG2 for inter-SCS safety communication.
- Binding is set properly for C0101001 and C0101003.
- For CONSU2 and P0102002, binding is set with variables that do not match the specified names.

C5.2.4 Checking with Analysis report

An analysis report displays analysis results in the same order as in Dependency Tree. It also displays the acknowledgement status set in the Acknowledge Dependencies dialog box. An analysis report can also be printed.

This section describes how to check dependencies for the following cases:

- When I/O parameters have been changed
- When information related to a subsystem communication I/O FB has been changed
- When information related to a PROFINET communication input FB or fire and gas communication input FB has been changed
- When settings of SCS link transmission have been changed
- When inter-SCS safety communication is used

Checking when input/output parameters have been changed

The results of analysis when input/output parameters have been changed are displayed in the "Current Version I/O Parameter Changes Cross Reference" item of the Cross Reference Analysis Report as a dependency between the input/output variables whose parameters were changed and programs.

An example of a case where input/output parameters have been changed is shown below.

Example:

DO modules (SDV531) are mounted on slots 3 and 5 of node 2 of an SCS

(1) Parameters in the module common area of slot 3 are changed

(2) Channel parameters of channel 5 of slot 3 and channel 7 of slot 3 are changed

(3) Wiring is added for channel 2 of slot 3 and channel 1 of slot 5

(4) Wiring is changed for channel 3 of slot 3 and channel 2 of slot 5

Assuming the changes outlined in (1) to (4) are made, the Cross Reference Analysis Report displays as follows:

Current Version I/O Parameter Changes Cross Reference

Variable	Comments	Used
V020301	2-3 SDV531 [01] Module	PROG5 .....(1)
V020302	2-3 SDV531 [02] Wiring-Added Module	PROG5 .....(3)+(1)
V020303	2-3 SDV531 [03] Wiring-Changed Module	PROG5 .....(4)+(1)
V020304	2-3 SDV531 [04] Module	PROG5 PROG6 .....(1)
V020305	2-3 SDV531 [05] Module Channel	PROG6 .....(2)+(1)
V020306	2-3 SDV531 [06] Module	PROG6 .....(1)
V020307	2-3 SDV531 [07] Module	PROG6 .....(1)
V020308	2-3 SDV531 [08] Module	PROG5 PROG6.....(1)
V020501	2-5 SDV531 [01] Wiring-Added	PROG7 .....(3)
V020502	2-5 SDV531 [02] Wiring-Changed	PROG7 .....(4)
V020507	2-5 SDV531 [07] Channel	PROG7 .....(2)

- Variable column

  Names of input/output variables.

- Comments column

The comments are displayed in the following formats:

- For FIO
  <Node number>-<slot number><module model>[<channel number>]<wiring information><parameter information>
- For N-IO
  <Node number>-<unit number><slot number><module model>[<channel number>]<wiring information><parameter information>

Wiring information (omitted if there are no changes)

- New addition: Wiring-Added
- Change: Wiring-Changed

Parameter information (omitted if there are no changes)

- Parameters common to modules have been changed: Module
- Channel parameters have been changed: Channel
- Both have been changed: Module Channel

- Used column

  Displays names of programs accessing relevant input/output variables. If FBs are reading or writing to/from the input/output variables, only the names of programs using the FBs are displayed and the names of the FBs are not displayed.

Checking when information related to a subsystem communication I/O FB, PROFINET communication input FB, or fire and gas communication input FB has been changed

After analyzing the changed settings which are relevant to a subsystem communication I/O FB, PROFINET communication input FB, or fire and gas communication input FB, the changed settings and their crossed references with programs will be displayed in the section for "Current Version I/O Parameter Changes Cross Reference" in the Cross Reference Analysis Report.

Example:

A communication module (ALR111M) is located at SCS Node 1, Slot 3 and the following variable names are defined:

- Definition 1: SCI_B01 - SCI_B04
- Definition 2: SCO_B01 - SCO_B03
- Definition 3: SCO_I01 - SCO_I04

In this case, implement the following changes.

(1) Parameters for definition 1 are changed (Node1-Slot3).

(2) A wiring for SCO_B04 is added to definition 2 (Node1-Slot3).

(3) A wiring for SCO_I01 of definition 3 is changed (Node1-Slot3).

(4) A new communication module (ALR111M) is added to Node2-Slot4 with a new definition and wiring SCO_R01 added.

After (1) to (4) are implemented, the Cross Reference Analysis Report display will be as follows.

Current Version I/O Parameter Changes Cross Reference

Variable	Comments	Used
SCI_B01	1-3 ALR111M Comm.Def	PROG4.....(1)

SCI_B02	1-3 ALR111M Comm.Def	PROG4.....(1)
SCI_B03	1-3 ALR111M Comm.Def	PROG4.....(1)
SCI_B04	1-3 ALR111M Comm.Def	PROG4 PROG6.....(1)
SCO_B04	1-3 ALR111M Wiring-Added	PROG7.....(2)
SCO_I01	1-3 ALR111M Wiring-Changed	PROG1.....(3)
SCO_R01	2-4 ALR111M Wiring-Added Module Comm.Def	PROG1.....(4)

- Variable column

  Names of FB variables.

- Comments column

  The format of the entries in the Comments column is explained below.

  <Node Number> - <Slot Number> <Module Model> <Wiring Information> <Parameter Information>

  Wiring information (omitted if there are no changes)

  - New addition: Wiring-Added
  - Change: Wiring-Changed

  Parameter information (omitted if there are no changes)

  - Communication parameters have been changed: Comm.def
  - Module parameters have been changed: Module (*1)

  *1: For a newly added communication module, Comm.def is shown in addition to Module.

The wiring information and parameter information regarding the changes are indicated as follows:

Table C5.2.4-1 Wiring information and parameter information regarding the changes

Changes	Wiring Information	Parameter Information
A communication module has been added (when a communication definition is added and wired FB is used in the POU)	Wiring-Added	Module Comm.Def
Settings for transmission are changed.	-	-
A communication definition has been added (when wired FB is used in the POU)	Wiring-Added	Comm.Def
A communication definition is deleted.	-	-
A communication definition is changed.	-	Comm.Def
An FB has been added	Wiring-Added	- (*1)
Wiring of a FB has been changed	Wiring-Changed	- (*1)
An FB has been deleted	-	-

*1: Comm.def will be displayed if communication definition is changed.

- Used column

  The names of programs accessing the corresponding FB variables are shown. When the FB variables are subject to reading or writing, only the names of the programs using the FB are shown and the names of the FB are not shown.

Checking when the settings of SCS link transmission have been changed

The results of analysis when settings of SCS Link Transmission have been changed are displayed in the "Current Version I/O Parameter Changes Cross Reference" item of the Cross Reference Analysis Report as a dependency between the SCS Link Transmission I/O FBs whose parameters were changed and programs.

Example:

In SCS Link Transmission Builder, the variables with the following variable names are defined in Station 2.

- LTSND02001 for the first bit, LTSND02002 for the second bit of Station 2 (Self Station)
- LTRCV04001 for the first bit, LTRCV04002 for the second bit, LTRCV04003 for the third bit of Station 4 (SCS)
- LTRCV05001 for the first bit of Station 5 (SCS)
- LTFCS06001 for the first bit, LTFCS06002 for the second bit of Station 6 (FCS)
  In this case, implement the following changes.

  (1) Add wiring definition (LTSND02003) for the third bit of Station 2.

  (2) Change reception timeout of Station 4.

  (3) Change input processing at fault in wiring definition (LTRCV04002) for the second bit of Station 4.

  (4) Move wiring definition (LTRCV04003) for the third bit of Station 4 to the fourth bit.

  (5) Add definition (LTFCSXX04003) for the third bit of Station 4.

  (6) Change input processing at fault in wiring definition (LTRCV05001) for the first bit of Station 5.

  (7) Move wiring definition (LTFCS06002) for the second bit of Station 6 to the third bit.

  (8) Add Station 7 (SCS), add wiring definition LTRCV07001 and LTRCV07002 for the first bit and the second bit of Station 7.

  After (1) to (8) are implemented, the Cross Reference Analysis Report display will be as follows.

  Current Version I/O Parameter Changes Cross Reference

Variable	Comments	Used
LTSND02003	LT02-003 Wiring-Added	PROG7...(1)
LTRCV04001	LT04-001 Station	PROG4...(2)
LTRCV04002	LT04-002 Station LinkTrans.Def	PROG4...(2) + (3)
LTFCSXX04003	LT04-003 Wiring-Added Station	PROG4...(2) + (5)
LTRCV04003	LT04-004 Wiring-Changed Station	PROG4...(2) + (4)
LTRCV05001	LT05-001 LinkTrans.Def	PROG6...(6)
LTFCS06002	LT06-003 Wiring-Changed	PROG2...(7)
LTRCV07001	LT07-001 Wiring-Added Station	PROG3...(8)
LTRCV07002	LT07-002 Wiring-Added Station	PROG3...(8)

- Variable column
  Variable names of SCS Link Transmission I/O FBs

- Comments column
  The notational convention in the Comments column is explained below.

  LT<SCS Station Number (2 digits)> - <Bit Number (3 digits)><Wiring Information><Parameter Information>

  Wiring information (omitted if there are no changes)
  - New addition: Wiring-Added
  - Change: Wiring-Changed

  Parameter information (omitted if there are no changes)
  - Change of reception timeout, transmission timeout or pre-alarm set point: Station
  - Change of input processing at fault: LinkTrans.Def
  - Both: Station LinkTrans.Def

The wiring information and parameter information regarding the changes are indicated as follows:

Table C5.2.4-2 Wiring information and parameter information regarding the changes

Change	Wiring	Parameter	Remarks
Add Station	Wiring-Added	Station	Detect when wired FB is used in POU
Delete Station	-	-	Do not detect
Change Station Type	Wiring-Added	Station	Detect when wired FB is used in POU
Change Station Parameter	-	Station	Change of reception timeout, transmission timeout or pre-alarm set point
Add SCS Link Transmission I/O FB variables to Wiring Definition	Wiring-Added	-(*1)	Detect when wired FB is used in POU
		Station (*1)	Change of reception timeout, transmission timeout or pre-alarm set point
Delete SCS Link Transmission I/O FB variables from Wiring Definition	-	-	Do not detect
Move SCS Link Transmission I/O FB variables of Wiring Definition	Wiring-Changed	-(*1)	Detect when wired FB is used in POU
		Station (*1)	Change of reception timeout, transmission timeout or pre-alarm set point
Change Wiring Parameter	-	LinkTrans.Def	Change of input processing at fault
		Station LinkTrans.Def	Change of input processing at fault, reception timeout, transmission timeout or pre-alarm set point

*1: When adding a wiring, changing a wiring or changing the input processing at fault, LinkTrans.Def will be omitted.

- Used column
  Displays names of the programs accessing the variables of SCS Link Transmission I/O FBs. When accessing the SCS Link Transmission I/O FBs from FU or FB, only the names of programs using the FUs or FBs are displayed and the names of the FUs or FBs are not displayed.

Identification of programs when Inter-SCS safety communication is used

Inter-SCS safety communication is implemented using FBs for communication and binding functions. In a communication configuration, the SCS sending data is called the producing side and the SCS receiving data is referred to as the consuming side.

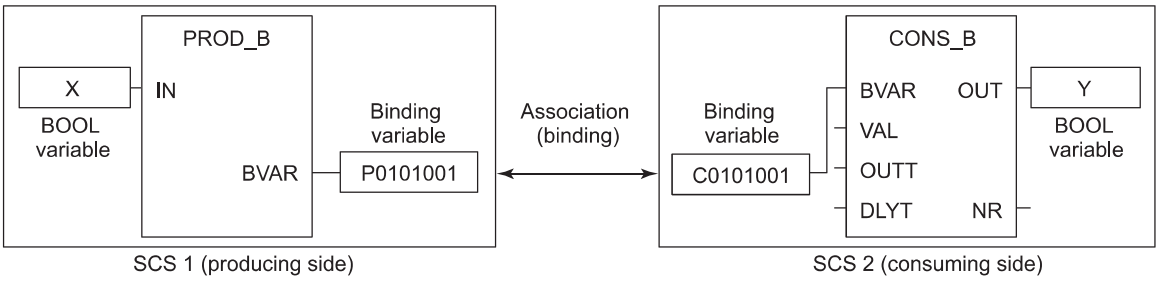


Figure C5.2.4-1 Inter-SCS communication (Example of BOOL-type variable)

The producing side and the consuming side share data using inter-SCS safety communication; they are thus dependent on each other. For this reason, if a program on the producing side has been changed, it is necessary to perform retesting or review of programs on the consuming side.

The procedure for identifying programs that may be affected is shown below.

1. Check programs displayed with red or yellow icons in Dependency Tree on the producing side.
2. Check variables for inter-SCS safety communication used in these programs.

   The "Current Version Bound Variable Usage" item of the Cross Reference Analysis Report shows binding variables used in each program. Variables starting with the letter P are variables on the producing side.
3. Check whether or not specified data has been changed for variables starting with the letter P in each program.

   If there are no changes in the specified data, the review of binding variables is finished.
4. Variables on the consuming side corresponding to binding variables whose data has been changed (variables starting with the letter P) have the same names as the binding variables, except that P is replaced with C.
5. Check the programs starting with the letter C that use the binding variables explained in step 4 in the "Current Version Bound Variable Usage" item of the Cross Reference Analysis Report.

   These programs and dependent programs are the targets of retesting or review.
6. Dependent programs are displayed in Dependency Tree by expanding the [Programs].

Current Version Bound Variable Usage

Program	Bound variables
PROG1	P0101001
PROG2	P0101002 P0101003
PROG5	
PROG6	
PROG7	P0101004
PROG8	

Figure C5.2.4-2 Current Version Bound Variable Usage of Cross Reference Analysis report (Example of producing side)

Current Version Bound Variable Cross Reference

Bound variables	Used
C0101001	PROGA
C0101002	PROGA
C0101003	PROGB
C0101004	PROGC

Figure C5.2.4-3 Current Version Bound Variable Cross-Reference item of Cross Reference Analysis report (Example of consuming side)

C5.2.5 Precautions on Cross Reference Analyzer

Cross Reference Analyzer cannot detect certain changes.

This section explains changes that are not detected by Cross Reference Analyzer and actions to be taken, and shows examples of procedures for checking such changes.

The user must check the following for SCS projects.

- Influence of input/output changes
- Change in tag name defined to allow manipulation from HIS
- Other changes not detectable by Cross Reference Analyzer

If library projects have been changed, it must be checked whether or not there are changes for the library projects as well.

Influence of input/output changes

Cross Reference Analyzer detects changes of input/output parameters and shows dependencies related to input/output variables.

However, it does not detect dependencies between inputs/outputs and system FBs that indicate input/output status.

These system FBs show the status of I/O corresponding to the node numbers, unit numbers, slot numbers and channel numbers specified for I/O variables.

Table C5.2.5-1 System Function Blocks related to inputs/outputs

Type name	Description
SYS_IOALLST	All I/O channels of SCS status indicator
SYS_NODEST	I/O channel data status indicator in FIO node
SYS_N_NODEST	All I/O channel data status indicator in N-IO node
SYS_NODEINF	FIO node status notification
SYS_N_NODEINF	N-IO node status notification
SYS_OUTST, SYS_OUTST16	FIO output module data status
SYS_N_IOST16	N-IO I/O module data status for 16 channels
SYS_INST	Detects fault in input module channels
SYS_CHST	Detects fault in channels
SYS_IOSD	Shuts down FIO output module output
SYS_N_IOSD	Shuts down N-IO I/O module output
SYS_OUTEN	FIO output module output enabled status
SYS_N_OUTEN	N-IO I/O module output enabled status
SYS_CH_OUTEN	FIO/N-IO output channel output enabled status
SYS_IOMDSP	FIO module status notification
SYS_N_IOMDSP	N-IO module status notification
SYS_ALRDSP	Outputs status of subsystem communication modules
SYS_LTSTS	SCS link transmission reception status monitor (*1)

*1: SYS_LTSTS will be affected by the setting change of SCS Link Transmission definition instead of the setting change of I/O.

If you change input/output parameters, the status of the inputs/outputs may change, which means that the output of these system FBs may change. In other words, such inputs/outputs and system FBs are dependent on each other.

Cross Reference Analyzer is unable to show dependencies between changes to input/output parameters and system FBs. If you are going to change input/output parameters, check whether or not performing such changes to input/output parameters affect other system components before downloading them to an SCS. An example of checking procedure is shown below.

1. Select a resource (SCS project) name in Dependency Tree of Cross Reference Analyzer.
2. Check "I/O Parameter Changes" displayed in the right pane of the window.

   If no input/output variables are changed, checking is finished.
3. If there are input/output variables that have been changed, check programs that use system FBs related to the inputs/outputs, and then judge whether the changes of the input/output parameters affect them. If it is judged that the FBs are affected, check the programs depending on the program in question by expanding relevant [Programs] in Dependency Tree and retest the programs depending on the program in question.

Change in tag name defined to allow for manipulation from HIS

From HIS instrument faceplates for "Override FB", "Grouping Override FB", "Password FB" and "Manual operation FB", you can change the variables in the application logic.

To allow manipulation from HIS, tag names for those FBs are set by Tag Name Builder. Even if a user changes the tag name, the change is not detected by Cross Reference Analyzer. Check whether or not tag names have been changed. Whether or not tag names have been changed can be checked by comparing the modified project data to the master database by means of Project Comparing Tool. Check can also be made by using output of self-documentation. An example of checking procedure by using output of self-documentation is shown below.

Preparation

Prepare the information before changes are made. That is, printout of the tag names of override FBs, grouping override FBs, password FBs, manual operation FBs and their corresponding internal variables (including POU names), which was printed by using the self-documentation function.

Checking procedure at online change download

1. If you change a tag name, a diagnostic information message is displayed to notify the tag name change at online change download. Check whether or not messages indicating tag name changes are displayed in the Diagnostic Information window of SCS Maintenance Support Tool.
   If no diagnostic information messages notifying tag name changes are displayed, no tag names have been changed. Checking is finished.
2. If diagnostic information messages notifying tag name changes are displayed, check that the tag names in the messages match with the intended changes.
3. Check programs of the application logic corresponding to the changed tag names in Dictionary View of SCS Manager. Test the checked program, as well as the programs that depend on the checked program. Check dependent programs by expanding the relevant [Programs] in Dependency Tree of Cross Reference Analyzer.
4. Print and store the printed documents for the next offline download.

Checking procedure at offline download

In case of offline download, compare the printed and saved list of tag names using the self-documentation function and the current status, and check the differences.

1. Display the current list of tag names in Tag Name Builder. Alternatively, print the list by using the self-documentation function.

2. Compare the current tag names with the tag names printed and saved in advance. If there are no differences, checking is finished.
3. If there are differences, check programs of the application logic corresponding to the changed tag names in Dictionary View of SCS Manager. Test the checked program, as well as the programs that depend on the checked program. Check dependent programs by expanding the relevant [Programs] in Dependency Tree of Cross Reference Analyzer.
4. Print and store the printed documents for the next offline download.

Other changes not detectable by Cross Reference Analyzer

Cross Reference Analyzer does not detect differences in items other than the definitions of the application logic. So, you need to check for changes using Project Comparing Tool or the output of self-documentation. Especially for the following definitions that are significant on safety, the user must check for changes before downloading to an SCS.

- Scan period for the application logic execution functions (defined in the Settings tab of Resources Properties in Link Architecture View)
- Use of optical ESB bus repeaters and their maximum extension distance (defined on SCS Constants Builder and I/O Parameter Builder)
- Extend scan period automatically (defined on SCS Constants Builder)
- Locking of internal variables (defined on SCS Constants Builder)
- Behavior at abnormal calculation (defined on SCS Constants Builder)
- Automatic IOM download (defined on SCS Constants Builder)
- Device Power-Off Period (defined with SCS Constants Builder)
- Device Startup Waiting Period (defined with SCS Constants Builder)
- Alarm Suppression During Device Reset (defined with SCS Constants Builder)
- Fire and gas communication startup time (defined with SCS Constants Builder)

An example of checking procedure by using the output of self-documentation is shown below.

Preparation

Prepare the information before changes are made. That is, printout of the settings of Resources Properties in Link Architecture View and definitions made on SCS Constants Builder, which was printed by using the self-documentation function.

Procedure before download

1. On SCS Manager, open Resources Properties in Link Architecture View and click the [Settings] tab. The scan period (cycle time) is shown in the tab page; so compare it with the scan period in the printout you kept to see if there is difference.
2. Open SCS Constants Builder. In the [SCS] tab page, the above mentioned definitions are shown. Compare them with those in the printout you kept and check for difference.
3. To be prepared for the next time, use the self-documentation function to print out the SCS project properties and definitions made on SCS Constants Builder and keep it.

C5.2.6 Comparison with the original project

Cross Reference Analyzer has the function to compare the work database with the master database of another SCS project, which allows you to verify that there is no difference between the regenerated SCS project and the original project.

This function eliminates the need to retest all the POUs in the case, for example, when an existing project is recreated in order to add a newly supported input/output module to it.

Place the original project at a location that is accessible by the SENG and specify it as the project to be compared; then run the analysis by Cross Reference Analyzer. You don't need to open the original project on SCS Manager or re-set the paths to the libraries.

An example of the comparison procedure is shown below.

Procedure for comparison with the original project

From the [Analyze] menu of the Cross Reference Analyzer, select [Compare with Original Project]. When Compare with Original Project starts up, a dialog box appears, prompting you to specify the top path to the SCS project which you want to compare. Specifying the path to the SCS project and clicking [OK] starts the comparison. The work database of the project you are working with on SCS Manager is compared with the master database of the project you have specified.

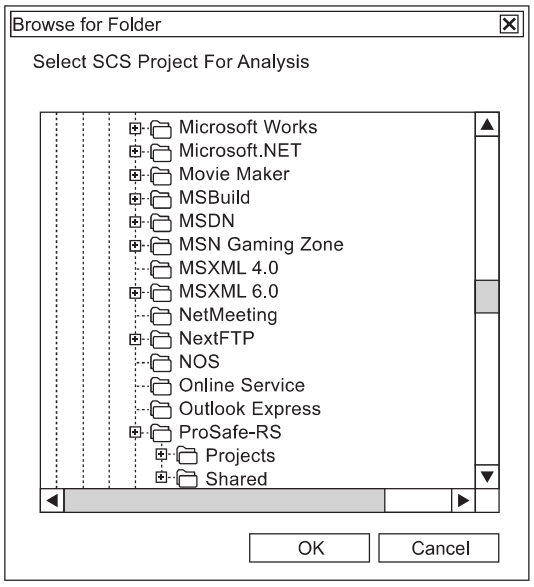


Figure C5.2.6-1 Dialog box for selecting the path to the original project

However, note that the comparison is performed only when the target names (SCS_TARGET/SCS_SIMULATOR) match between the project you are working with on SCS Manager and the project specified for comparison. If the target names do not match, Cross Reference Analyzer regards it as an error and the analysis fails. When all POUs have been acknowledged through comparison with the original project, you can download the project to an SCS. After downloading is completed, if you display the analysis results using the previous analysis result displaying function of Cross Reference Analyzer, the results of comparison with the original project will be shown.

Indication on Cross Reference Analyzer

If you have run the analysis by using the [Compare with Original Project] command, the indication on the Cross Reference Analyzer window and the printout of the analysis report will be as shown below. You can identify the original project that is used for comparison from these indications.

- Path to the original project is shown on the title bar.

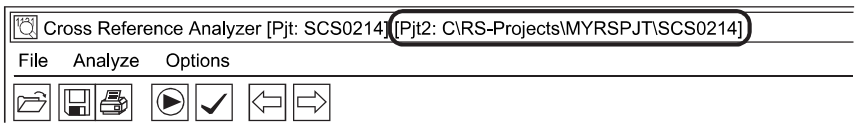


Figure C5.2.6-2 Title bar

- Path to the original project is printed in the report

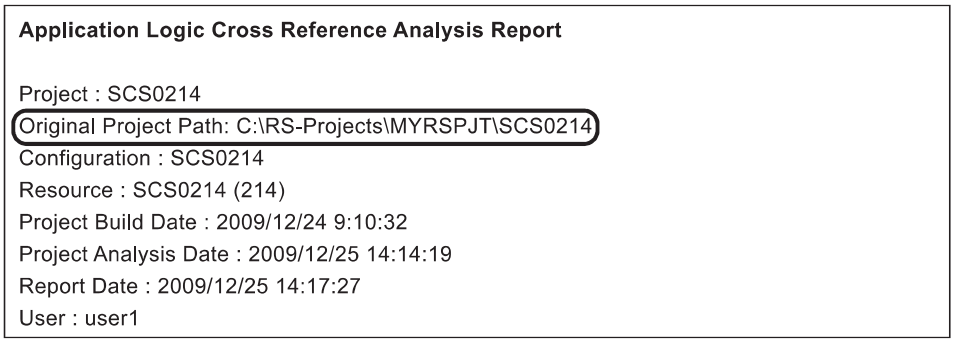


Figure C5.2.6-3 Report

Notes on comparison

If you add or delete programs after you creating a new project and importing data to it, all the programs following the added or deleted program will be regarded as changed programs during comparison with other project. When you create a new project and import data to it, use Cross Reference Analyzer to compare the created project with the original project and download it to the SCS before you make any further changes.

Checking the regenerated project

Use Cross Reference Analyzer to verify the equivalence between the regenerated project and the original project. For the data that cannot be verified by Cross Reference Analyzer, you need to check that the regenerated SCS project and the original SCS project are the same by means of Project Comparing Tool. If you have made further changes to the regenerated project, perform checking using Cross Reference Analyzer and self-documentation output to make sure the range of retesting, as should be done with the earlier revisions.

SEE ALSO For more information about procedures for checking a regenerated project and the definition items of the project that need to be checked, refer to:

- E3.3, “Data transfer procedure during SCS project regeneration” on page E3-9
- C5.2.5, “Precautions on Cross Reference Analyzer” on page C5-46

C6. Simulation tests

Applications should be tested in the simulator running on SENG by using the logic simulation test or the SCS simulation test. When running an SCS simulation test on SCS projects with Current Project attribute, create an SCS project for testing by using the Test Project Creation Tool as preparation for the test. Register the SCS project for testing in an AD project for testing.

Application logic can be debugged with the Application Debug Function, Forcing of I/O variable and Online Monitoring Function. In the logic simulation test or the SCS simulation test, I/O channels are equivalent to being locked all the time. In the logic simulation test or the SCS simulation test, connect iDefine by using the iDefine Test Manager and you can use the iDefine test functions to test the parts created in iDefine.

SEE ALSO

For more information about logic simulator test operations, refer to:

2., “Logic simulation test operations” in Test Function Guide (IM 32P04B30-01EN)

For more information about preparing and running SCS simulation tests, refer to:

3., “SCS simulation tests” in Test Function Guide (IM 32P04B30-01EN)

For more information about the operations for using iDefine in simulation tests, refer to:

6., “Using iDefine in tests” in Test Function Guide (IM 32P04B30-01EN)

C7. Offline download to the target SCS

During offline download, the SCS database, which contains all the information required for operation of an SCS, is transmitted from the SENG to the SCS; meanwhile, the SCS functions are stopped. The SCS database is downloaded via the control bus and stored in the flash memory of the SCS and the non-volatile memory of input/output modules. The SCS database downloaded to the SCS is saved as the master database together with the source files in the SENG.

Downloaded items

- SCS system programs
- Application database
  The application database created by the Safety application definition function and CENTUM integration function is downloaded to the CPU module.
- I/O configuration information
  The parts of the database created by the I/O definition function related to input/output modules are downloaded to the input/output modules.

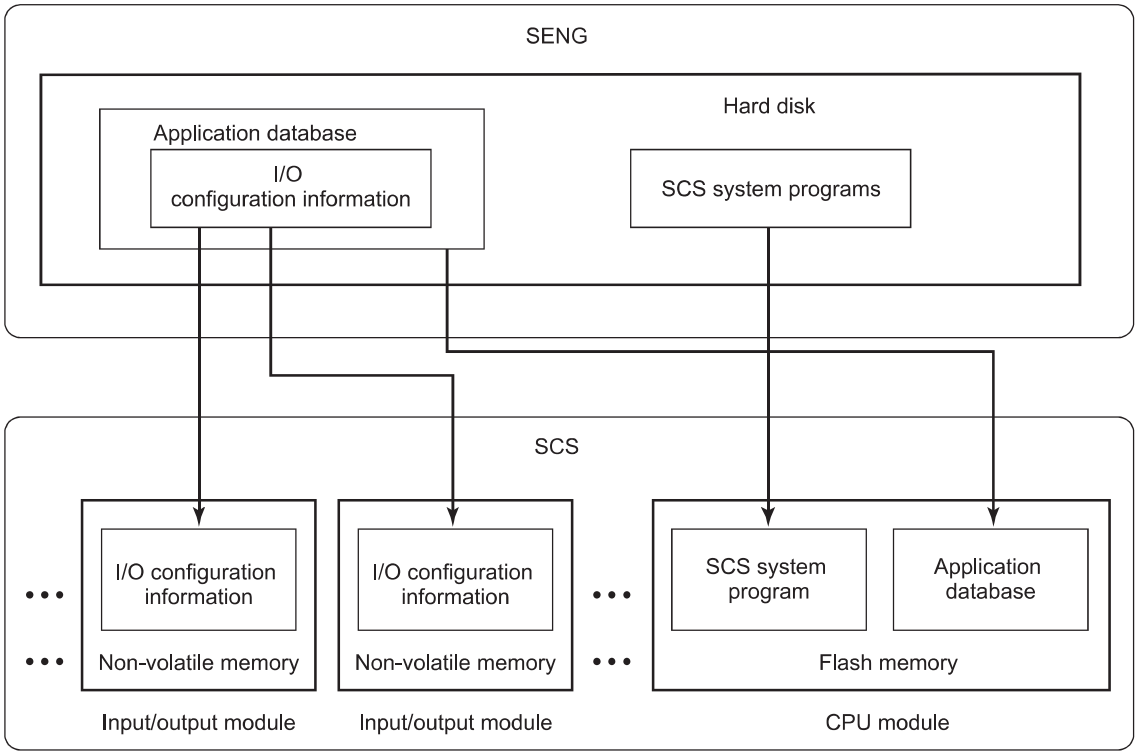


Figure C7-1 Offline download

CAUTION

The following operations are performed if you run offline download. Actions to prevent false trip are required before running offline download.

- Functions running on the SCS stop, and all the output modules output the fail-safe values that are specified in I/O parameters.
- Inter-SCS safety communication is disconnected.
- The forcing function is cancelled.
- Override from the HIS is cancelled.
- Break points set by the target test function are cancelled.
- SOEs and diagnostic information collected so far in the SCS are deleted (they are saved in the NVRAM (nonvolatile RAM)).
- Password for changing the SCS security level is deleted.

Procedure for offline download

This section describes procedures from building an application logic to performing offline download.

IMPORTANT

Perform Clean Project in a timely manner; specifically, before FAT (Factory acceptance tests) or SAT (Site acceptance tests). Before you execute offline download, we recommend you perform Clean Project.

SEE ALSO For more information about clean project, refer to:

"Cleaning Projects" in "Build" in "Code Generator" in "Workbench" in the Workbench User's Guide

What to do before offline download

Build the application logic and analyze it by using Integrity Analyzer and Cross Reference Analyzer.

TIP The items that may require retesting but not detected by Cross Reference Analyzer must be checked by the user.

IMPORTANT

Call up the SCS Information dialog box and confirm that the number of logical I/O points in use does not exceed the number of assigned I/O licenses.

If the target SCS is running, set the SCS security level to Level 0 by using the SCS Security Level Management Function.

Start the offline download

1. From the [Debug] menu of SCS Manager, select [Download].

On the CENTUM Integration, a dialog box asking you if you want to save Operation Mark or not appears.

2. Save Operation Mark if necessary.

TIP

- If Integrity Analyzer or Cross Reference Analyzer has already been launched when you start offline download, a message prompting to close the analyzer is notified and the download ends with an error.
- If the SCS security level is Level 1 or Level 2 when you start offline download, a message prompting to set Level 0 is notified and the download ends with an error. Set the SCS security level to "0" and start offline-downloading.
- If the I/O Lock window or Inter-SCS Communication Lock window is left open when you start offline download, an error message appears and the download processing ends.

3. A dialog box asking you if you are sure to start an offline download appears. Click [OK]. A dialog box for setting a password for changing the SCS security level appears. After that, a dialog box prompting you to manage versions of the SCS project appears. When an offline download completes, SCS is restarted. The SCS database offline downloaded to the SCS is automatically stored in SENG as a master database together with source files.
4. On the CENTUM Integration, download the database of the CENTUM project also.

Dealing with the offline download confirmation dialog box

The system checks to see if there is a possibility that the online change variables area in the database has been used before executing the offline download. If the online change variables area is used, a confirmation dialog box appears. This situation can be solved by performing a clean project and a build.
In the confirmation dialog box, select [Cancel] to terminate the offline download processing. Perform a clean project and a build, and then execute offline download. The offline download starts when you click [OK] in the confirmation dialog box.

Offline download process in I/O list engineering

When you execute an offline download of an SCS project that was created with I/O list engineering, the status of the safety I/O list, safety communication I/O list, and the IOM information are checked. More specifically, whether the safety I/O list, safety communication I/O list, and IOM information were edited after the builds by Generation Manager succeeded is checked. If it corresponds to the check items, an error occurs and the offline download stops.

If the safety I/O list, safety communication I/O list, and IOM information cannot be checked due to disrupted communication with the AD Server, a warning will appear but you will still be able to download the project. After the connection with the AD Server is restored, the system will check whether any offline download was run during the connection interruption if either of the following measures is taken:

- Use the System Structure Navigator in AD Organizer and execute the update function of the Revision History Utility.
- Use SCS Manager to open the SCS project.

If an offline download is performed during the connection interruption, a warning appears when the corresponding SCS project is opened in SCS Manager. This warning will disappear if the build and download are performed.

When the offline download succeeds, labels are set to the safety I/O list, safety communication I/O list, and IOM information. The label represents a character string as mentioned below.

```
SCS Project Name-Download-Date and Time
```

End the offline download

Set the passwords used when changing the SCS security level.

Manage the operation history by using the operation history management utility of AD Organizer. Check-in the SCS project with the Version Control Tool.

SEE ALSO For more information about the operation history management utility of AD Organizer, refer to:

C2.6, “Operations of the revision history function” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about the version control tool, refer to:

F5., “Version control” in Engineer's Reference Manual (IM 32P04B10-01EN)

Security of SCS

SCS security levels provide adequate security through specifying the passwords. Passwords for different security levels can be set for each SCS.

- Setting and changing passwords
- Changing SCS security levels

Note that it is necessary to return the SCS security level to Level 2 before closing an SCS project.

This section describes how to set passwords for changing SCS security levels and how to change the levels.

IMPORTANT

No password has been set after executing offline download and master database offline download. Make sure to set passwords again.

TIP The access to SCS is controlled by SCS itself according to its security level. Operations on the SENG is not be prohibited according to the SCS security level, however.

How to set and change passwords

The password that is used to change the SCS security level is stored within the SCS. This password can be set or changed from the Set SCS Security Level dialog box.

IMPORTANT

No password has been set after executing offline download and master database offline download. Make sure to set a password at this stage.

1. Select [Maintenance] from the [Tools] menu of SCS Manager.
   The Maintenance Launcher menu appears.
2. Select [Set SCS Security Level] from the Maintenance Launcher menu.
   The Set SCS Security Level dialog box appears.

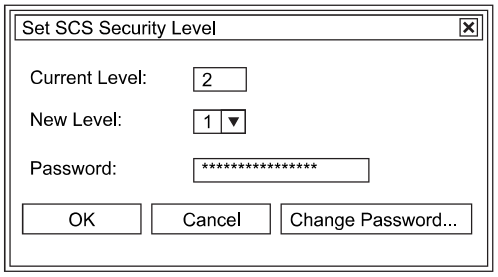


Figure C7-2 Set SCS Security Level dialog box

3. Click the [Change Password] button.
   The Change SCS Security Level Password dialog box appears.

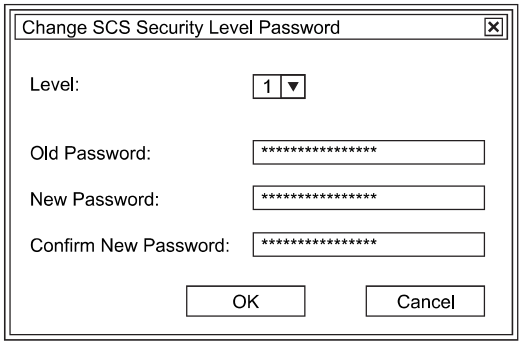


Figure C7-3 Change SCS Security Level Password dialog box

4. Select the security level for which you set a password in [Level:].
   It is necessary to set one password for changing to Level 1 and one for Level 0, respectively.
5. Enter the current password in the [Old Password:] field.
6. Enter a new password in the [New Password:] field, and once again in the [Confirm New Password:] field.
   The passwords you have entered appear as a series of asterisks (*).

   A password is a maximum 16 of single-byte alphanumeric characters and following symbols including a space character. The password is case-sensitive.

   ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~

   You do not need to enter [Old Password:] if you have not set any password before, or if you have just executed an offline download or a master database offline download.
7. Click the [OK] button.
   The confirmation dialog box appears.

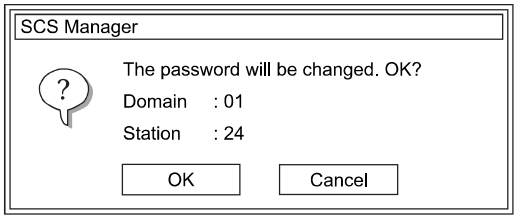


Figure C7-4 Confirmation dialog box

8. Click the [OK] button.
   Both new and old passwords will be sent to SCS. If the password is successfully changed, the dialog box notifying the success appears. The new password becomes valid. If the password change fails, a dialog box will be displayed to notify the failure.

How to change SCS security levels

The SCS security level can be changed in the Set SCS Security Level dialog box of SCS Manager.
The table below shows the combinations of levels for which security level changes are allowed via operations on the Set SCS Security Level dialog box.

Table C7-1 Security levels that can be changed through operations in the Set SCS Security Level dialog box

Current SCS security level	New SCS security level (*1)		
	Level 2	Level 1	Level 0
Level 2	-	Yes (*2)	Yes (*2)
Level 1	Yes (*2)	-	Yes (*2)
Level 0	Yes(*3)	No	-

*1: Yes: The security level can be changed.
No: The security level cannot be changed.
*2: The security level can be changed to the target SCS security level.
*3: Security level changes can be made only in SCS simulator.

To change the security level, you need to enter the password. However, you don't need to enter a password when changing the security level from Level 1 to Level 2.

You cannot raise the security level from Level 0 to Level 2 from the Set SCS Security Level dialog box. In SCS Simulator of SCS Test Functions, however, you can raise from Level 0 to Level 2 on the Set SCS Security Level dialog box. This operation does not require a password.

CAUTION

To set the SCS security level back to Level 2 after changing to Level 0, you must restart the SCS, execute offline download, or execute master database offline download. In particular, be sure to execute offline download if you used break points in debugging of the application logic.

These operations require stopping of the system. When you change the security level to Level 0, do so very carefully considering the consequences of the system stop.

The SCS security level can be changed in the following procedure.

1. In SCS Manager, open an SCS project whose security level you want to change.
2. Select [Maintenance] from the [Tools] menu of SCS Manager.
   The Maintenance Launcher menu appears.
3. Select [Set SCS Security Level] from the Maintenance Launcher menu.
   The Set SCS Security Level dialog box appears. The current security level is displayed in [Current Level:]; this item is display only and cannot be changed.

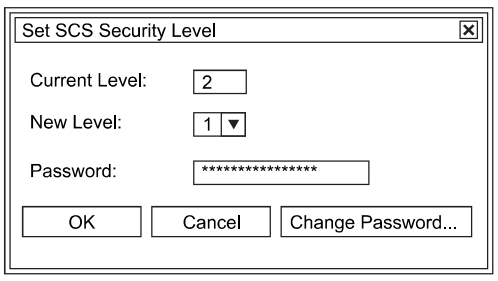


Figure C7-5 Set SCS Security Level dialog box

4. Select the security level you want in [New Level:] and enter the password for the level you want in [Password:] text box.
   All characters you enter are displayed as asterisks (*).

5. Click the [OK] button.
   The confirmation dialog box appears.

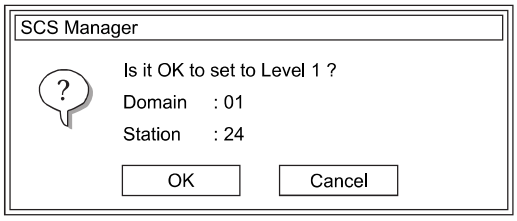


Figure C7-6 Confirmation dialog box (when changing to Level 1 or Level 2)

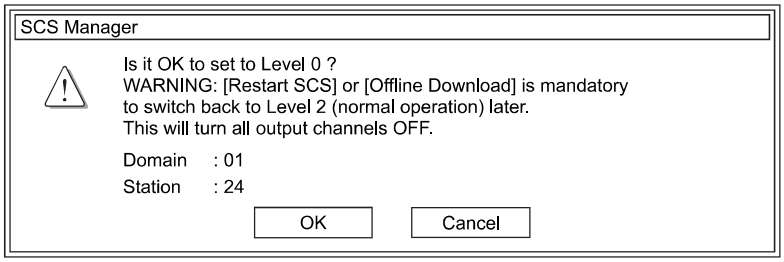


Figure C7-7 Confirmation dialog box (when changing to Level 0)

6. Click the [OK] button.
   When changing the security level to Level 0, the following dialog box appears to confirm the change again. When you set the level back to Level 2 from Level 0, the system stops. Confirm that this does not cause any problems. To proceed with the change, click [OK].

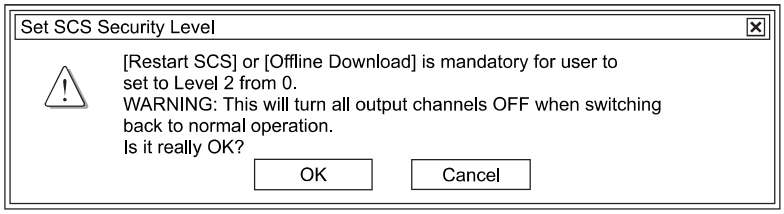


Figure C7-8 Dialog box confirming change to Level 0

If the security level of SCS is changed, the message showing the result of change is displayed.

The error message is displayed if the security level could not be changed.

Confirming the SCS security level reset by SCS Manager

If the security level of SCS project currently opened in SCS Manager is not Level 2, the confirmation dialog box prompting to reset the security level to Level 2 appears when closing it.

IMPORTANT

This dialog box is for confirmation only. Open the corresponding SCS project again and change the security level using the Set SCS Security Level dialog box.

The confirmation dialog box appears in the following timings.

- When closing an SCS project by exiting SCS Manager

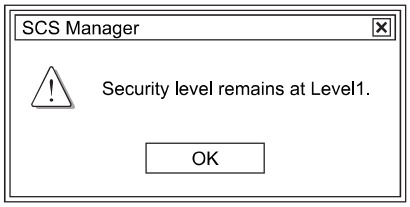


Figure C7-9 Example of Confirmation dialog box (when closing by exiting SCS Manager)

Clicking the [OK] button to exit SCS Manager leaves the security level unchanged.

- When closing an SCS project by opening another SCS project

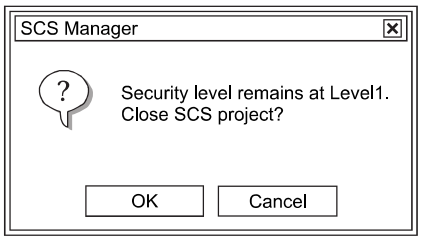


Figure C7-10 Example of Confirmation dialog box (when closing by opening another SCS project)

Click the [OK] button to close the currently opened SCS project without changing its security level, and then open another SCS project.

Click the [Cancel] button to keep the currently opened SCS project opened, and another SCS project will not open.

C8. Output enable operation

How to enable the outputs, the detailed procedure and how to start the output module will be explained in this section.

TIP

In this document, I/O shutoff switch and DO shutoff switch of the universal type I/O module are referred to as an output shutoff switch.

Overview on Output enable operation

When the operating mode of SCS is Waiting mode, some output channels are in Output Disable status, so that they cannot output the application logic results. Moreover, after SCS is started, the inter-SCS safety communication cannot send data to consumer side, the SCS Link Transmission and the subsystem communication cannot function either.

The Output Enable Operation will enable the output channels to output the application logic results, will start the inter-SCS safety communication, the SCS link transmission and the subsystem communications.

Output Enable operation can be performed for the whole SCS only. The output channel cannot be specified individually. Therefore, you cannot enable only one of the inter-SCS safety communication, SCS Link Transmission or subsystem communication.

Enabling output

Click the [Output enabled] button in the I/O Channel Status dialog box; the processing result of the application logic is output to the field and the SCS operating mode changes to the Running mode. Note that all nodes, all output modules and all channels must be in normal status in order for the SCS to be changed to the Running mode. If there is any error, the status does not change even if you perform the Output Enable Operation.

SEE ALSO

For more information about I/O Channel Status dialog box, refer to:

H4., “Displaying I/O channel status” on page H4-1

Start output module operation

If an error serious enough to activate the Output Shutoff switch occurs, there is a case where the output module stops its output and waits for the Output Module Start depending on an error cause. Perform the Start Output Module operation to start the output modules whose output is stopped.

The Start Output Module operation is performed individually. It can be performed regardless of the SCS security level.

The SCS continues to be in the Waiting mode even after the Start Output Module operation is completed. The channel in the Output Disable status will not change to Output Enable, either. Perform the Output Enable operation to change channels in the output disabled state to the output enabled state.

Note that this Start Output Module operation does not influence the output modules of which the Output Shutoff switch has not been actuated.

1. Select the output module whose output is stopped in Hardware Configuration Tree View of the SCS State Management window. Click [Start output module] button on the toolbar. After this is confirmed using the Confirmation dialog box, the selected output module starts up. The output from all channels will continue to be "0" even after the output module starts up.
2. Perform the output enable operation.

The output module is connected to the output of application logic and the result of the application logic is output from the module.

Enable Output operation

- Each output channel of SCS has two statuses, Enabled Output and Output Disabled, when the output is disabled, the output from application logic is not connected to the actual output channel, and OFF or pre-specified fail safe value is output to the field. Perform the Enable Output Operation to connect the output values from the application logic to the output channels. All normal outputs (DO module channels, AO module channels, Subsystem Communication output) are enabled by the output enable operation from an SENG.

  When SCS starts, all output channels are in the output disabled status.

- Transmission is started in the inter-SCS safety communication and subsystem communication output by the first output enable operation after SCS startup.

- When an output module fails, all output channels on the output module enter the output disabled status.
  When an output channel fails, the output channel enters the output disabled status.

- In the case of subsystem communication, it does not result in the output disabled status even if an error occurs in the subsystem communication (communication module error or communication error).

- The output enable operation can be performed from the application logic using a system function block. There are two types of function blocks that can perform the output enable operation: SYS_STAT, which enables safety outputs and outputs in inter-SCS safety communication, and SYS_STAT_SC, which enables subsystem communication outputs. Use these system function blocks and perform the output enable operation if it is desired to have different output start timings for output modules and the subsystem communication.

SEE ALSO For more information about specifications of SYS_STAT, refer to:

11.1, “SYS_STAT (SCS status management)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about specifications of SYS_STAT_SC, refer to:

12.13, “SYS_STAT_SC (subsystem communication output status indicator)” in POU Reference Manual (IM 32P03B20-01EN)

C9. Target tests

In a target test, the application logic is tested on the actual SCS. SCS Manager is used to perform test operations and display the statuses and the results. Testing by overriding from HIS is performed in an environment where ProSafe-RS is integrated with CENTUM. The target test function of CENTUM can be used as necessary. For the parts that were created by using iDefine, connect iDefine and SCS through the iDefine Test Manager in AD Organizer and run the test using the iDefine test function.

IMPORTANT

Target tests are mandatory for ProSafe-RS. The user must test the application in target tests at the final stage.

To use all the functions provided in the test function instead of simply monitoring, set the SCS security level to Level 0. The same applies when using the iDefine test function.

- Application logic can be debugged with the Application Debug Function, Forcing of I/O variable and Online Monitoring Function.
- Application can be executed without mounting I/O modules or wiring field devices when the Forcing Function for the I/O modules is used.
- Application logic can be debugged using the Forcing Function for I/O variables by changing conditions of the application logic.

By using the target hardware, perform tests on all signal paths and logics (FU/FB).

SEE ALSO

For more information about target test operations, refer to:

4., “Target tests” in Test Function Guide (IM 32P04B30-01EN)

For more information about the operations for using iDefine in target tests, refer to:

6.4, “Using iDefine in target tests” in Test Function Guide (IM 32P04B30-01EN)

D. Procedures to create applications using the I/O list engineering method

This part gives an overview of the procedures of AD Organizer when using I/O list engineering and the procedures when using iDefine.

The safety I/O list and safety communication I/O list are used in the engineering process. Acquire the safety I/O list and safety communication I/O list from the customer or create a new one.

The user can use the safety I/O list to make definitions based on the P&ID tag name in the application, and proceed to build the application without having to wait for the detailed design of the I/O module or the data communication. By using a safety communication I/O list, you can define communication modules and proceed with building the application.

In the Safety I/O Editor, you can import and edit the safety I/O list that you have prepared in advance or create a new safety I/O list.

In the Safety Communication I/O Editor, you can import and edit the safety communication I/O list that you have prepared in advance or create a new safety communication I/O list.

In the IOM Definition Editor, you can assign SCS nodes and input/output modules.

The changes made in AD Organizer editors can be reflected in SCS projects by using Generation Manager.

With I/O list engineering, you can also use iDefine to create application logics.

Create an application logic by using iDefine based on the IOM information that was defined in AD Organizer and reflect the application logic in SCS by using AD Organizer.

SEE ALSO For more information about Generation Manager, refer to:

D4., “Overview of RS generation” on page D4-1

D1. Engineering based on the safety I/O list

In I/O list engineering, you can create and edit safety I/O lists by using AD Organizer.

The engineering data is reflected in the SCS project by using the RS Generation Manager of AD Organizer.

D1.1 Overview of I/O list engineering

You can create a safety I/O list based on the I/O information list, containing information about AIO, DIO, and so on, that is obtained from the plant designer.

A safety I/O list is created by defining safety I/O in the Safety I/O Editor and then importing the I/O information list. In the Safety I/O Editor, one row is displayed for each I/O point, showing the information that identifies whether it is input or output.

Follow these steps to create a safety I/O list:

1. Start up the Safety I/O Editor.
2. Import the I/O information list to the safety I/O list.
   When imported, the setting items in the I/O information list, which is provided in Microsoft Excel.xlsx format, are mapped to the setting items of the safety I/O list. You can save and reuse the mapping information.
3. Define I/O module assignments.
   By using the grid rule function, you can perform a bulk edit and detailed check of the I/O module assignment information.

   For use in the grid rule function, setting items that users can freely define as reference information are provided. These setting items are called User Define.
4. Compare the I/O information lists before and after the import and reflect the differences to the existing data.

TIP

You can export the safety I/O list file. The exported file is in the Microsoft Excel.xlsx format.

5. Check the I/O module assignment results.
   The following information appears:
   - IOM configuration
   - Details of safety I/O connection for each IOM
6. Save and check in the safety I/O list.
7. When engineering by using iDefine, export the safety I/O list and IOM definition data for iDefine.

SEE ALSO

For more information about the procedures to export files for iDefine from AD Organizer, refer to:

D5.2.1, “Exporting the ProSafe-RS I/O file from AD Organizer” on page D5-9

D1.2 Creating a new safety I/O list

Follow these steps to create a new safety I/O list:

1. Select the I/O-List folder of the System Structure Navigator.
2. From the context menu, select [New Safety I/O List].
   The newly created safety I/O list is displayed in the System Structure Navigator in edit mode.
3. Enter unique safety I/O list name.
   The safety I/O list name that is entered is referred to as the P&ID group.

   A new safety I/O list is created. Once it is newly created, it is automatically checked in to the server.

Folder location of the safety I/O list definition

When RS project, SCS project, node, slot, and terminal numbers have not yet been defined, safety I/O lists are defined as the files under the I/O-List folder. Once these are defined, the safety I/O lists are copied to the I/O_definition folder under the N-IO folder or FIO folder of each SCS.

After the definition of the safety I/O list has been copied, you can select the safety I/O list from under the FIO or N-IO folder of SCS and start Safety I/O Editor from the context menu. Only the contents that are defined in the corresponding file are shown in each editor.

D1.3 Operating a safety I/O list

This section describes how to rename and delete a safety I/O list.

Changing the name of the safety I/O list

Follow these steps to change the name of the safety I/O list:

1. Right-click on the safety I/O list in the System Structure Navigator and select [Rename]. The P&ID group of the safety I/O list name appears in the edit status.
2. Enter a new P&ID group. The name of the safety I/O list changes.

Deleting the safety I/O list

You need to delete the safety I/O list after deleting all I/O information that is assigned to the I/O module. Follow these steps to delete the safety I/O list:

- Select the safety I/O list to delete using System Structure Navigator and click [Delete] on the tool bar of AD Organizer.

TIP

- When the Safety I/O Editor is started, the safety I/O list cannot be deleted.
- You can delete only one safety I/O list at a time.

D1.4 Defining I/O information by using Safety I/O Editor

This section describes how to use Safety I/O Editor to edit a safety I/O list.

D1.4.1 Starting the Safety I/O Editor

You can start the Safety I/O Editor from the System Structure Navigator in AD Organizer. The modes of the Safety I/O Editor are edit mode, revision history mode and read-only mode.

You can open two windows simultaneously with the following combination:

- Edit mode and read-only mode
- Revision history mode and read-only mode

You cannot open two windows with the combination of edit mode and revision history mode.

Starting the Safety I/O Editor for editing

Depending on the operation purpose, the startup method of the Safety I/O Editor varies.

IMPORTANT

To edit I/O information for each SCS, you can start the Safety I/O Editor after setting the station configuration and defining the I/O module assignment information in the safety I/O list.

- Perform one of the following operations using the System Structure Navigator to start the Safety I/O Editor:
  - When editing I/O information for each P&ID group
    Select and double-click the safety I/O list in the [I/O-List] folder.
  - When editing I/O information for each applicable RS project
    Right-click the RS project and select [Open] > [Safety I/O Editor].
  - When editing I/O information for each applicable SCS
    Right-click the target SCS and select [Safety I/O Editor].
  - When editing I/O information for each applicable module
    Double click the [I/O definition] under the applicable module folder.

  The Safety I/O Editor appears in the document window area.

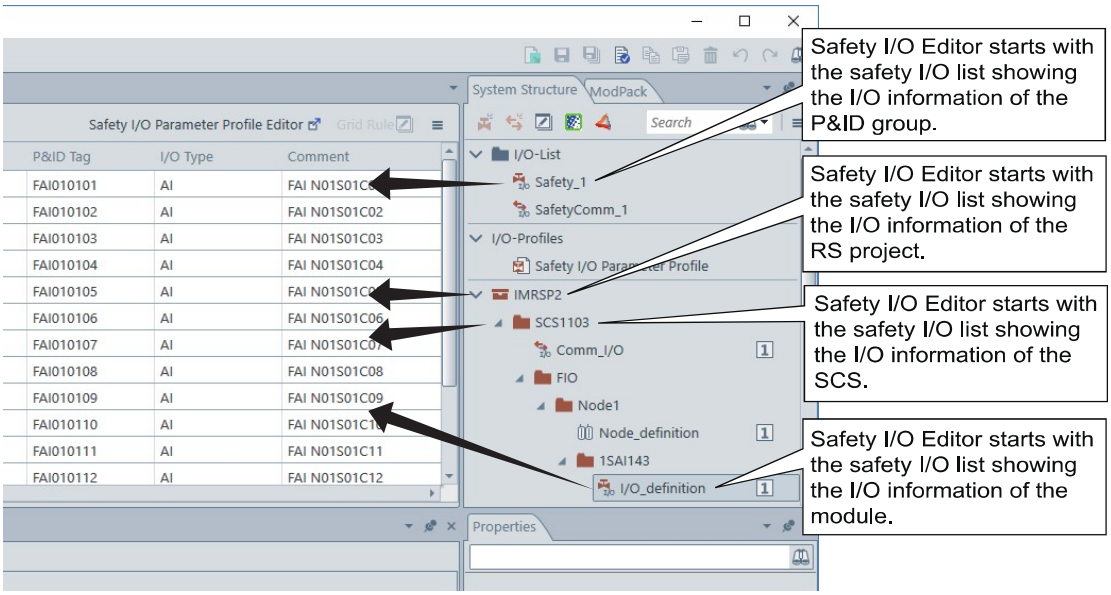


Figure D1.4.1-1 Safety I/O Editor

TIP

When the Safety I/O Editor is started, the source for which you have started the editor appears in the window title.

Starting the Safety I/O Editor for read-only

Depending on the operation purpose, the startup method of the Safety I/O Editor varies.

- Perform one of the following operations using the System Structure Navigator to start the Safety I/O Editor in read-only mode:
  - When reading definitions for each P&ID group
    Right-click the safety I/O list in the [I/O-List] folder and select [Open (Read-Only)].
  - When reading definitions for each applicable RS project
    Right-click the RS project and select [Open (Read-Only)] > [Safety I/O Editor].
  - When reading definitions for each applicable SCS
    Right-click the target SCS and select [Safety I/O Editor (Read-Only)].
  - When reading definitions for each applicable module
    Right-click the [I/O definition] under the applicable module folder and select [Open (Read-Only)].

  The Safety I/O Editor appears in the document window area in read-only mode.

TIP

If content is being edited in the edit mode editor, the contents being edited are also reflected in the read-only mode editor. However, the update is manual.

Switching the display of the safety I/O list

You can switch the display of the safety I/O list for each I/O type. You need to perform one of the following operations to switch the display.

- To display all I/O and setting items
  From the drop-down list on the left side of the toolbar in the Safety I/O Editor, select [All].
- To display only analog I/O and related setting items
  From the drop-down list on the left side of the toolbar in the Safety I/O Editor, select [AIO].
- To display only discrete I/O and related setting items
  From the drop-down list on the left side of the toolbar in the Safety I/O Editor, select [DIO].

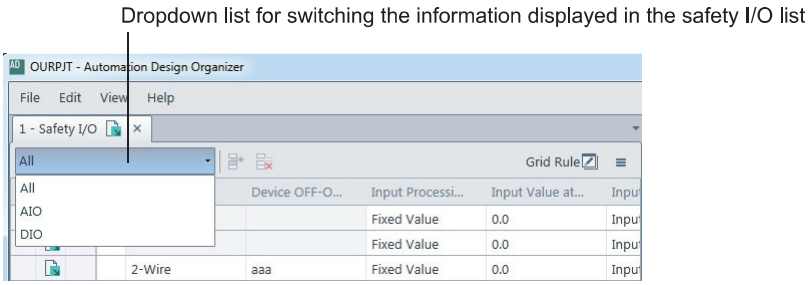


Figure D1.4.1-2 Switching the display of the safety I/O list

Setting items of the Safety I/O Editor

The following table shows the setting items of the Safety I/O Editor.

Table D1.4.1-1 List of setting items of the Safety I/O Editor

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
For I/O list management	Area	Area name	-	-
	P&ID Sheet	P&ID sheet name	-	-
I/O list common	P&ID Tag	P&ID tag name Key information required to identify each I/O The P&ID tag must be unique within the P&ID group.	1	I/O Parameter Builder P&ID tag name (*2)
	I/O Type	I/O type. Select from the following AI, AO, DI, DO	1	-
	Comment	Variable comment of the IO variable that is defined in Dictionary	-	Variable in Dictionary Variable comment
	Range LO	Scale low limit	-	-
	Range HI	Scale high limit	-	-
	Eng Unit	Engineering unit	-	-
	I/O Tag	IO Variable Name Normally, set the same name as the P&ID tag, or an abbreviated name. Defined in Dictionary View and assigned to each channel on the I/O Wiring View The I/O tag must be unique within the SCS.	1	Variable in Dictionary Variable name I/O Wiring View
	Variable Group	Variable Group	-	Dictionary View

Continues on the next page

Table D1.4.1-1 List of setting items of the Safety I/O Editor (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
IOM assignment information	RS Project	The RS project name to which this I/O is assigned	2	I/O Wiring View
	SCS	The SCS number to which this I/O is assigned	2	I/O Wiring View
	Node Type	The node type to which this I/O is assigned Select either of the following • ESB Bus/Optical ESB Bus • NESB Bus	2	I/O Wiring View
	Node	Node number to which this I/O is assigned	2	I/O Wiring View
	IOM Category	IOM category to which this I/O is assigned The selectable list can be determined according to the I/O type (Example: Analog Input/Output)	2	I/O Parameter Builder (Select N-I/O list base plate)
	IOM Type	IOM type to which this I/O is assigned The selectable list can be determined according to the I/O category (Example: SAI143 (4 to 20 mA, 16-channel, module isolation))	2	I/O Wiring View
	Unit	Use only for N-IO Unit number to which this I/O is assigned	(*3)	I/O Wiring View
	Slot	Slot number to which this I/O is assigned	2	I/O Wiring View
	Terminal	Terminal number to which this I/O is assigned	2	I/O Wiring View
	Duplex	Duplex specification of the IOM to which this I/O is assigned	3	I/O Wiring View
	I/O Parameter Profile	Safety I/O parameter profile	-	-
	Signal Type	Signal type The selectable list can be determined according to the I/O type (Example: For I/O Type = AI, it is a list of 4-20 mA, 1-5V, 1-10V, … etc.) The Signal Type-IS is not used normally. Use it only for N-IO barrier supported base plate, and specify the signal between field and barrier in Signal Type, and the signal between barrier and IOM in Signal Type-IS.	1	I/O Type + Signal Type(*) of AD Organizer is reflected in Signal Type + Signal Conversion of I/O Parameter Builder (*): For the N-IO barrier supported base plate, Signal Type-IS
	Signal Type-IS			

Continues on the next page

Table D1.4.1-1 List of setting items of the Safety I/O Editor (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
I/O description (IOM Builder description)	Signal Conversion	Signal Conversion Type	3	Relevant setting items of I/O Parameter Builder
	Signal LO	Low limit of the field I/O signal	1	Relevant setting items of I/O Parameter Builder
	Signal HI	High limit of the field I/O signal	1	Relevant setting items of I/O Parameter Builder
	Signal Unit	Engineering unit of the field I/O signal	1	Relevant setting items of I/O Parameter Builder
	Wire type	Wire type	3	Relevant setting items of I/O Parameter Builder
	Device OFF-ON Variable Name	Device OFF-ON Variable Name Variable names for instructing a reset of fire and gas equipment	3	Relevant setting items of I/O Parameter Builder
	Reset Group ID	Reset Group ID Collection of fire and gas equipment subject to being reset simultaneously with a single reset operation	3	Relevant setting items of I/O Parameter Builder
	Input Processing at Fault	Input processing at fault	3	Relevant setting items of I/O Parameter Builder
	Input Value at Fault %	Input value at fault	3	Relevant setting items of I/O Parameter Builder
	Input Processing at Transmitter Fault	Specify input at transmitter fault	3	Relevant setting items of I/O Parameter Builder
	Detect IOP (High)	Detect IOP (High)	3	Relevant setting items of I/O Parameter Builder
	Detect IOP (Low)	Detect IOP (Low)	3	Relevant setting items of I/O Parameter Builder
	IOP High Limit	Threshold of IOP (High) %	3	Relevant setting items of I/O Parameter Builder
	IOP Low Limit	Threshold of IOP (Low) %	3	Relevant setting items of I/O Parameter Builder
	Detect Transmitter Fault (High)	Detect Transmitter Fault (High)	3	Relevant setting items of I/O Parameter Builder
	Detect Transmitter Fault (Low)	Detect Transmitter Fault (Low)	3	Relevant setting items of I/O Parameter Builder

Continues on the next page

Table D1.4.1-1 List of setting items of the Safety I/O Editor (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
I/O Description (IOM Builder description)	Threshold of Transmitter Fault (High) %	Threshold of Transmitter Fault (High) %	3	Relevant setting items of I/O Parameter Builder
	Threshold of Transmitter Fault (Low) %	Threshold of Transmitter Fault (Low) %	3	Relevant setting items of I/O Parameter Builder
	Field Power Diagnosis	Field Power Diagnosis	3	Relevant setting items of I/O Parameter Builder
	Reference junction compensation	Reference junction compensation	3	Relevant setting items of I/O Parameter Builder
	Burnout	Specify burnout	3	Relevant setting items of I/O Parameter Builder
	Time to Chattering Recovery Notice (s)	Time to Chattering Recovery Notice Monitoring time from when chattering ends to normal recovery	3	Relevant setting items of I/O Parameter Builder
	I/O Shutoff Switch	Shutoff Switch for AI/AO/DI(NIO)	3	Relevant setting items of I/O Parameter Builder
	Output Shutoff Switch	Specify output shutoff switch of FIO Specify DO shutoff switch of N-IO	3	Relevant setting items of I/O Parameter Builder
	Output Processing at Fault	Specify Output Processing at Fault	3	Relevant setting items of I/O Parameter Builder (*4)
	Output Value at Fault %	Output Value at Fault	3	Relevant setting items of I/O Parameter Builder
	Tight-shut/Full-open	Specify Tight-shut/Full-open	3	Relevant setting items of I/O Parameter Builder
	Tight-shut Value %	Tight-shut Value	3	Relevant setting items of I/O Parameter Builder
	Full-open Value %	Full-open Value	3	Relevant setting items of I/O Parameter Builder
	Detect Short Circuit	Detect Short Circuit	3	Relevant setting items of I/O Parameter Builder

Continues on the next page

Table D1.4.1-1 List of setting items of the Safety I/O Editor (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
I/O description (IOM Builder description)	Detect Disconnection	Detect Disconnection	3	Relevant setting items of I/O Parameter Builder
	Detect LFD	Detect LFD	3	Relevant setting items of I/O Parameter Builder
	Pulse Test	Pulse Test	3	Relevant setting items of I/O Parameter Builder
	Pulse Test (OFF)	Pulse Test (OFF)	3	Relevant setting items of I/O Parameter Builder
	Pulse Test (ON)	Pulse Test (ON)	3	Relevant setting items of I/O Parameter Builder
	Low Voltage Pulse Test (ON)	Low Voltage Pulse Test (ON)	3	Relevant setting items of I/O Parameter Builder
	SOER (Setting for SOER)	SOER Setting	3	Relevant setting items of I/O Parameter Builder
	Trip Signal (Setting for SOER)	Specify Trip Signal	3	Relevant setting items of I/O Parameter Builder
	Command	Command Line	3	Relevant setting items of I/O Parameter Builder
Connection Device Info	Device Com Type	Device Communication Protocol (Enter HART/Conventional, etc.)	-	-
	Device Tag	Device Tag	-	-
	Device Tag Comment	Device Tag Comment	-	-
	Device ID	Device Serial Number	-	-
	Device Address	Device Address	-	-
	Device Manufacturer ID	Device Manufacturer ID	-	-
	Device Type ID	Device Type ID	-	-
	Device Revision	Device Revision Number	-	-
	Device Route Info 1	Device Communication Topology Information	-	-
	Device Route Info 2	Device Communication Topology Information (when IOM is redundant)	-	-
	Device Installed Location	Device Installed Location	-	-
	Device Parameter	Device Parameter	-	-

Continues on the next page

Table D1.4.1-1 List of setting items of the Safety I/O Editor (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
For I/O list management	Component ID	Component ID	-	-
	Intrinsic Safe	Intrinsic Safe	-	-
	External Power to transmitter	External Power to transmitter	-	-
	Instrument Type	Instrument Type	-	-
	Instrument Type Description	Instrument Type Description	-	-
	Loop Name	Loop Name	-	-
	Panel Name	Panel Name	-	-
	Junction Box Name	Junction Box Name	-	-
FieldMate Validator	FieldMate Validation Status	FieldMate Validation Status	-	-
	Validation Status Update Time	Validation Status Update Time	-	-
	Left IOM Validation Status	Left IOM Validation Status	-	-
	Right IOM Validation Status	Right IOM Validation Status	-	-
	Field Device Validation Status	Field device Validation Status	-	-
	Channel Configuration Updated Time	Channel Configuration Updated Time	-	-
	Overwrite Status	Update Status by Using Editor	-	-
I/O Setting Protection	Protect	Protection that prevents the I/O settings from being changed	-	-

Continues on the next page

Table D1.4.1-1 List of setting items of the Safety I/O Editor (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
For iDefine reference	Typical	Typical name or Typical ID	-	-
	HH Setpoint	HH trip set point of I/O	-	-
	H Setpoint	High trip set point of I/O	-	-
	L Setpoint	Low trip set point of I/O	-	-
	LL Setpoint	LL trip set point of I/O	-	-
	Hysteresis	Hysteresis value	-	-
	MOS Group	Value of the GRP argument of GOV_B/GOV_IB FB	-	-
	FUP Group	Value of the GR argument of ANN_FUP/FUP_RST FB	-	-
	SOE ID	String constant for SOE	-	-
	Fault 1	Medium value for Fault1 (mA). For F1H/F1L of GASDTR FB.	-	-
	Fault 2	Medium value for Fault2 (mA). For F2H/F2L of GASDTR FB.	-	-
	Fault 3	Medium value for Fault3 (mA). For F3H/F3L of GASDTR FB.	-	-
	Fault 1 ID	Detailed description of Fault1. For IDF1 of GASDTR FB.	-	-
	Fault 2 ID	Detailed description of Fault2. For IDF2 of GASDTR FB.	-	-
	Fault 3 ID	Detailed description of Fault3. For IDF3 of GASDTR FB.	-	-
	Tag High Limit	Scale high limit (for CENTUM integration)	-	-
	Tag Low Limit	Scale low limit (for CENTUM integration)	-	-
	Tag Security Level	Security level (for CENTUM integration)	-	-
	Switch Position Label	Switch position label (for CENTUM integration)	-	-
	Tag Mark	Tag mark (for CENTUM integration)	-	-
	Alarm Level	Alarm level (for CENTUM integration)	-	-
	Upper Window	Upper window (for CENTUM integration)	-	-
	Upper Equipment Name	Upper equipment name (for CENTUM integration)	-	-
User Define Column	UDC1 to UDC40	User-defined column	-	-

Continues on the next page

Table D1.4.1-1 List of setting items of the Safety I/O Editor (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
For I/O list management	P&ID Group	P&ID Group Name Specify a unique range for the P&ID tag. The name that is set at the time of creating the I/O list in System Structure Navigator is automatically reflected.	1	-

*1: Whether column settings are required or not are indicated in the following categories:
- 1: Always set
- 2: Set after assigning the I/O to SCS and IOM
- 3: Configuration is required after assigning the I/O to SCS and IOM
- -: Setting not required

*2: For FIO, up to 16 single-byte characters. For N-IO, up to 32 single-byte characters. Characters that exceed the limit are truncated during the reflection process.

*3: For N-IO, 2
For other than N-IO, -

*4: For DO module of FIO, it is reflected to Output Value in Detecting Error.

D1.4.2 Importing the I/O information list

You need to prepare the I/O information in Microsoft Excel xlsx format. Follow these steps to import the I/O information:

1. Select the Sub menu button from the Safety I/O Editor, and select Import.
   The Import wizard appears.
2. In the File box, specify the Microsoft Excel file in xlsx format of the I/O information to be imported.
   Sheet Name shows the sheet name of the I/O information list, Header Row Position shows the first row number, and Target P&ID Group shows the P&ID group that is included in the I/O information list.

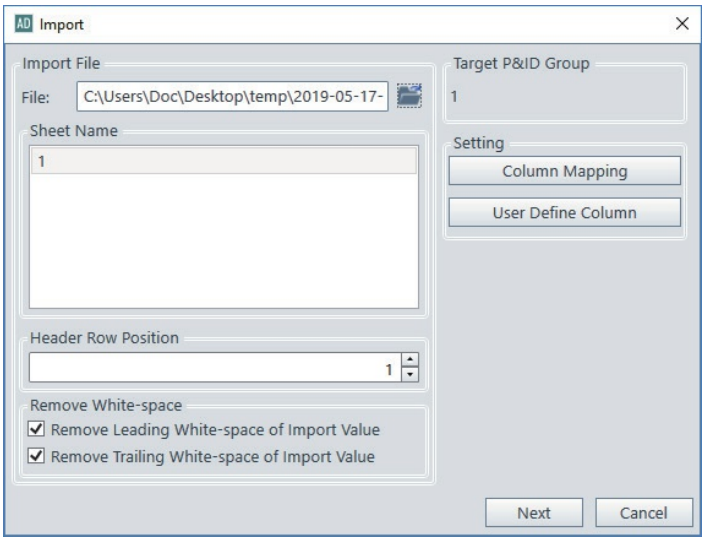


Figure D1.4.2-1 Import wizard

3. Select the sheet to be imported in Sheet Name.
4. Enter the row number in which the setting item name is entered in Header Row Position.
5. Set the following details in Settings if necessary.
   More specific instructions are given later.
   - If the setting item of the I/O information list to be imported does not match the setting item of the safety I/O list, click the [Column Mapping] button to map the setting items.
   - If the setting item of the I/O information list to be imported cannot be mapped to the setting item of the safety I/O list, click the [User Define Column] button, and after adding the new setting item to the safety I/O list, perform the mapping to these new items.
6. Select the [Remove Leading White-space of Import Value] check box or the [Remove Trailing White-space of Import Value] check box optionally.
7. Click [Next].
   The screen will switch to the Comparison and Setting screen.
8. Select either [All Check (Add/Update/Delete)] or [Part Check (Add/Update)].
   All the rows in the list of I/O information are imported.

   If you have selected [All Check (Add/Update/Delete)], the rows that are not available in the I/O information list are deleted from the safety I/O list.

   If you have selected [Part Check (Add/Delete)], the rows that are not available in the I/O information list are not deleted from the safety I/O list.
9. Click [Finish].
   The I/O information list is imported, and the safety I/O list is checked out.

Mapping the setting items of the I/O information list to the setting items of the safety I/O list

The operations for mapping are the same with safety communication I/O lists. When mapping setting items of a safety communication I/O list, replace safety I/O list with safety communication I/O list.

To import the I/O information list, not all of the setting item names may necessarily match. Thus, it is necessary to map the setting items of the I/O information list so that they match the setting items of the safety I/O list. Follow these steps to perform mapping:

1. In the Import wizard, click [Column Mapping].
   The Column Mapping dialog box appears. The setting items that do not match the setting items of the safety I/O list are displayed in [Unmapped], while the setting items that match are displayed in [Mapped]. [Client] shows the setting items of the I/O information list, while [AD Suite] shows the setting items of the safety I/O list.

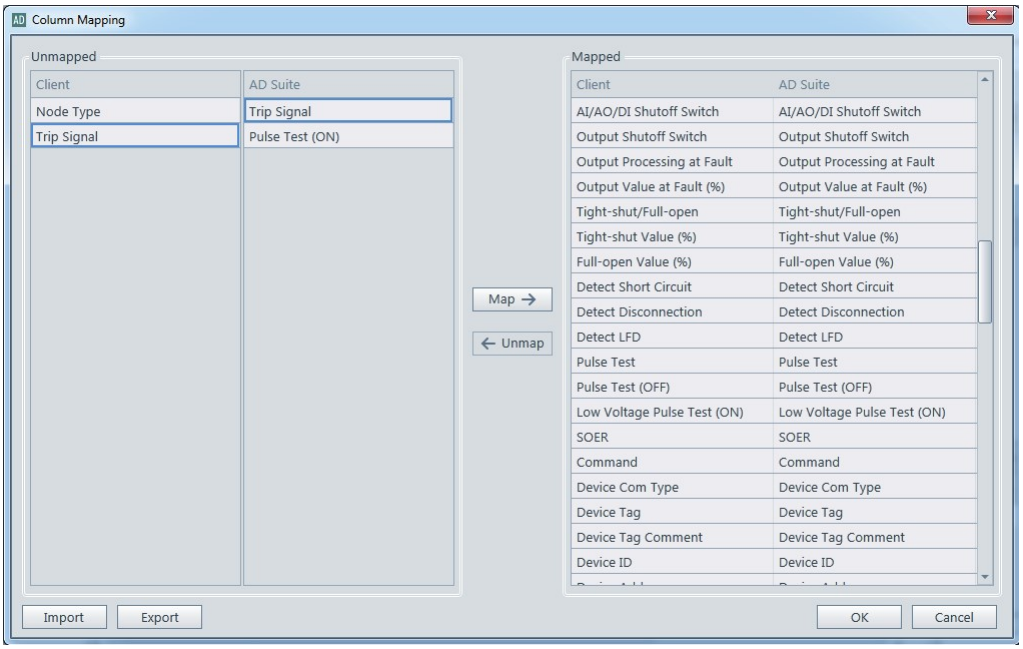


Figure D1.4.2-2 Column Mapping dialog box

2. In [Unmapped], select the setting items of the I/O information list and the setting items of the safety I/O list that are to be mapped.
3. Click the [Map] button.
   The setting items of the I/O information list and the setting items of the safety I/O list are mapped and displayed in [Mapped].
4. Click the [OK] button.
   The mapping information is created.
5. Click the [Next] button in the Import wizard.
   The I/O information list is imported based on the mapping information.

TIP

You can export the mapping information to a Microsoft Excel xlsx format file. You can also import the exported file and map the setting items based on this information.

Modifying the mapping information in AD Organizer that has been upgraded to version R4.05 or later

To import the I/O information list that was created using a version earlier than R4.05 to the safety I/O list and safety communication I/O list, modify the column mapping information of user-defined columns as necessary.

For example, if you have created Typical as an alias name in a user-defined column, open the Column Mapping dialog box when importing and follow these steps to modify the settings so that the data is imported to the standard column (Typical):

1. In the Mapped area, select the row that includes the upgraded column name (_Typical).
2. Click [Unmap].
   The pair is moved to the Unmapped area.
3. In the Unmapped area, select the column name (Typical) in the Client section and the column name (Typical) that is newly added in R4.05 to the AD Suite section.
4. Click [Map].
   The pair is moved to the Mapped area.

Exporting mapping information

You can export the mapping information of the I/O information list and the safety I/O list to a Microsoft Excel xlsx format file in the Column Mapping dialog box. Follow these steps to export the mapping information:

1. In the Column Mapping dialog box, click [Export].
   The Select a location and set a file name dialog box appears.
2. Specify the export location and file name, and click the [OK] button.

Importing mapping information

You can import the exported mapping information. Follow these steps to import the mapping information:

1. In the Column Mapping dialog box, click [Import].
   The File Selection dialog box appears.
2. Specify the Microsoft Excel xlsx file of the mapping information to be imported, and click [OK].

D1.4.3 Comparing and reflecting the I/O information before and after import

Follow these steps to compare the I/O information before and after import and reflect it in the safety I/O list:

1. Select the [Mode] settings of the Comparison and Settings screen in the Import wizard from the following options.
   - To compare the added, modified, and deleted I/O information, select [All Check (Add/Update/Delete)].
   - To compare the added and modified I/O information, select [Part Check (Add/Update)].
2. Click [Finish].
   The Safety I/O Editor switches to Deviation mode.

   The imported I/O information is displayed on the left pane of the Safety I/O Editor, while the current safety I/O list is displayed on the right pane. In this case, the differences in the I/O information are displayed in blue color.

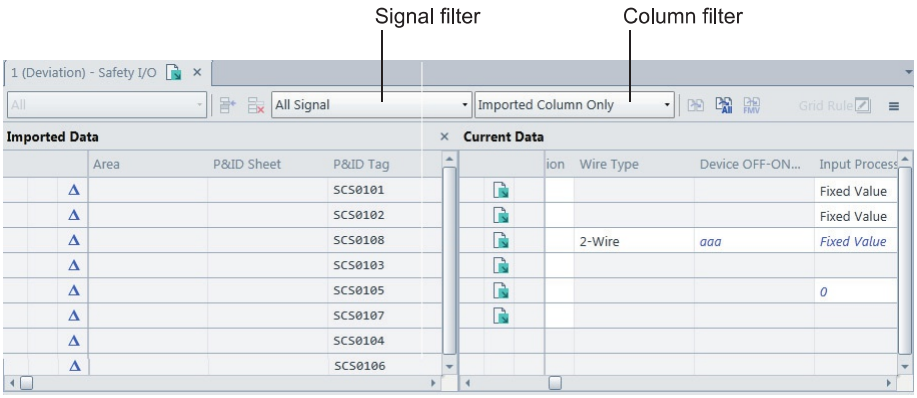


Figure D1.4.3-1 Safety I/O Editor for Deviation mode during import

TIP

- The I/O information before and after the import are compared using the P&ID tag as the key. If there is no relevant P&ID tag for the current safety I/O list, a new row is added to the safety I/O list.
- If a column value is not available in the imported file, the default value of that column is double-underlined to be displayed as the Imported Data. If the value of a column is not available in the imported file as well as in Current Data, the value is not imported.

3. You need to select the operation to reflect the imported I/O information list to the safety I/O list from the following.
   - To reflect only the selected I/O information, click the [Reflect Selected Area] button of the Safety I/O Editor tool bar in Deviation mode. The differences present in the selected range are reflected in the safety I/O list.
   - To reflect the entire I/O information, click the [Reflect All (regardless of selection)] button of the Safety I/O Editor tool bar in Deviation mode. All differences present are reflected in the safety I/O list.

TIP

If the safety I/O list is not checked out, it will be checked out.

Switching the safety I/O list display in Deviation mode

You can switch the Safety I/O Editor display in Deviation mode.

- Displaying for each edited content

The display of the safety I/O list in Deviation mode can be switched for each I/O point. You need to perform one of the following operations to switch the display.

- Displaying all I/O points
  Select [All Signal] in the signal folder of the Safety I/O Editor in Deviation mode.
- Displaying only the edited I/O points
  Select [Different Signal Only] in the signal folder of the Safety I/O Editor in Deviation mode.

- Displaying for each setting item
  The safety I/O list display can be switched in Deviation mode for each setting item. You need to perform one of the following operations to switch the display.
  - Displaying all setting items
    Select [All Column] in the column folder of the Safety I/O Editor tool bar in Deviation mode.
  - Displaying only the imported setting items
    Select [Imported Column Only] in the column folder of the Safety I/O Editor tool bar in Deviation mode.

D1.4.4 Editing a safety I/O list

You can use the following methods to edit a safety I/O list:

- Edit a new safety I/O list directly without importing an I/O information list
  With this method, you add a row of settings for each I/O point one by one.
- Import an I/O information list
  With this method, you import an I/O information list file and edit as required.

Creating a safety I/O list without importing an I/O information list

The user can directly edit the safety I/O list by using the Safety I/O Editor.

1. Open the System Structure Navigator.
2. Create a new safety I/O list.
3. Edit the safety I/O list.
   The data can be edited in two ways: you can edit each row manually, or edit the data in batch by using grid rules.

Editing a safety I/O list

Follow these steps to edit a safety I/O list:

You can add I/O points to the safety I/O list if you start the Safety I/O Editor for a P&ID group or a target module.

1. Double-click the cell of the safety I/O list.
   A dialog box appears, asking you to confirm the check-out.
2. Click [Yes].
   The I/O points are checked out, and check-out icons appear in the safety I/O list.
3. Edit the cells of the safety I/O list.

TIP

- When assigning the input points to the I/O module, define RS Project, SCS, Node Type, Node, IOM Category, IOM Type, Unit, Slot, Terminal, and Duplex. When these values are defined, the I/O points are copied to the I/O_definition file under the SCS folder. In this case, if the node, I/O module folder, and I/O_definition file do not exist, they are created automatically.
- If you set I/O points for which the I/O module assignment information is not defined, all I/O points for which the P&ID group is the same, and for which the I/O module assignment information is not defined are checked out. When I/O information is entered in the I/O points for which the I/O module assignment information is defined, all I/O points which are assigned to the same I/O module are checked out.

Adding I/O points to the safety I/O list

Follow these steps to add the I/O points to the safety I/O list:

1. Select I/O points from the safety I/O list. You can select I/O points in the following ways:
   - Select one or more rows
   - Select only one cell
2. Click the [Add Row] button on the tool bar.
   When one or more rows have been selected, the selected number of rows are added above the selected rows.

   When only one cell has been selected, one row is added below the last row. The added I/O points are checked out.

TIP

The I/O points can be added to the safety I/O list when the Safety I/O Editor is started up for each P&ID group or target module.

Deleting I/O points to the safety I/O list

Follow these steps to delete the I/O points to the safety I/O list:

1. Select the I/O points to be deleted in the safety I/O list.
2. Click the [Delete Row] button on the tool bar.
   The selected I/O points are deleted.

D1.4.5 Exporting the I/O information in the safety I/O list

The I/O information of the safety I/O list can be exported to a Microsoft Excel xlsx format file. Follow these steps to export the I/O information in the safety I/O list:

1. Select the [Sub menu] button from the Safety I/O Editor, and select [Export].
   The Export dialog box appears.

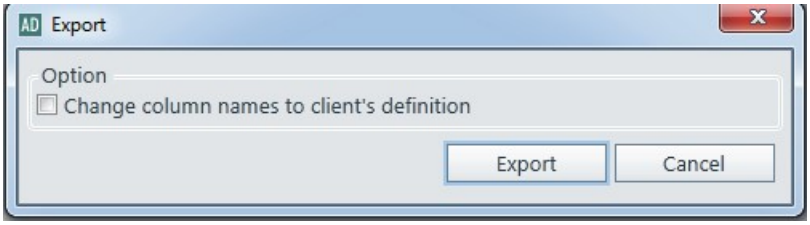


Figure D1.4.5-1 Export dialog box

TIP

When the [Change column names to client's definition] check box is selected, and [Export] is clicked, the setting item name of the safety I/O list is changed based on the mapping information that is set while importing the I/O information list.

2. Click [Export].
   The Select a location and set a file name dialog box appears.

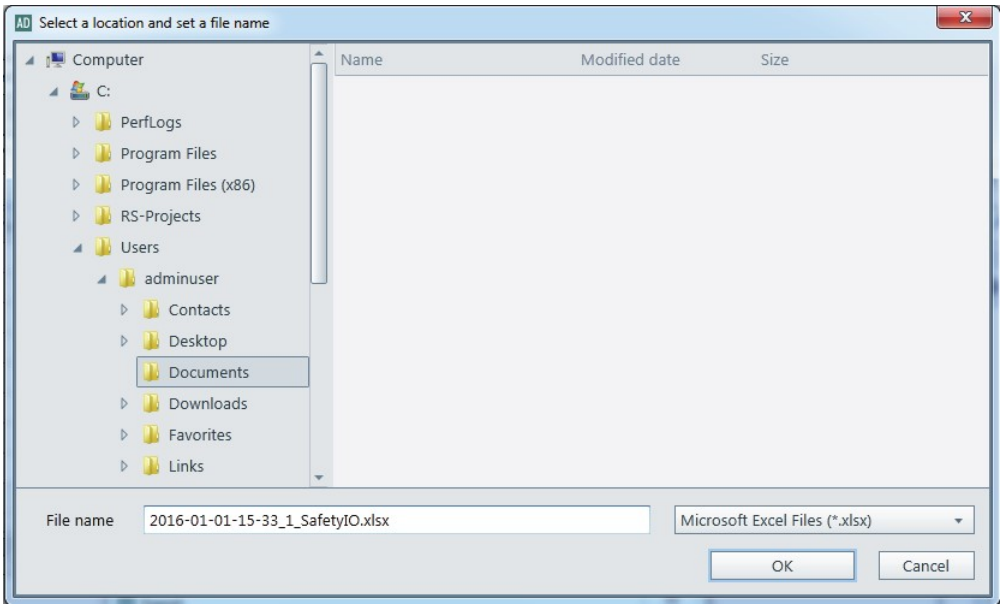


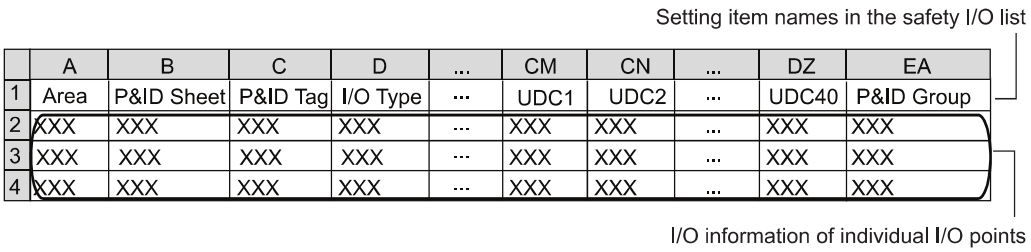
Figure D1.4.5-2 Select a location and set a file name dialog box

3. Specify the export location and file name, and click [OK].

Export file format

The exported file is created in the following format.

- File format
  Microsoft Excel .xlsx file
- Sheet name
  It will be the P&ID group name.
- Sheet description
  It is created in the following format.



	A	B	C	D	...	CM	CN	...	DZ	EA
1	Area	P&ID Sheet	P&ID Tag	I/O Type	···	UDC1	UDC2	···	UDC40	P&ID Group
2	XXX	XXX	XXX	XXX	···	XXX	XXX	...	XXX	XXX
3	XXX	XXX	XXX	XXX	···	XXX	XXX	...	XXX	XXX
4	XXX	XXX	XXX	XXX	···	XXX	XXX	...	XXX	XXX

Figure D1.4.5-3 Sheet description

TIP

If you assign an alias to a user-defined column, the Setting item name in the safety I/O list that corresponds to the user-defined column becomes an alias.

D1.4.6 Purpose of user definition and changing user-defined name

In addition to the default setting items, 40 setting items that users can define freely are provided in the safety I/O list. I/O information that is included in the user-defined setting items is reference information. This I/O information is not reflected to the SCS project. However, when engineering by using iDefine, the user-defined I/O information is included in the ProSafe-RS I/O file. As such, we recommend that you configure the ID and other information that you want to refer to when creating an application logic by using iDefine here. If you assign an alias to a user-defined column, the user-defined column header of the ProSafe-RS I/O file that is exported to iDefine becomes the defined alias.

You can use the user-defined setting items as reference information when using the grid rules.

Any name can be specified for the user-defined setting items. Follow these steps to specify any name for the user-defined setting items:

1. Select User Define Column Setting from the sub menu of the safety I/O list.
   The User Define Column Setting dialog box appears.

   The initial value of the setting item name is displayed in User Definition Column.

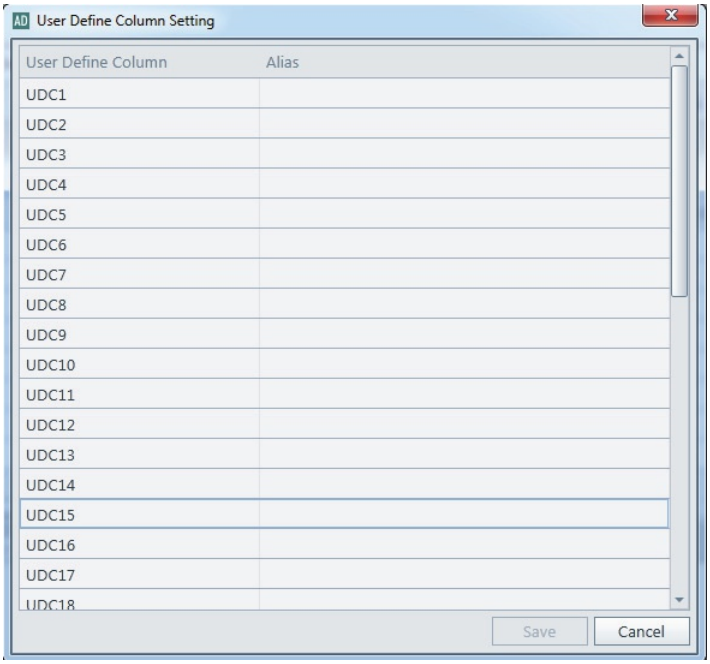


Figure D1.4.6-1 User Define Column Setting dialog box

2. Enter the name that needs to be changed in [Alias], and click [Save].
   The new name is displayed in the user-defined setting item of the safety I/O list.

D1.5 Using the safety I/O parameter profile

The safety I/O parameter profile is a named set of I/O channel parameter values. The I/O channel parameters can be configured all at once by applying the predefined safety I/O parameter profile to the I/O of the safety I/O list. Consistency can be ensured in I/O channel parameter settings for which the same profile has been applied by applying the safety I/O parameter profile to the I/O of multiple safety I/O lists. If you have changed the parameter values of a safety I/O parameter profile, you can reflect the modifications to the I/O of all safety I/O lists for which the profile has been applied.

Steps for using the safety I/O parameter profile

This section describes the following steps for using the safety I/O parameter profile:

- Starting Safety I/O Parameter Profile Editor
- Checking out the safety I/O parameter profile
- Defining the safety I/O parameter profile
- Deleting the safety I/O parameter profile
- Saving and checking in the safety I/O parameter profile
- Assigning the safety I/O parameter profile to the I/O parameter of the safety I/O list
- Reflecting the updated safety I/O parameter profile to the I/O of the safety I/O list
- Exporting the safety I/O parameter profile
- Importing the safety I/O parameter profile
- Behaviors when importing the safety I/O list with the safety I/O parameter profile assigned

D1.5.1 Starting Safety I/O Parameter Profile Editor

Perform this step to start Safety I/O Parameter Profile Editor:

- In System Structure Navigator, under I/O-Profiles, double-click [Safety I/O Parameter Profile].
  The Safety I/O Parameter Profile Editor appears in the document window area of the AD Organizer.

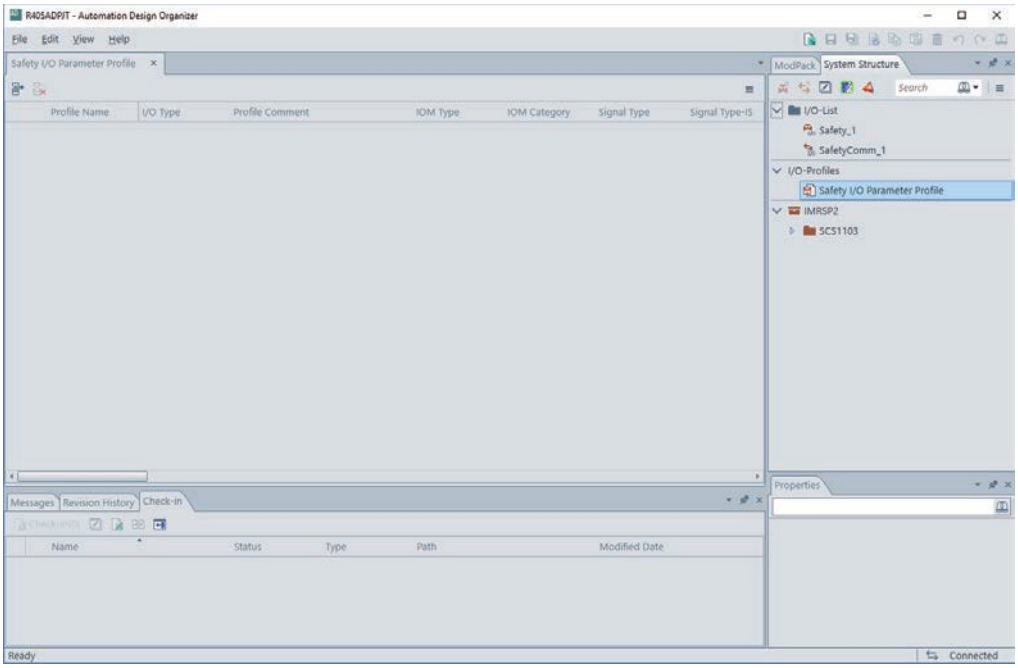


Figure D1.5.1-1 Safety I/O Parameter Profile Editor

TIP

If the safety I/O parameter profile has been defined, rows appear in the I/O parameter list area.

D1.5.2 Checking out the safety I/O parameter profile

You must check out a safety I/O parameter profile before defining it.

Perform this step to check out a safety I/O parameter profile:

- In System Structure Navigator, with the safety I/O parameter profile selected, click [Check-out] on the tool bar of AD Organizer.

SEE ALSO For more information about check-out operation, refer to:

"■ Checking out manually" in B4.2.1, "Check-out" in Engineer's Reference Manual (IM 32P04B10-01EN)

D1.5.3 Defining the safety I/O parameter profile

Follow these steps to define the safety I/O parameter profile:

1. In Safety I/O Parameter Profile Editor, click [Add row(s)].
   A row of profiles is added to the I/O parameter list area.
2. Type the name of the safety I/O parameter profile and press [Enter].
   The name of the safety I/O parameter profile is set.
3. Click the necessary column cell and define the profile.

TIP

The maximum number of safety I/O parameter profiles that you can define is 1000.

Definition items of the safety I/O parameter profile

The following table describes a list of the definition items of the safety I/O parameter profile.

Table D1.5.3-1 List of definition items of the safety I/O parameter profile

Column name	Description
Profile Name (*1)	Name of the I/O parameter profile.
I/O Type (*1)	I/O type
Profile Comment	Comment for the profile. Displayed as a tooltip in the I/O parameter profile column of Safety I/O Editor.
IOM Type (*1)	I/O Module name
IOM Category (*1)	I/O Module type
Signal Type	Signal type
Signal Type-IS	Signal type of the base plate for barrier for N-IO
Signal Conversion	Signal conversion
Signal LO	Low limit of the field I/O signal
Signal HI	High limit of the field I/O signal
Signal Unit	Engineering unit of the field I/O signal
Wire Type	Wire type of N-IO
Device OFF-ON Variable Name	Variable names for instructing a reset of fire and gas equipment
Reset Group ID	Reset Group ID
Input Processing at Fault	Input processing at fault
Input Value at Fault %	Input value at fault
Input Processing at Transmitter Fault	Specify input at transmitter fault
Detect IOP (High)	Detect IOP (High)
Detect IOP (Low)	Detect IOP (Low)
IOP High Limit	Threshold of IOP (High) %
IOP Low Limit	Threshold of IOP (Low) %
Detect Transmitter Fault (High)	Detect Transmitter Fault (High)
Detect Transmitter Fault (Low)	Detect Transmitter Fault (Low)
Threshold of Transmitter Fault (High) %	Threshold of Transmitter Fault (High)
Threshold of Transmitter Fault (Low) %	Threshold of Transmitter Fault (Low)
Field Power Diagnosis	Field Power Diagnosis
Reference Junction Compensation	Reference junction compensation

Continues on the next page

Table D1.5.3-1 List of definition items of the safety I/O parameter profile (Table continued)

Column name	Description
Burnout	Specify burnout
Time to Chattering Recovery Notice (s)	Time to chattering recovery notice
I/O Shutoff Switch	Specify I/O shutoff switch of N-IO
Output Shutoff Switch	Specify output shutoff switch of FIO and DO shutoff switch of N-IO
Output Processing at Fault	Specify output processing at fault
Output Value at Fault %	Output value at fault
Tight-shut/Full-open	Specify Tight-shut/Full-open
Tight-shut Value %	Tight-shut value
Full-open Value %	Full-open value
Detect Short Circuit	Detect short circuit
Detect Disconnection	Detect disconnection
Detect LFD	Detect LFD
Pulse Test	Pulse test
Pulse Test (OFF)	Pulse test (OFF)
Pulse Test (ON)	Pulse test (ON)
Low Voltage Pulse Test (ON)	Low voltage pulse test (ON)
SOER	SOER setting
Trip Signal (Setting for SOER)	Specify trip signal
Command	Command

*1: Mandatory definition items

When you define items other than Profile Name, I/O Type, Profile Comment, IOM Type, and IOM Category in the safety I/O parameter profile, the items will be reflected to the I/O of the safety I/O list.

D1.5.4 Deleting the safety I/O parameter profile

Follow these steps to delete the safety I/O parameter profile:

1. In the I/O parameter list area of Safety I/O Parameter Profile Editor, select the safety I/O parameter profile to delete.
2. On the tool bar of Safety I/O Parameter Profile Editor, click [Delete row(s)].
   The selected safety I/O parameter profile is deleted.

IMPORTANT

- Do not delete safety I/O parameter profiles that are in use.
- An error occurs if you try to delete a safety I/O parameter profile that is in use and perform check-in.

SEE ALSO For more information about unassignment of safety I/O parameter profile, refer to:

D1.5.6, “Assigning the safety I/O parameter profile to the I/O of the safety I/O list” on page D1-33

D1.5.5 Saving and checking in the safety I/O parameter profile

Save and check in the safety I/O parameter profile. This operation saves the safety I/O parameter profile in the AD project.

Follow these steps to save and check in the safety I/O parameter profile:

1. While the focus is on Safety I/O Parameter Profile Editor, click [Save] on the tool bar of AD Organizer.
2. In the Check-in window, perform a check-in of the defined safety I/O parameter profile. The check-out icon of the safety I/O parameter profile disappears.

TIP

The safety I/O parameter profile also appears in the following editors and window:

- Grid Rule Editor
- ModPack Editor
- Revision History Window

SEE ALSO

For more information about operations for a check-in, refer to:

"■ Checking in manually" in B4.2.4, "Check-in" in Engineer's Reference Manual (IM 32P04B10-01EN)

D1.5.6 Assigning the safety I/O parameter profile to the I/O of the safety I/O list

The safety I/O parameter profile that has been defined by using Safety I/O Editor is assigned to the I/O of the safety I/O list.

Follow these steps to assign the safety I/O parameter profile to the I/O of the safety I/O list:

1. Start the Safety I/O Editor in edit mode.
2. In Safety I/O Editor, select the cell of the I/O Parameter Profile column for the row for which you want to assign the safety I/O parameter profile.
   A drop-down list appears.
3. Select the safety I/O parameter profile to assign.
   The I/Os of the selected safety I/O parameter profile are assigned to the safety I/O list.

TIP

- The safety I/O parameter profile in which the I/O Type, IOM Type, and IOM Category match is assigned to the I/O of the safety I/O list.
- The I/Os with a safety I/O parameter profile assigned become read-only in Safety I/O Editor.
- To unassign the safety I/O parameter profile, select the cell of the corresponding I/O Parameter Profile column in Safety I/O Editor and delete the profile name.

D1.5.7 Reflecting the updated safety I/O parameter profile to the I/O of the safety I/O list

If you modify a safety I/O parameter profile in Safety I/O Parameter Profile Editor after assigning it to the I/O of the safety I/O list, reflect the changes in the safety I/O list.

The following methods can be used to reflect the updated safety I/O parameter profile to the I/O of the safety I/O list:

- Reflecting it in the safety I/O list by using Safety I/O Editor
- Reflecting it in the safety I/O list by using the I/O Parameter Update dialog box

■ Reflecting it in the safety I/O list by using Safety I/O Editor

Follow these steps to reflect the updated the safety I/O parameter profile in the safety I/O list by using Safety I/O Editor:

1. Start the Safety I/O Editor in edit mode.
2. In Safety I/O Editor, right-click the cell of the row in which the safety I/O parameter profile is to be reflected and select [Update I/O Parameter].
   The updated safety I/O parameter profile is reflected to the I/O of the safety I/O list.

TIP

- I/O parameter profiles that are not updated appear in yellow.
- In Safety I/O Editor, you can select the cells of the rows in which multiple safety I/O parameter profiles are to be reflected and reflect the changes.

3. While the focus is on Safety I/O Editor, click [Save] on the tool bar of AD Organizer.
4. By using the Check-in window, check in the reflected safety I/O list.

SEE ALSO

For more information about starting Safety I/O Editor in edit mode, refer to:

"■ Starting the Safety I/O Editor for editing" on page D1-6

For more information about operations for a check-in, refer to:

"■ Checking in manually" in B4.2.4, "Check-in" in Engineer's Reference Manual (IM 32P04B10-01EN)

■ Reflecting it in the safety I/O list by using the I/O Parameter Update dialog box

Follow these steps to reflect the updated the safety I/O parameter profile in the safety I/O list by using the I/O Parameter Update dialog box:

1. In System Structure Navigator, under I/O-Profiles, right-click [Safety I/O Parameter Profile] and select [Update I/O Parameter].
   The I/O Parameter Update dialog box appears.

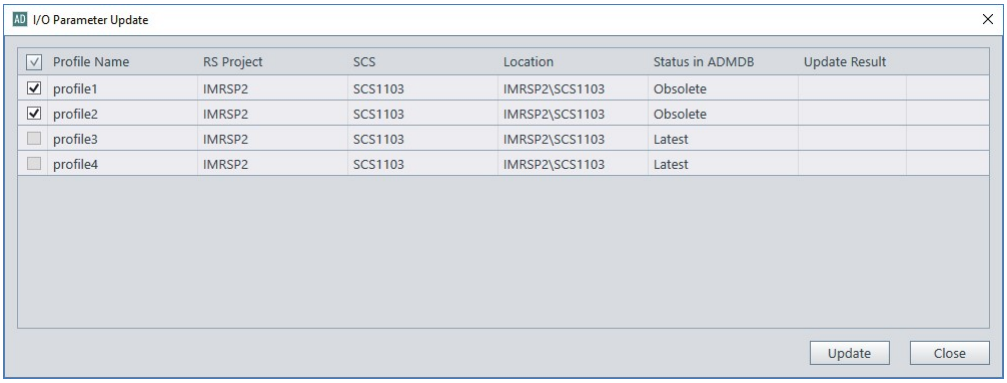


Figure D1.5.7-1 I/O Parameter Update dialog box

TIP

When the I/O Parameter Update dialog box appears, all safety I/O parameter profiles with items that have not been updated are selected. Safety I/O parameter profiles that have been updated cannot be selected.

2. Select the safety I/O parameter profile to update and click [Update].
   The updated safety I/O parameter profile is reflected to the I/O of the safety I/O list.
3. By using the Check-in window, check in the reflected safety I/O list.

SEE ALSO

For more information about operations for a check-in, refer to:

"■ Checking in manually" in B4.2.4, "Check-in" in Engineer's Reference Manual (IM 32P04B10-01EN)

D1.5.8 Exporting the safety I/O parameter profile

You can export the safety I/O parameter profile. Follow these steps to export the safety I/O parameter profile:

1. In the I/O parameter list area of Safety I/O Parameter Profile Editor, select one or multiple safety I/O parameter profiles to export.
2. In Safety I/O Parameter Profile Editor, click [Sub menu] and select [Export].
   The Folder selection dialog box appears.
3. Select the folder to which you want to export the safety I/O parameter profile and click [OK].

TIP

One file is exported and saved in xlsx format.

D1.5.9 Importing the safety I/O parameter profile

You can import the safety I/O parameter profile. Follow these steps to import the safety I/O parameter profile.

TIP You need to perform the check-out of a safety I/O parameter profile before importing it.

1. In Safety I/O Parameter Profile Editor, click [Sub menu] and select [Import].
   The File selection dialog box appears.
2. Select the safety I/O parameter profile file to import and click [OK].
   The safety I/O parameter profile that was imported in the I/O parameter list area appears.

TIP If you are importing a safety I/O parameter profile for the first time, assign the profile to the safety I/O list after the import. If you are importing an updated safety I/O parameter profile, reflect the changes to the I/O of the safety I/O list after the import.

SEE ALSO For more information about assigning the safety I/O parameter profile to the I/O of the safety I/O list, refer to:

D1.5.6, “Assigning the safety I/O parameter profile to the I/O of the safety I/O list” on page D1-33

For more information about reflecting the updated safety I/O parameter profile to the I/O of the safety I/O list, refer to:

D1.5.7, “Reflecting the updated safety I/O parameter profile to the I/O of the safety I/O list” on page D1-34

If a safety I/O parameter profile with the same name as the safety I/O parameter profile to be imported already exists in the AD Project

If a safety I/O parameter profile with the same name (not case-sensitive) as the safety I/O parameter profile to be imported already exists in the AD Project, the following Resolve Import Conflict dialog box appears when importing the safety I/O parameter profile.

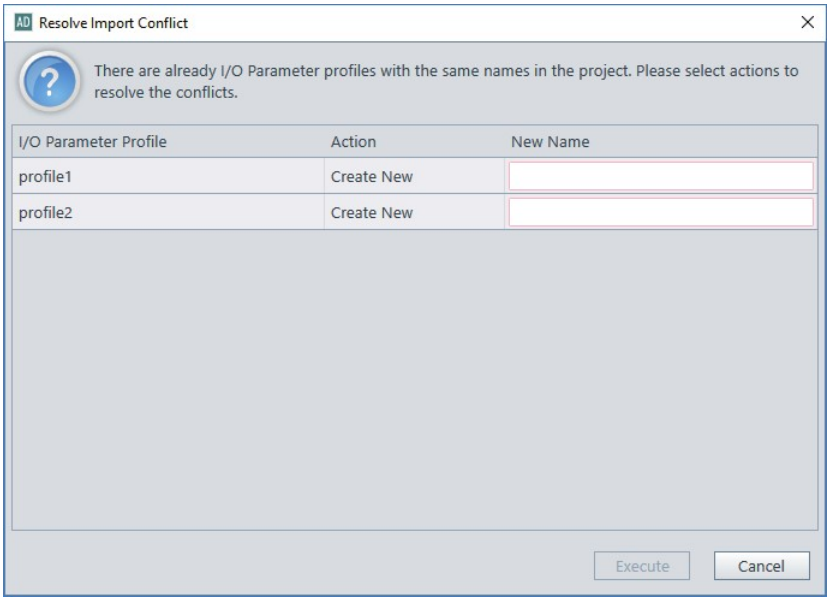


Figure D1.5.9-1 Resolve Import Conflict dialog box

If the Resolve Import Conflict dialog box appears, follow any of these steps:

- When importing by overwriting the existing safety I/O parameter profile
  In Action, select [Update] and click [Execute].

- When importing as a different safety I/O parameter profile
  In Action, select [Create New] and click [Execute] after entering a name that does not exist in New Name.
- When canceling the import
  In Action, select [Cancel] and click [Execute].

D1.5.10 Behaviors when importing the safety I/O list with the safety I/O parameter profile assigned

The safety I/O list is imported to Safety I/O Editor based on the P&ID Tag. When importing the safety I/O list with the safety I/O parameter profile assigned, the status of the I/O Parameter Profile column and I/O channel parameters in Safety I/O Editor become as follows:

If the safety I/O parameter profile name is changed by the import and the safety I/O parameter profile with the same name as the one after the change exists in the AD project, the I/O channel parameters are updated based on the corresponding safety I/O parameter profile that exists in the AD project.

However, if there are no changes in the safety I/O parameter profile name used before and after the import, the I/O channel parameters remain their status the same as before the import.

In addition, the I/O Parameter Profile column of the safety I/O list is shown in pink to indicate erroneous data after the import in the following cases:

- When the safety I/O parameter profile with the same profile name does not exists in the AD project
- When the safety I/O parameter profile with the same profile name exists in the AD project, but the I/O Type, IOM Type, and IOM Category do not match

In this case, take the necessary measures such as profile registration, profile name change, and profile deletion.

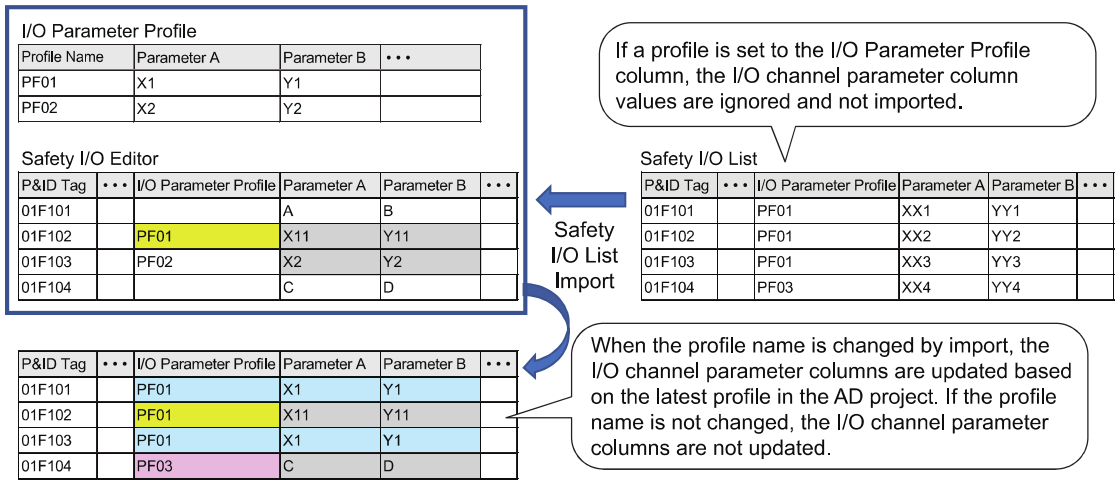


Figure D1.5.10-1 Status of the I/O parameter profile column in Safety I/O Editor after importing the safety I/O list

D1.5.11 Precautions for importing and restoring SCS projects including safety I/O parameters

This section describes precautions for importing and restoring SCS projects including safety I/O parameters.

Importing SCS

The behaviors when importing the SCS project including the safety I/O list with the safety I/O parameter profile assigned is as follows:

- If the safety I/O parameter profile with the same profile name does not exist in the AD project, the import ends up in a failure.
  If importing SCS fails, register the safety I/O parameter profile in the AD project and then import SCS again.
- If the safety I/O parameter profile with the same profile name exists in the AD project, and the imported I/O parameter value is the same as the I/O parameter value of the safety I/O parameter profile of the AD project, the import ends up in a success.
- If the safety I/O parameter profile with the same profile name exists in the AD project, and the imported I/O parameter value is different from the I/O parameter value of the safety I/O parameter profile of the AD project, the import ends up in a success. However, since the I/O parameter values are different from the values stored in the AD project, the values of the import source SCS are applied. The I/O Parameter Profile column of the safety I/O list is shown in yellow to indicate that there is a difference.
  If there is a difference, update the I/O parameter value as necessary.

Restoring SCS projects by Version Control Tool and Master Database Restoring function

The behaviors when restoring the SCS project including the safety I/O list to which the safety I/O parameter profile is assigned using the Version Control Tool and Master Database Restoring function is as follows:

- If the safety I/O parameter profile with the same profile name does not exist in the AD project, the restoring ends up in a failure.
  If the restoring fails, register the safety I/O parameter profile in the AD project and then restore the SCS project again.
- If the safety I/O parameter profile with the same profile name exists in the AD project, and the restored I/O parameter value is the same as the I/O parameter value of the safety I/O parameter profile of the AD project, the restoring ends up in a success.
- If the safety I/O parameter profile with the same profile name exists in the AD project, and the restored I/O parameter value is different from the I/O parameter value of the safety I/O parameter profile of the AD project, the restoring ends up in a success. However, since the I/O parameter values are different from the values stored in the AD project, the values of the restoring source SCS are applied. The I/O Parameter Profile column of the safety I/O list is shown in yellow to indicate that there is a difference.
  If there is a difference, update the I/O parameter value as necessary.

D1.6 Saving the safety I/O list and performing check-in

You can save the safety I/O list and perform check-in. By performing this operation, the safety I/O list is stored in the AD project.

Saving the safety I/O list

Follow these steps to save the safety I/O list:

1. Select the Safety I/O Editor.
2. On the tool bar of AD Organizer, click the [Save] button.

TIP

- When the I/O module assignment information of the safety I/O list is edited, the safety I/O list (I/O_definition) in the I/O module of the assignment destination is automatically checked out, and the content of the definition is reflected.
- When the Safety I/O Editor is in Deviation mode, you cannot save the safety I/O list.

Performing check-in of the safety I/O list

In the Check-in window, check in the defined safety I/O list.

The check-out icon of the safety I/O list disappears.

D2. Engineering based on the safety communication I/O list

The I/O information of the safety communication I/O list can be defined, browsed, or edited by using Safety Communication I/O Editor. With the safety communication I/O list, you can manually enter I/O information or import and edit an I/O information list obtained from a plant designer. The items subject to definitions of the safety communication I/O list are the following communication categories and module types amongst the FIO.

Table D2-1 Items subject to definitions of the safety communication I/O list

Communication category	Module type
Serial	ALR111M, ALR121M (for subsystem communication)
Ethernet	ALE111M (for subsystem communication)
PROFINET	S2LP131 (for safety subsystem communication)

With the safety communication I/O list, you can configure Ethernet communication I/O, serial communication I/O, and fire and gas communication I/O for each I/O point.

The following shows the work flow of engineering for the safety communication I/O list.

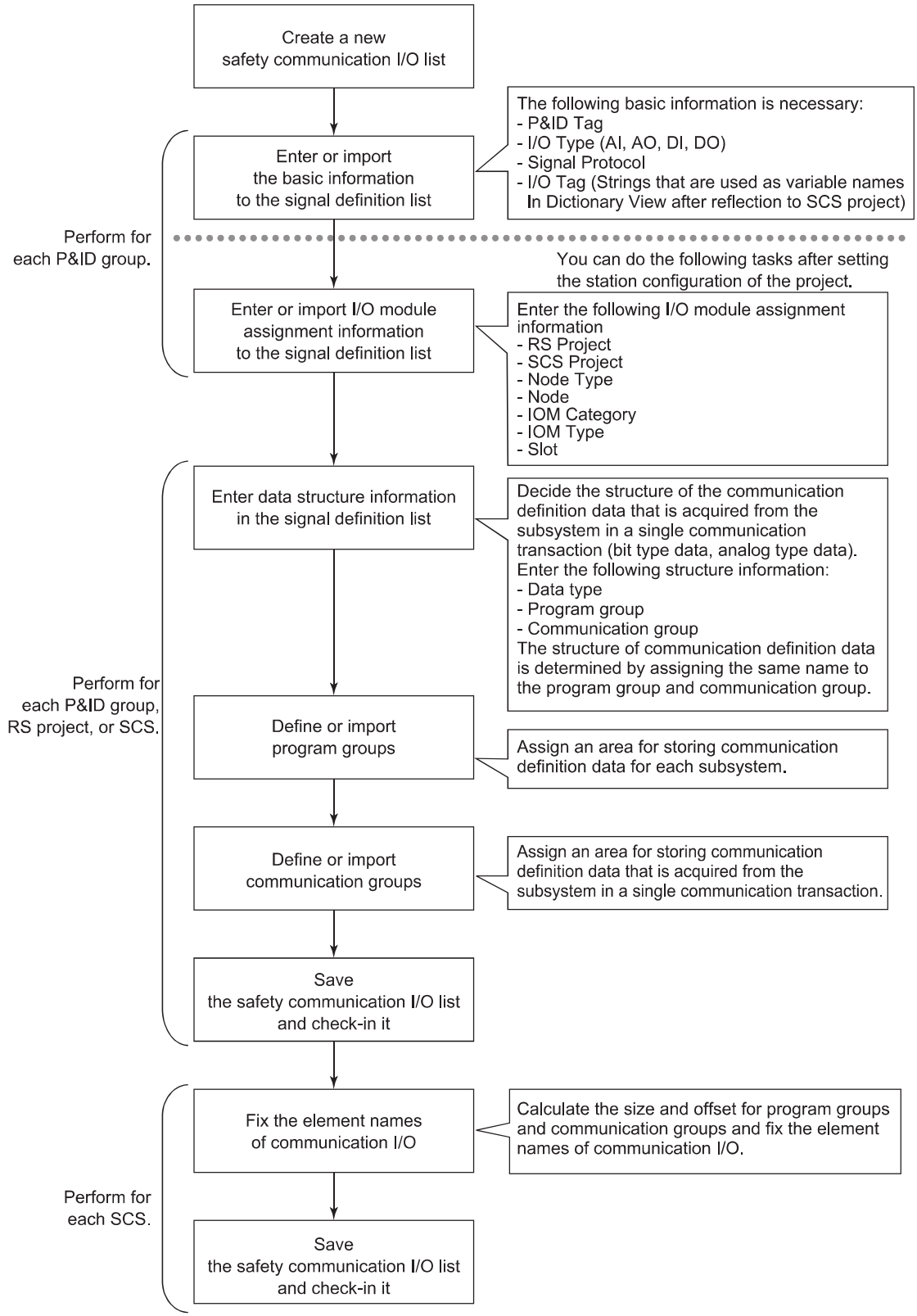


Figure D2-1 Work flow of engineering for the safety communication I/O list

SEE ALSO

For more information about operations for every P&ID group and SCS, refer to:

"■ Starting the Safety Communication I/O Editor for editing" on page D2-6

For more information about data structures, program groups, and communication groups, refer to:

D2.5.1, "Overview of definitions for communication with subsystems" on page D2-22

D2.1 Creating a new safety communication I/O list

Follow these steps to create a safety communication I/O list:

1. Select the I/O-List folder of System Structure Navigator.
2. From the context menu, select [New Safety Communication I/O].
   The newly created safety communication I/O list appears in the edit mode in System Structure Navigator.
3. Enter a unique safety communication I/O list name.
   A new safety communication I/O list is created. Once the list is newly created, it is automatically checked in to the server.

TIP

The safety communication I/O list name that is entered is referred to as the P&ID group.

SEE ALSO

For more information about how to change the name of a safety communication I/O list after creating the safety communication I/O list, refer to:

"■ Changing the name of the safety communication I/O list" on page D2-5

For more information about the maximum number of safety communication I/O lists, refer to:

A4., "Application capacity of AD Suite" in Engineer's Reference Manual (IM 32P04B10-01EN)

■ Folder location of the safety communication I/O list definition

After RS Project and SCS Project are set in the safety communication I/O list, a file containing the I/O information for an individual SCS is copied to the Comm_I/O folder under the corresponding SCS folder.

Thereafter, you can select the Comm_I/O folder to start Safety Communication I/O Editor from the context menu. Only the contents that are defined in the corresponding file are shown in the editor.

D2.2 Operating a safety communication I/O list

This section describes how to rename and delete a safety communication I/O list.

Changing the name of the safety communication I/O list

Follow these steps to change the name of the safety communication I/O list:

1. Right-click on the safety communication I/O list in System Structure Navigator and select [Rename].
   The P&ID group of the safety communication I/O list name appears in the edit status.
2. Enter a new P&ID group.
   The name of the safety communication I/O list changes.

Deleting the safety communication I/O list

You need to delete the safety communication I/O list after deleting all I/O information that is assigned to the I/O module. Follow these steps to delete the safety communication I/O list:

- Select the safety communication I/O list in System Structure Navigator and click [Delete] on the tool bar of AD Organizer.

TIP

- When the Safety Communication I/O Editor is running, the safety communication I/O list cannot be deleted.
- You can delete only one safety communication I/O list at a time.

SEE ALSO

For more information about input/output module assignment information, refer to:

D2.4, “Entering I/O information in the signal definition list” on page D2-17

D2.3 Starting Safety Communication I/O Editor

You can start the Safety Communication I/O Editor from the System Structure Navigator in AD Organizer. The modes of the Safety Communication I/O Editor are edit mode, revision history mode and read-only mode.

You can open two windows simultaneously with the following combination:

- Edit mode and read-only mode
- Revision history mode and read-only mode

You cannot open two windows with the combination of edit mode and revision history mode.

Starting the Safety Communication I/O Editor for editing

Depending on the operation purpose, method for starting Safety Communication I/O Editor varies.

IMPORTANT

To edit I/O information for each RS project or SCS, you can start Safety Communication I/O Editor after setting the station configuration and defining the I/O module assignment information in the signal definition list.

Perform one of the following operations using the System Structure Navigator to start the Safety Communication I/O Editor:

- When editing I/O information for each P&ID group
  Double-click the safety communication I/O list in the [I/O-List] folder.

  Safety Communication I/O Editor appears in the document window area of AD Organizer and the I/O points belonging to the P&ID group appear in the safety communication I/O list.
- When editing I/O information for each applicable RS project
  Right-click the RS project in System Structure Navigator and select [Open] > [Safety Communication I/O Editor].

  Safety Communication I/O Editor appears in the document window area of AD Organizer and the I/O points belonging to the applicable RS project appear in the safety communication I/O list.
- When editing I/O information for each applicable SCS
  In System Structure Navigator, double-click on [Comm_I/O] under the applicable SCS.

  Safety Communication I/O Editor appears in the document window area of AD Organizer and the I/O points belonging to the applicable SCS appear in the safety communication I/O list.

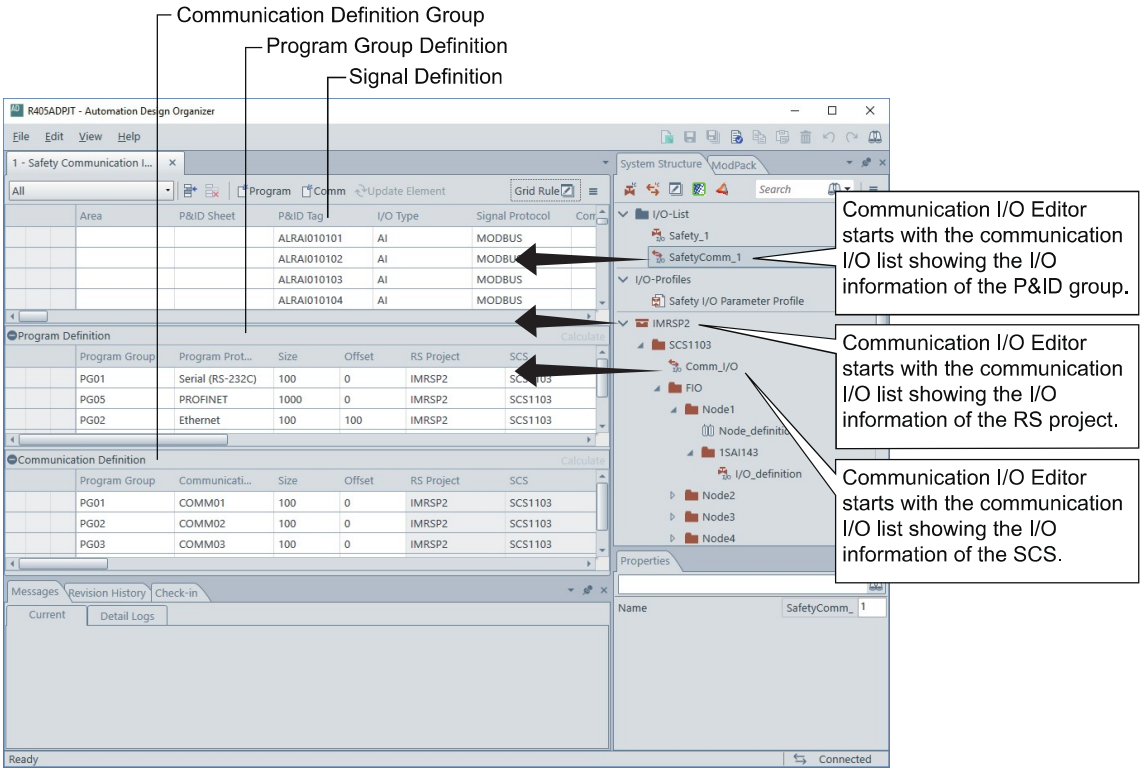


Figure D2.3-1 Safety Communication I/O Editor

TIP

- In the safety communication I/O list, Ethernet communication I/O and serial communication I/O for subsystem communication and fire and gas communication I/O for safety subsystem communication are each shown with a line for every I/O point.
- The program group definition list and communication group definition list are defined for each SCS regardless of how Safety Communication I/O Editor is started.
- When Safety Communication I/O Editor is started, information of the source from which you started the editor is shown in the window title.

The functions that you can use will vary depending on the project and definition items that were selected prior to starting Safety Communication I/O Editor. The following table shows the differences.

Table D2.3-1 Differences of functions depending on how the editor is started

Definition item or project selected upon startup	Export function (*1)	Import function (*1)	Size/Element automatic calculation	Editing of the Wiring column
P&ID group (I/O-list)	Yes	Yes	No	Read-only
RS project	Yes	No	No	Read-only
SCS project	Yes	No	Yes	Write-only

*1: Indicates whether or not the function will operate.
Yes: The function can be operated
No: The function cannot be operated

Starting the Safety Communication I/O Editor for read-only

Depending on the operation purpose, method for starting Safety Communication I/O Editor varies.

- Perform one of the following operations using the System Structure Navigator to start the Safety Communication I/O Editor in read-only mode:

- When reading definitions for each P&ID group
  Right-click the safety communication I/O list in the [I/O-List] folder and select [Open (Read-Only)].
- When reading definitions for each applicable RS project
  Right-click the RS project and select [Open (Read-Only)] > [Safety Communication I/O Editor].
- When reading definitions for each applicable SCS
  Right-click the [Comm I/O] under the applicable SCS and select [Open (Read-Only)].

The Safety Communication I/O Editor appears in the document window area in read-only mode.

TIP

If content is being edited in the edit mode editor, the contents being edited are also reflected in the read-only mode editor. However, the update is manual.

Switching the display of the safety communication I/O list

You can switch the display of the safety communication I/O list for each I/O type. Perform the following operation to switch the display:

- From the drop-down list on the upper-left pane of the safety communication I/O list, select the items you wish to display.

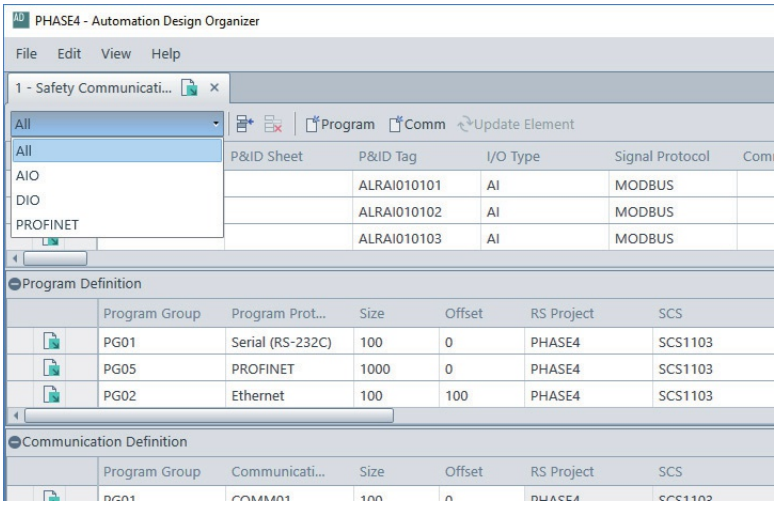


Figure D2.3-2 Drop-down list for switching the display

Only the selected items are shown.

Setting items of Safety Communication I/O Editor

The following lists are defined with Safety Communication I/O Editor:

- Signal definition list
- Program group definition list
- Communication group definition list

The following figure shows where the lists are defined.

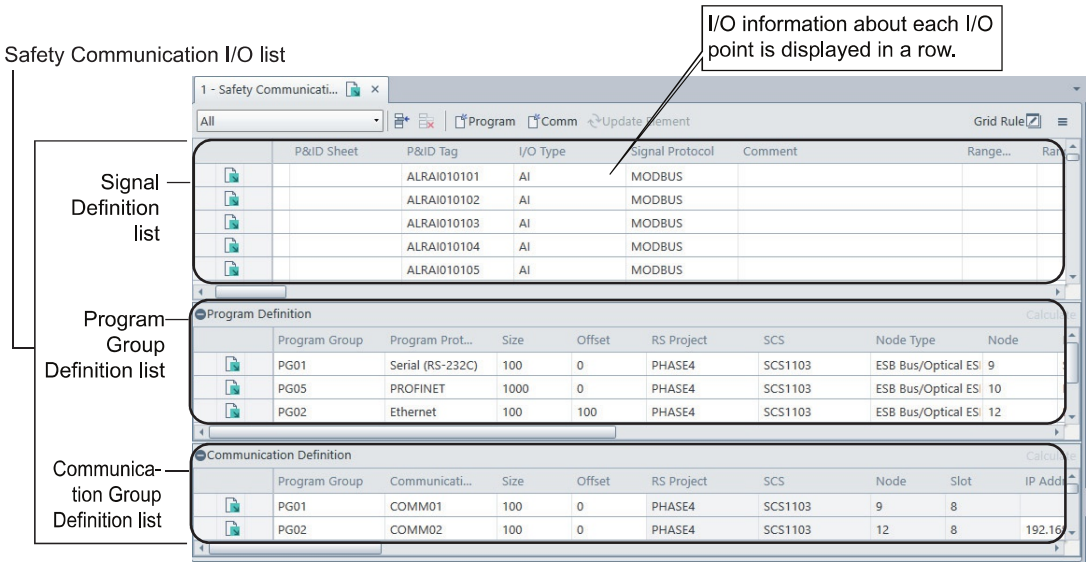


Figure D2.3-3 Window configuration of Safety Communication I/O Editor

The following table shows each of the setting items.

Setting items for the signal definition list

Table D2.3-2 List of setting items of the "signal definition list"

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
For I/O list management	Area	Area name	-	-
	P&ID Sheet	P&ID sheet name	-	-

Continues on the next page

Table D2.3-2 List of setting items of the "signal definition list" (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
I/O list common	P&ID Tag	P&ID tag name Key information required to identify each I/O. The P&ID tag must be unique within the P&ID group.	1	-
	I/O Type	I/O type. Select from the following: AI, AO, DI, DO	1	-
	Signal Protocol	The signal type. Select from the following: MODBUS MODBUS (SLS) PROFINET PROFIsafe	1	-
	Comment	The variable comment of the IO variable that is defined in Dictionary View.	-	Dictionary View: Comment Communication I/O Builder (Comm. I/O Wiring, PROFINET Comm. I/O Wiring)
	Range LO	Low limit	-	-
	Range HI	High limit	-	-
	Eng Unit	Engineering unit	-	-
	I/O Tag	I/O tag name Normally, set the same name as the P&ID tag, or an abbreviated form thereof. The I/O tag must be unique within the SCS. A character string that will become the variable name in Dictionary View after reflection onto the SCS project. Otherwise, a variable name that will be wired with Communication I/O Builder.	1	Dictionary View: Name Communication I/O Builder (Comm.I/O Wiring, PROFINET Comm.I/O Wiring)
	Variable Group	Variable Group	-	Dictionary View

Continues on the next page

Table D2.3-2 List of setting items of the "signal definition list" (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
Communication I/O definitions	Program Group	The program group to which this signal belongs	2	-
	Communication Group	The communication definition group to which this signal belongs		Communication I/O Builder (PROFINET Comm.I/O Definition)
	PN-Data	Valid only when using PROFINET. Data name prescribed with the PROFIBUS GSD file.		Communication I/O Builder (PROFINET Comm.I/O Definition)
	Wiring	Specifies whether to newly register this variable to Dictionary View or to assign it to a variable that has already been registered. Select from the following: (Global)/List of FB instances of local variables and FB instances of user-defined FB parameters		Communication I/O Builder (Comm.I/O Definition, Comm.I/O Wiring, PROFINET Comm.I/O Definition, and PROFINET Comm.I/O)
	Position	The order of %WW or %WB within a single communication group		-
	Bit Position	Defines the Bit position when using %WB		-
	Comm Device & Address	Addresses of other devices		Communication I/O Builder (Comm.I/O Definition)
	Data Type	Data type Select from the following: U8/I8/U16/I16/U32/I32/F32/Bit		Communication I/O Builder (Comm.I/O Definition, Comm.I/O Wiring, PROFINET Comm.I/O Definition, and PROFINET Comm.I/O Wiring)
	Element	Element number This can normally be calculated automatically.	3	Communication I/O Builder (Comm.I/O Definition, PROFINET Comm.I/O Definition)
	Fix Element	A setting for fixing the element number. Select either Yes/No. When Yes is selected, the element number does not change even when Update Element is pressed.	3	-
	Reverse	Reverse data	2	Communication I/O Builder (Comm.I/O Definition)

Continues on the next page

Table D2.3-2 List of setting items of the "signal definition list" (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
IOM assignment information	RS Project	The SCS and IOM assignment information to which this signal is being assigned. By defining the Program Group column, the corresponding program group definitions are reflected and then later become read-only.	-	The content defined here is taken into IOM Definition Editor and then reflected onto I/O Wiring View when implementing RS Generation.
	SCS			
	Node Type			
	Node			
	IOM Category			
	IOM Type			
	Slot			
I/O description	Input Processing at Fault	Input processing at fault	-	Communication I/O Builder: Input Processing at Fault
	Input Value at Fault	Input value at fault		Communication I/O Builder: Input Value at Fault

*1: Whether column settings are required or not are indicated in the following categories:
Meaning of the Mandatory setting or not column
- 1: Configuration is always required
- 2: Configuration is required after assigning the I/O to SCS and IOM
- 3: Configuration is preferred after assigning the I/O to SCS and IOM
- -: Configuration is not required

Other settings items such as Connection Device Info, For I/O list management, For iDefine reference, and User Define Column also appear.

SEE ALSO

For more information about columns common to Safety I/O Definition Editor that are included in the signal definition list, refer to:

"■ Setting items of the Safety I/O Editor" on page D1-7

Setting items for the program group definition list

Table D2.3-3 List of setting items of the "program group definition list"

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
Program definition	Program Group	Defines the program group name	3	-
	Program Protocol	This is read-only. The value is selected from the following: • Serial (RS-232C) • Serial (RS-422) • Serial (RS-485) • Serial (RS-422/ RS-485) • Ethernet • PROFINET		-
	Size	The size of this program definition This becomes the area of %XW.		Communication I/O Builder: Buffer size (Program)
	Offset	Specifies the beginning position of this program definition as the offset from the beginning of the SCS communication I/O area. This becomes the first number of %XW.		Communication I/O Builder: Buffer
	RS Project	The name of the RS project to which this program definition will be assigned		-
	SCS	The SCS number to which this program definition will be assigned		-
	Node Type	The node type to which this program definition will be assigned (only "ESB Bus/Optical ESB Bus" can be selected).		-
	Node	The node number to which this program definition will be assigned		I/O Wiring View, I/O Parameter Builder
	IOM Category	The IOM category to which this program definition will be assigned. PROFINET for fire and gas devices		-
	IOM Type	The IOM type to which this program definition will be assigned		I/O Wiring View, I/O Parameter Builder
	Slot	The slot number to which this program definition will be assigned		I/O Wiring View, I/O Parameter Builder

Continues on the next page

Table D2.3-3 List of setting items of the "program group definition list" (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
Program definition	Duplex	The specification for duplexing the IOM to which this program definition will be assigned.	3	I/O Parameter Builder: Module
Program definition (*2)	IOM Host Name	This is read-only. The device tag name of S2LP131 (reflected from the definition by PROFINET Configurator).	-	I/O Parameter Builder: Module
	IOM Address	This is read-only. The IP address of S2LP131 (reflected from the definition by PROFINET Configurator).		I/O Parameter Builder: Module
	IOM Subnet Mask	This is read-only. The subnet mask of S2LP131 (reflected from the definition by PROFINET Configurator).		I/O Parameter Builder: Module
	IOM Default Gateway	This is read-only. The default gateway of S2LP131 (reflected from the definition by PROFINET Configurator).		I/O Parameter Builder: Module
	Connection Device Type	Select from the following: • Modbus • ProSafe-SLS • PROFINET		I/O Parameter Builder: Module
Safety communication I/O list management	P&ID Group	This is read-only. The value for the same column name of the program group definition.	-	-

*1: Whether column settings are required or not are indicated in the following categories: Meaning of the Mandatory setting or not column
- 1: Configuration is always required
- 2: Configuration is required after assigning the I/O to SCS and IOM
- 3: Configuration is preferred after assigning the I/O to SCS and IOM
- -: Configuration is not required

*2: PROFINET Configurator can be started from Safety Communication I/O Editor.

Setting items of the communication group definition list

Table D2.3-4 List of setting items of the "communication group definition list"

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
Communication definition	Program Group	The program group to which this communication definition belongs	3	-
	Communication Group	Defines the communication group name	3	Communication I/O Builder (PROFINET Comm.I/O Definition)
	Size	The size of this communication definition	3	Communication I/O Builder (Comm.I/O Definition, PROFINET Comm.I/O Definition)
	Offset	Specifies the beginning position of this communication definition as the offset from the beginning of the program definition.	3	-
	RS Project	This is read-only. The value indicates the IOM to which this communication definition will be assigned. By defining the Program Group column, the corresponding program group definitions are reflected.	-	-
	SCS			-
	Node			I/O Wiring View
	Slot			I/O Wiring View
	IP Address	The IP address	3	Communication I/O Builder (PROFINET Comm Definition)
	2nd IP Address	The IP address for duplex subsystems	3	Communication I/O Builder: 2nd IP Address
	Connection Device Tag	The name of the device having the IP address	-	Communication I/O Builder (PROFINET Comm Definition)
	Connection Device Tag Comment	The comment for the previous device	-	-
	Port	The port number	3	Communication I/O Builder: Port
	Station	The station number	3	Communication I/O Builder (Comm.I/O Definition)
	SLSEVENT	SLSEVENT (*2) The default value is No. When changing this to Yes, the size will be fixed at 24.	3	Communication I/O Builder (Comm.I/O Definition)

Continues on the next page

Table D2.3-4 List of setting items of the "communication group definition list" (Table continued)

Category	Column name	Description	Mandatory setting or not (*1)	SCS Manager item where the setting is reflected through RS Generation
Communication definition (*3)	PN-Device Slot Tag	This is read-only. The definition of PROFINET Configurator. (Reflected from the definition by PROFINET Configurator.)	3	Communication I/O Builder (PROFINET Comm Definition)
	Subnet Mask			
	Default Gateway			
	PN-Updating Time			
	PN-Watchdog Time	This is read-only. The definition of PROFINET Configurator. (Reflected from the definition by PROFINET Configurator.)	3	Communication I/O Builder (PROFINET Comm.I/O Definition)
	PN-Slot			
	PN-Module			
	PN-Sub Slot			
	PN-Submodule	This is read-only. The definition of PROFINET Configurator. (Reflected from the definition by PROFINET Configurator.)	3	Communication I/O Builder (PROFINET Comm.I/O Definition)
	PN-Signal Information			
	F_Check_iPar	This is read-only. PROFIsafe-related definition. (Reflected from the definition by PROFINET Configurator.)	3	Communication I/O Builder (PROFINET Comm.I/O Definition)
	F_SIL			
	F_CRC_ Length			
	F_CRC_ Seed			
	F_Passivation			
	F_Block_ID			
	F_Par_Version			
	F_Source_Add			
	F_Dest_Add			
	F_WD_Time			
	F_WD_Time_2			
	F_iPar_CRC			
	F_Par_CRC			
Safety communication I/O list management	P&ID Group	This is read-only. The value for the same column name of the program group definition.	-	-

*1: Whether column settings are required or not are indicated in the following categories: Meaning of the Mandatory setting or not column
- 1: Configuration is always required
- 2: Configuration is required after assigning the I/O to SCS and IOM
- 3: Configuration is preferred after assigning the I/O to SCS and IOM
- -: Configuration is not required

*2: When defining SLSEVENT, set only the program definition and communication definition without setting the signal definition. A signal cannot be associated with a communication group for the SLSEVENT definition. An error will occur when trying to save if a signal is defined.

*3: PROFINET Configurator can be started from Safety Communication I/O Editor.

SEE ALSO For more information about PROFINET Configurator, refer to:

E1.5.2, “Applying settings by using PROFINET Configurator” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

D2.4 Entering I/O information in the signal definition list

Define I/O information in the signal definition list. When the SCS and communication modules to be assigned to the I/O points are decided, define this information as well.

■ Editing the signal definition list

Follow these steps to edit the I/O information of the signal definition list:

1. Select the safety communication I/O list in System Structure Navigator and click [Check-out] on the tool bar of AD Organizer.
   The safety communication I/O list is checked out.
2. Select the signal definition list of Safety Communication I/O Editor and click [Add Row] on the tool bar.
   An I/O point is added to the signal definition list.
3. Enter I/O information into the cells in the signal definition list.

SEE ALSO For more information about setting items of the signal definition list, refer to:

"■ Setting items of Safety Communication I/O Editor" on page D2-8

● Editing the I/O information of the signal definition list

Follow these steps to edit the I/O information of the signal definition list:

1. Select a cell in the signal definition list.
   A dialog box appears, asking you to confirm the check-out.
2. Click [Yes].
   The I/O point is checked out and the icon for the item of [Checked-out Status] in the signal definition list changes.
3. Enter I/O information into the cells in the signal definition list.

TIP I/O points can be added to the signal definition list when Safety Communication I/O Editor is started for each P&ID group or target SCS.

SEE ALSO For more information about setting items of the signal definition list, refer to:

"■ Setting items of Safety Communication I/O Editor" on page D2-8

● Adding an I/O point to the signal definition list

Follow these steps to add I/O points to the signal definition list when the safety communication I/O list is not checked out:

1. Select an I/O point from the signal definition list.
2. Click [Add Row] on the tool bar.
   An I/O point is added above the selected I/O point and this added I/O point is checked out.

TIP I/O points can be added to the signal definition list when Safety Communication I/O Editor is started for each P&ID group or target SCS.

Initializing the I/O information of an edited signal definition list

Follow these steps to return the I/O information of an edited signal definition list to its initial values:

1. Select one or more cells of the signal definition list.
2. Right-click on the selected cell and select [Reset to Default].

Deleting an I/O point from the signal definition list

Follow these steps to delete an I/O point from the signal definition list:

1. Select the I/O point to delete from the signal definition list.
2. Click [Delete Row(s)] on the tool bar.
   The selected I/O points are deleted.

Entering basic information of I/O points

Enter the following items as basic information of the signal definition list:

- P&ID Tag
- I/O Type
- Signal Protocol
- I/O Tag
- Data type

Refer to the following table for settings of the Signal Protocol, I/O Type, and Data type.

Table D2.4-1 Relationship between the Signal Protocol and the Data type

Signal Protocol	I/O Type	Data type
MODBUS	AI AO	U16 I16 I32 F32
	DI DO	Bit
MODBUS (SLS)	AI AO	U16
	DI DO	Bit
PROFINET	AI	U8 I8 U16 I16 U32 I32 F32
PROFIsafe	AI	U8 I8 U16 I16 U32 I32 F32

As needed, define the following items for defining the data structure to obtain from the sub-system being connected to:

Program Group	:	The program group to which the I/O point belongs.
Communication Group	:	The communication definition group to which the I/O point belongs.
Position / Bit Position	:	The order of %WW and %XW in the communication definition group. Bit Position defines the bit position of %WW.
Comm Device & Address	:	The addresses of other devices.

Position denotes the order of %WW and %XW within a single communication group. Bit Position is the bit position when the Data type of DI or DO is Bit. These items are used when deciding the numbers for %WW and %XW.

TIP

%WW is an area assigned to communication modules for subsystem communication while %XW is an area assigned to communication modules for safety subsystem communication.

IMPORTANT

Do not define SLSEVENT, a data type used with ProSafe-SLS communication, in the signal area and configure only the program group definition and communication definition group. A signal cannot be associated with a communication group for the SLSEVENT definition. An error will occur when trying to save.

Entering I/O module assignment information of the signal definition

The following are precautions when assigning an I/O points of the signal definition to an I/O module.

- When assigning I/O points to an I/O module, define RS Project, SCS, Node Type, Node, IOM Category, IOM Type, and Slot. When these values are defined, the I/O points are copied to the Comm_I/O file under the SCS folder.
- When I/O information is entered to I/O points for which the I/O module assignment information is not defined, all I/O points for which I/O module assignment information is not defined are checked out. When I/O information is entered to I/O points for which the I/O module assignment information is defined, all I/O points which are assigned to the same SCS are checked out.

Purpose of user definition and changing user-defined name

In addition to the default setting items, 40 setting items that users can define freely are provided in the safety communication I/O list. I/O information that is included in the user-defined setting items is reference information. This I/O information is not reflected to the SCS project. However, when engineering by using iDefine, the user-defined I/O information is included in the ProSafe-RS I/O file. As such, we recommend that you configure the ID and other information that you want to refer to when creating an application logic by using iDefine here. If you assign an alias to a user-defined column, the user-defined column header of the ProSafe-RS I/O file that is exported to iDefine becomes the defined alias.

You can use the user-defined setting items as reference information when using the grid rules.

Any name can be specified for the user-defined setting items. Follow these steps to specify any name for the user-defined setting items:

1. From the sub menu of the safety communication I/O list, select [User Define Column Setting].
   The User Define Column Setting dialog box appears.

   The initial values of the setting item names are displayed in User Definition Column.

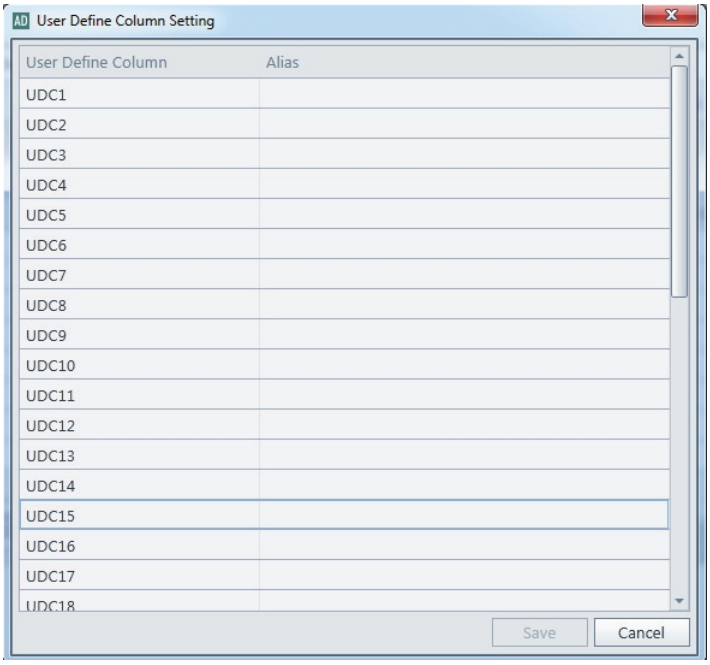


Figure D2.4-1 User Define Column Setting dialog box

2. Enter the name that needs to be changed in [Alias], and click [Save].
   The new name is displayed in the user-defined setting item of the safety communication I/O list.

D2.5 Converting I/O information into a data structure that can be communicated with subsystems

This section describes how to convert I/O information into a data structure that can be communicated with subsystems being connected by using Safety Communication I/O Editor.

D2.5.1 Overview of definitions for communication with subsystems

In order to communicate with subsystems, after assigning a communication I/O data area for each subsystem being connected, you must set what kind of data to obtain from the connected subsystems and in which part of the connected subsystems the data will be written. With this setting, each assigned area is split into units of data which can be obtained or set with a single round of communication with the connected subsystem and then defined for how each of these will communicate by using Safety Communication I/O Editor. The following figure shows an overview of communication definitions for subsystems.

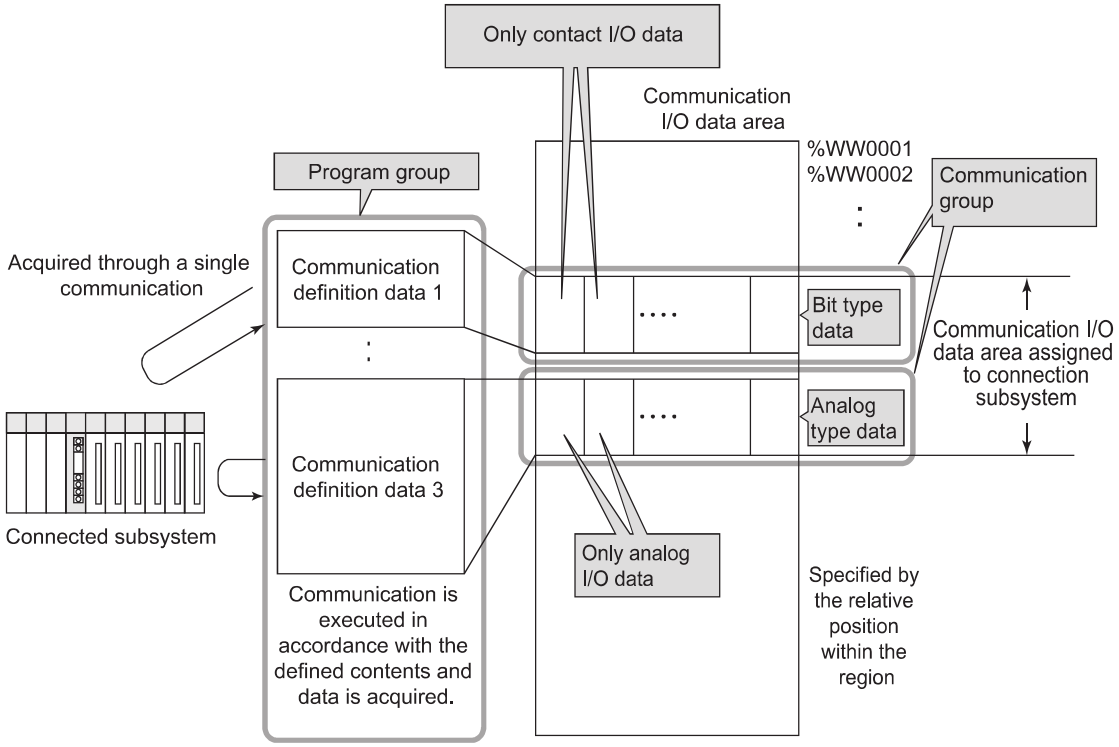
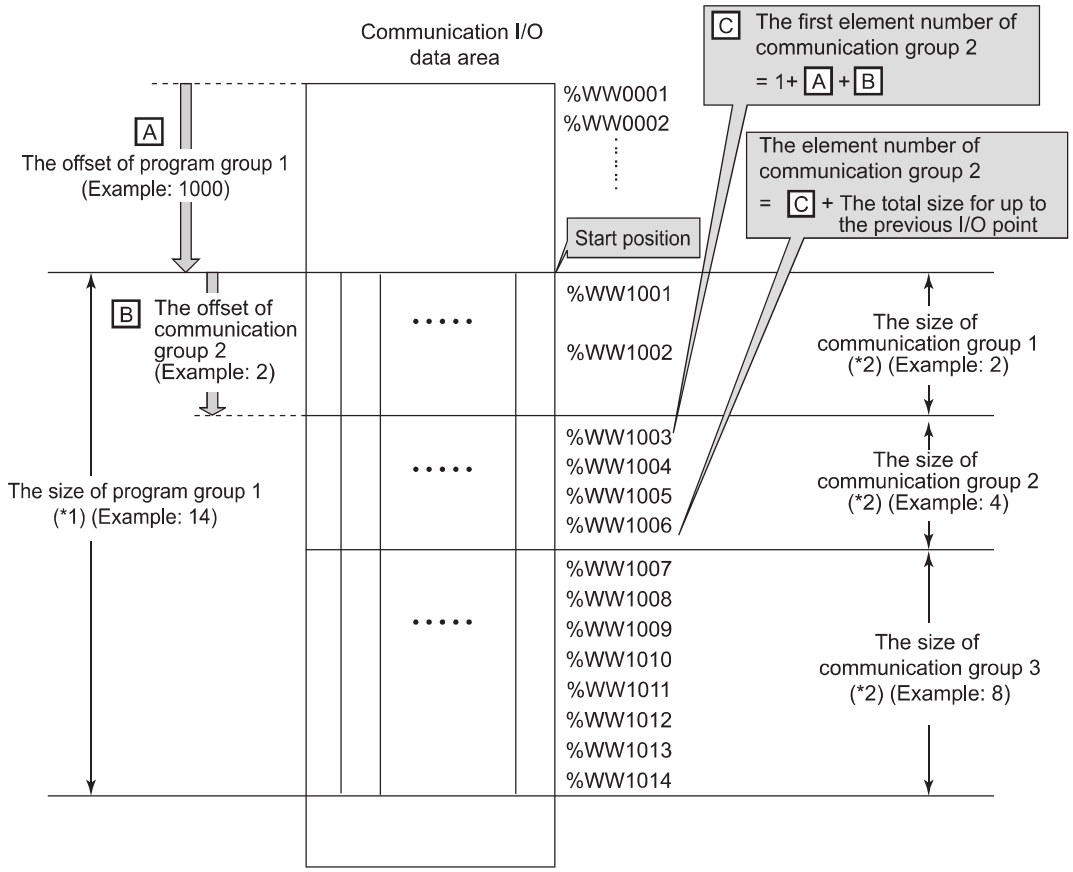


Figure D2.5.1-1 Overview of communication definitions

Element numbers in the communication I/O data area

The following figure shows an example of the assignment of element numbers in the communication I/O data area.



*1: The total size for the communication groups assigned to program group 1
*2: The total size for the I/O points assigned to each communication group

Figure D2.5.1-2 Example of assignment of element numbers in the communication module I/O data area

Flow of definitions for communication with subsystems

Follow these steps when converting I/O information into a data structure that can be communicated with subsystems:

1. Decide the data structure.
2. Assign a communication I/O data area for each subsystem being connected.
   - Define program groups.
   - Define communication groups.
3. Establish the element number of the communication I/O.

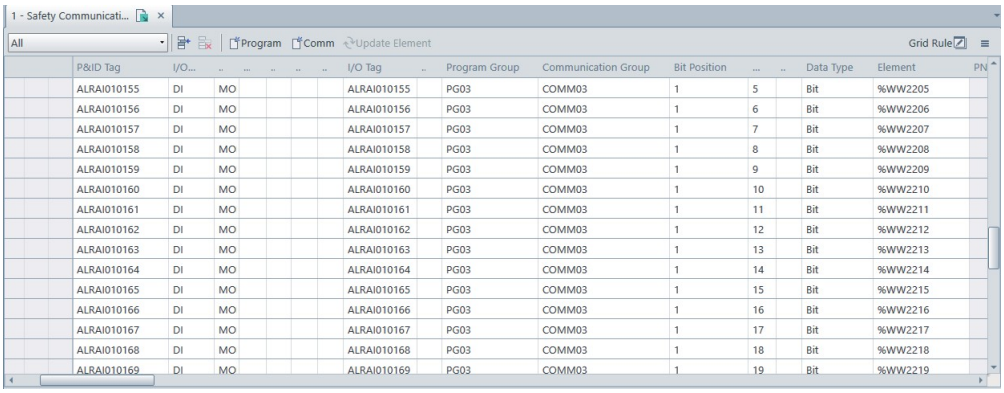
D2.5.2 Deciding the data structure

The data structures obtained from connected subsystems consist of bit-type data and analog-type data. This section describes the definitions of each type of data structure.

Defining the bit-type data structure

Bit-type data is configured of only the I/O points of bit data. Follow these steps to define the structure of this bit-type data:

1. In the signal definition list, enter the same program group name to the Program Group of the I/O points to include in a single set of the bit-type data.
2. In the signal definition list, enter the same communication group name to the Communication Group of the I/O points to include in a single set of the bit-type data.



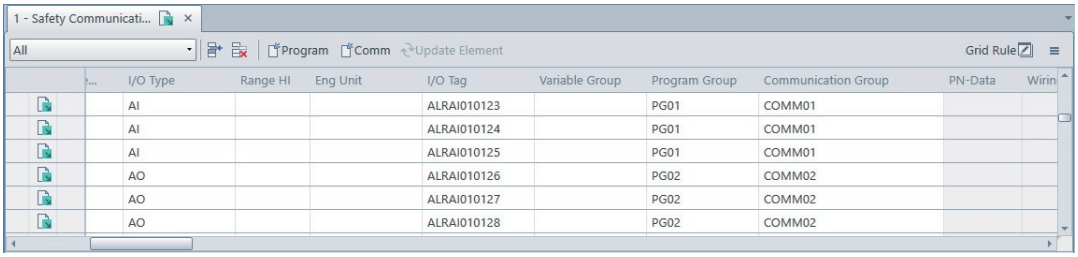
P&ID Tag	I/O...	..	...	..	..	..	I/O Tag	..	Program Group	Communication Group	Bit Position	...	..	Data Type	Element	PN
ALRAI010155	DI	MO					ALRAI010155		PG03	COMM03	1	5		Bit	%WW2205	
ALRAI010156	DI	MO					ALRAI010156		PG03	COMM03	1	6		Bit	%WW2206	
ALRAI010157	DI	MO					ALRAI010157		PG03	COMM03	1	7		Bit	%WW2207	
ALRAI010158	DI	MO					ALRAI010158		PG03	COMM03	1	8		Bit	%WW2208	
ALRAI010159	DI	MO					ALRAI010159		PG03	COMM03	1	9		Bit	%WW2209	
ALRAI010160	DI	MO					ALRAI010160		PG03	COMM03	1	10		Bit	%WW2210	
ALRAI010161	DI	MO					ALRAI010161		PG03	COMM03	1	11		Bit	%WW2211	
ALRAI010162	DI	MO					ALRAI010162		PG03	COMM03	1	12		Bit	%WW2212	
ALRAI010163	DI	MO					ALRAI010163		PG03	COMM03	1	13		Bit	%WW2213	
ALRAI010164	DI	MO					ALRAI010164		PG03	COMM03	1	14		Bit	%WW2214	
ALRAI010165	DI	MO					ALRAI010165		PG03	COMM03	1	15		Bit	%WW2215	
ALRAI010166	DI	MO					ALRAI010166		PG03	COMM03	1	16		Bit	%WW2216	
ALRAI010167	DI	MO					ALRAI010167		PG03	COMM03	1	17		Bit	%WW2217	
ALRAI010168	DI	MO					ALRAI010168		PG03	COMM03	1	18		Bit	%WW2218	
ALRAI010169	DI	MO					ALRAI010169		PG03	COMM03	1	19		Bit	%WW2219	

Figure D2.5.2-1 Bit-type data structure definition

Defining the analog-type data structure

Analog-type data is configured of only the I/O points of the same data type amongst analog I/O data. Follow these steps to define the structure of this analog-type data:

1. In the signal definition list, enter the same program group name to the Program Group of the I/O points to include in a single set of the analog-type data.
2. In the signal definition list, enter the same communication group name to the Communication Group of the I/O points to include in a single set of the analog-type data.



...	I/O Type	Range HI	Eng Unit	I/O Tag	Variable Group	Program Group	Communication Group	PN-Data	Wirin
	AI			ALRAI010123		PG01	COMM01		
	AI			ALRAI010124		PG01	COMM01		
	AI			ALRAI010125		PG01	COMM01		
	AO			ALRAI010126		PG02	COMM02		
	AO			ALRAI010127		PG02	COMM02		
	AO			ALRAI010128		PG02	COMM02		

Figure D2.5.2-2 Analog-type data structure definition

D2.5.3 Defining program groups

By defining program groups, you can configure I/O information for each connected subsystem. A maximum of 12 program groups can be defined. The breakdown is as follows:

- Up to 4 subsystem communication I/O (Models: ALR111M/ALR121M/ALE111M) groups
- Up to 8 safety subsystem communication (Model name: S2LP131) groups

Follow these steps to define the program groups:

1. Click [Program] on the tool bar of Safety Communication I/O Editor.
   The program group set with Program Group of the signal definition list is added to the program group definition list, and the I/O information is configured for each connected subsystem. At this time, the default value for Size is 2 while the default value for Offset is blank.

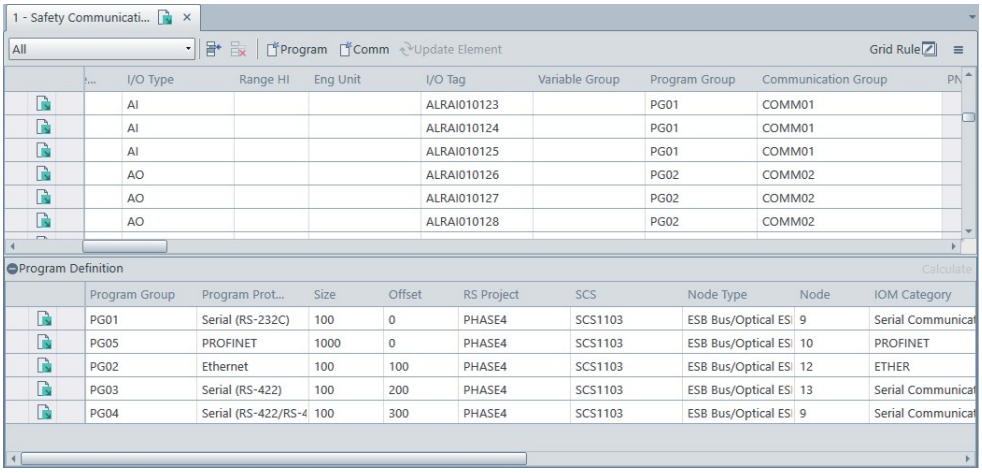


Figure D2.5.3-1 Program group definition

2. On the tool bar of AD Organizer, click [Save].

SEE ALSO For more information about setting items of the program group definition list, refer to:

"■ Setting items of Safety Communication I/O Editor" on page D2-8

D2.5.4 Defining communication group

By defining communication groups, you can configure I/O information for each set of communication definition data. Follow these steps to define the communication groups:

1. Click [Communication] on the tool bar of Safety Communication I/O Editor.
   The communication group set with Communication Group of the signal definition list is added to the communication group definition list and the I/O information is configured for each set of communication definition data. At this time, the default value for Size is 1 while the default value for Offset is 0.

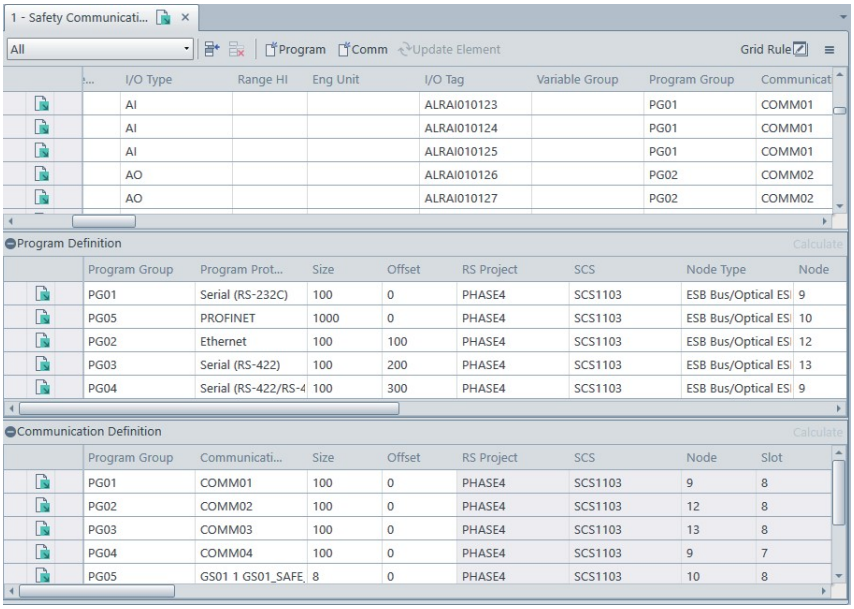


Figure D2.5.4-1 Communication group definition

TIP

The maximum number of communication groups that can be assigned to a single program group is as follows:

- 128 per program group for program protocols other than PROFINET
- With SCSP3, program groups for the PROFINET protocol can be defined in addition to the above making the maximum 200 per program group

2. On the tool bar of AD Organizer, click [Save].

SEE ALSO

For more information about setting items of the communication group definition list, refer to:

"■ Setting items of Safety Communication I/O Editor" on page D2-8

D2.5.5 Fixing the element numbers of the communication I/O

After defining or editing the basic information, I/O module assignment information, and data structure information with the signal definition list, you must fix the element numbers of the communication I/O.

IMPORTANT

- After defining RS Project and SCS of the I/O points for which to fix element numbers with the signal definition list, start Safety Communication I/O Editor by selecting the target SCS in the System Structure Navigator.
- When Fix Element of the signal definition list is set to [Yes], I/O information cannot be changed. If you want to change the I/O information, change Fix Element to [No].

Follow these steps to decide the element numbers of communication I/O:

1. Click [Calculate] on the communication group definition list.
   The size of the communication group is calculated and appears under Size in the communication group definition list.
2. Check Size in the communication group definition list and enter the size of the communication group under Offset.
3. Click [Calculate] on the program group definition list.
   The size of the program group is calculated and appears under Size in the program group definition list.
4. Check Size in the program group definition list and enter the size of the program group under Offset.
5. Click [Update Element] on the tool bar of Safety Communication I/O Editor.
   The consistency of the I/O information is checked and element numbers of the communication I/O are set.

TIP

When Fix Element of the signal definition list is set to [Yes], the element numbers of the communication I/O become fixed.

SEE ALSO

For more information about setting items of the safety communication I/O list, refer to:

"■ Setting items of Safety Communication I/O Editor" on page D2-8

D2.5.6 Procedure for creating and wiring communication I/O variables

A communication I/O is wired to an instance of a subsystem communication I/O FB or fire and gas communication FB. The FB instance is defined as a global variable, local variable, or parameter of a user-defined FB instance.

Global variables are defined by using Safety Communication I/O Editor of AD Organizer and can be created when the reflection process is run for the target SCS by using Generation Manager.

I/O Tag in the signal definition of the safety communication I/O list will become the variable name in Dictionary View after reflection onto the SCS project. In addition, this will be the variable name that is wired in Communication I/O Builder.

The description shown in the following table can be used as a method for describing the variable name to be wired.

Table D2.5.6-1 How to describe a variable name

Variable name	Scope	Description
VAR1	Global (*1)	Global variable
VAR2@PROG1	PROG1	Local variable of a function of PROG1
FB01.VAR3	Global (*1)	Parameter VAR3 of instance FB01 of a user-defined function block
FB01.VAR3@PROG1	PROG1	Parameter VAR3 of user-defined FB instance FB01 locally defined to the function of PROG1
FB01.FB2.VAR3	Global (*1)	Parameter VAR3 of instance FB2 of a user-defined FB used within instance FB01 of a user defined FB (limit for nesting of FB)

*1: In order to handle variables other than global variables with the safety communication I/O list, the information of the variables and parameters of subsystem communication I/O FB included in the POU created with iDefine or SCS Manager is required. In order to handle this information with the safety communication I/O list, do not describe global variables in the Wiring column of signal definitions.

TIP

The options for the Wiring column are updated upon obtaining information from the iDefine setting file and SCS project at the timings shown below when the safety communication I/O list for an SCS is opened in Safety Communication I/O Editor:

- When the safety communication I/O list is opened
- When Refresh is clicked

When a local variable or user-defined FB instance parameter has been specified in the Wiring column of the signal definition, Generation Manager does not create a global variable described in the I/O Tag column. Local variables or user-defined FB instance parameters created with iDefine or SCS Manager are used. Variables defined with iDefine cannot be edited with SCS Manager.

Variables other than global variables are applied to communication definitions using the applicable communication module in Safety Communication I/O Editor. The applicable variables and parameter types are the FB for the communication of each.

These variables and FB parameters can be wired to communication I/O by defining Wiring of Signal Definition in the Safety Communication I/O Editor.

This section describes the work flow for creating all FB instances as global variables and wiring them to communication I/Os, then wiring some of the communication I/Os to local variables or FB parameters.

1. The default value for Wiring of the signal definition is [(Global)]. Select [(Global)] for Wiring of the signal definition, and then run the reflection process with Generation Manager. Global variables are created in Dictionary View with the variable names specified in I/O Tag.

   If Element is set, the relevant variable is set in Variable Name for the specified data area on the Comm. I/O Wiring tab of Communication I/O Builder.

TIP

The options for Wiring are updated upon obtaining information from the iDefine setting file and SCS project at the timings shown below when the safety communication I/O list for an SCS is opened in Safety Communication I/O Editor:

- When the safety communication I/O list is opened
- When [Refresh] is clicked

2. Create local variables and parameters of user-defined FB instances with SCS Manager or iDefine, and import the iDefine-config file containing the definitions to AD Organizer. The local variables and parameters of user-defined FB instances are displayed in Wiring.
3. Select the local variable or the parameter of a user-defined FB instance you want to wire.

IMPORTANT

Wiring is editable when Safety Communication I/O Editor is started for a selected SCS. When the editor is started upon selecting I/O-list or RS project, Wiring is read-only.

4. Using Generation Manager, run the reflection process.
   The global variables that you created in step 1 are deleted.

   If Element is set, the local variable or parameter of a user-defined FB instance specified in Wiring is set in Variable Name for the specified data area on the Comm. I/O Wiring tab of Communication I/O Builder.

D2.6 Importing I/O information into the safety communication I/O list

You can import a list of I/O information obtained from a plant designer into the safety communication I/O list. When the list of I/O information contains program group definitions and communication group definitions, these are imported as well.

TIP

You can import I/O information into the safety communication I/O list when Communication I/O Editor is started for each P&ID group.

Import file format

Create the file to be imported in the following format:

- File format
  .xlsx file for Microsoft Excel
- Sheet name
  Set a name of your choice.
- Sheet description
  Lines of setting item names and I/O information corresponding to these items must be entered. Enter one line of I/O information at a time for each type of I/O information. The following shows an example of the content of the sheet.

Types of I/O information

Names of setting items in the I/O information list (Header row of the list to be imported)

		A	B	C	D	E	...	BQ	BR	...	DD	DE	...	DP
1			Management Information		Common Information		Communication I/O definition Information	Reference Information (Not RS Generation)				I/O List Label		
2	ROW_TYPE		Area	P&ID Sheet	P&ID Tag	I/O Type	···	UDC1	UDC2	···	UDC40	P&ID Group	···	F_Par_CRC
3			XXX	XXX	XXX	XXX	···	XXX	XXX	...	XXX	XXX	···	XXX
4	SG		XXX	XXX	XXX	XXX	···	XXX	XXX	···	XXX	XXX	···	XXX
5	PG						···			...			···	
6	CG						···			...			···	XXX

I/O information of different types of I/O information

Figure D2.6-1 Example of sheet description

The following table shows the input values corresponding to the types of I/O information.

Table D2.6-1 Types and input values of I/O information

Type of I/O information	Input value
Signal definition	SG or blank
Program group definition	PG
Communication group definition	CG

TIP

When a value other than SG, PG, or CG is entered in ROW_TYPE, the type of I/O information being imported will be interpreted as signal definition.

SEE ALSO

For more information about types of I/O information, refer to:

D2.5, “Converting I/O information into a data structure that can be communicated with subsystems” on page D2-21

Importing the I/O information list

You need to prepare the I/O information file in the xlsx format of Microsoft Excel. Follow these steps to import the I/O information file in the xlsx format for Microsoft Excel:

1. Click [Sub menu] in Safety Communication I/O Editor and select [Import].
   The Import wizard appears.
2. In the field for File, specify the file in the xlsx format of Microsoft Excel containing the I/O information to be imported.
   Sheet Name shows the sheet name of the I/O information list, Header Row Position shows the row number in which the setting item is entered, and Target P&ID Group shows the P&ID group name that is included in the I/O information list.

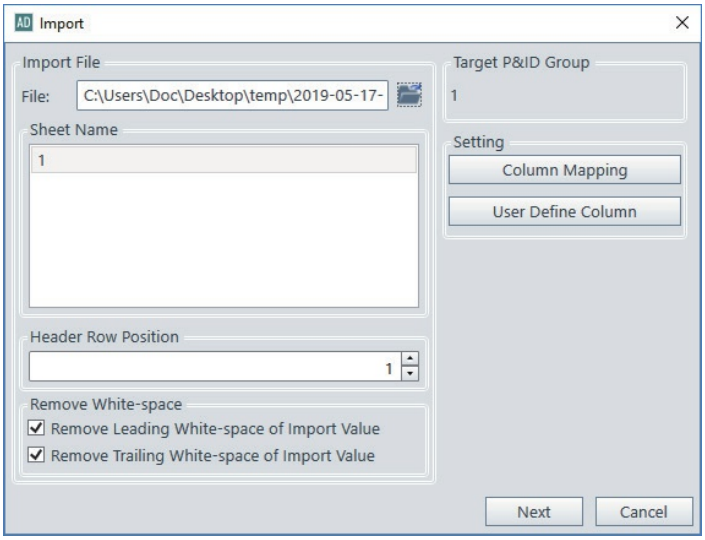


Figure D2.6-2 Import wizard

3. Select the sheet to be imported in Sheet Name.
4. Enter the row number in which the setting item is entered in Header Row Position.
5. Set the following details in Settings if necessary. More specific instructions are given later.
   - If the setting item of the I/O information list to be imported does not match the setting item of the signal definition list, click [Column Mapping] to map the setting items.
   - If the setting item of the I/O information list to be imported cannot be mapped to the setting item of the signal definition list, click [User Define Column] and, after adding the new setting item to the communication I/O list, perform the mapping to these new items.
6. Select the [Remove Leading White-space of Import Value] or [Remove Trailing White-space of Import Value] check boxes optionally.
7. Click [Next].
   The screen will switch to the Comparison and Setting screen.
8. Select either [All Check (Add/Update/Delete)] or [Part Check (Add/Update)].
   All the rows in the list of I/O information are imported.

   If you have selected [All Check (Add/Update/Delete)], the rows that are not available in the I/O information list are deleted from the safety communication I/O list.

   If you have selected [Part Check (Add/Delete)], the rows that are not available in the I/O information list are not deleted from the safety communication I/O list.
9. Click [Finish].
   The I/O information list is imported, and the safety communication I/O list is checked out.

Mapping the setting items of the I/O information list to the setting items of the signal definition list

The procedures are the same as mapping of the safety I/O list.

SEE ALSO For more information about procedures for mapping the safety I/O list, refer to:

- "■ Mapping the setting items of the I/O information list to the setting items of the safety I/O list" on page D1-17
- "■ Modifying the mapping information in AD Organizer that has been upgraded to version R4.05 or later" on page D1-18

For more information about importing and exporting mapping information, refer to:

- "■ Exporting mapping information" on page D1-18
- "■ Importing mapping information" on page D1-18

Reflecting the I/O information upon comparing the information from before and after the import

The procedures are the same as with Safety I/O Editor.

SEE ALSO For more information about comparing the safety communication I/O lists from before and after an import, and reflecting the list , refer to:

D1.4.3, "Comparing and reflecting the I/O information before and after import" on page D1-19

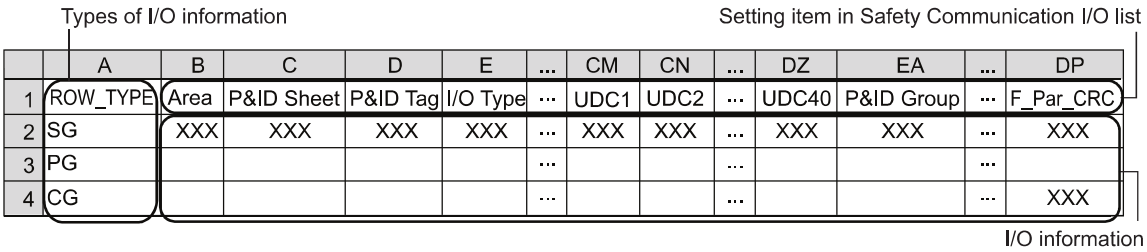
D2.7 Exporting the I/O information in the safety communication I/O list

You can export the information of the safety communication I/O list by operating Safety Communication I/O Editor.

Export file format

The exported file is created in the following format.

- File format
  .xlsx format of Microsoft Excel
- Sheet name
  It will be the P&ID group name.
- Sheet description
  Lines of setting item names and I/O information corresponding to these items will be exported. One line of I/O information is exported for each type of I/O information.



	A	B	C	D	E	...	CM	CN	...	DZ	EA	...	DP
1	ROW_TYPE	Area	P&ID Sheet	P&ID Tag	I/O Type	···	UDC1	UDC2	···	UDC40	P&ID Group	···	F_Par_CRC
2	SG	XXX	XXX	XXX	XXX	···	XXX	XXX	...	XXX	XXX	···	XXX
3	PG					···			...			···	
4	CG					···			...			···	XXX

Figure D2.7-1 Sheet description

TIP

If you assign an alias to a user-defined column, the Setting item in Safety Communication I/O list that corresponds to the user-defined column becomes an alias.

The following table shows the relationship between the values of ROW_TYPE and the types of I/O information.

Table D2.7-1 Values of ROW_TYPE and types of I/O information

ROW_TYPE value	Type of I/O information
SG	Signal definition
PG	Program group definition
CG	Communication group definition

D2.8 Saving and checking in the safety communication I/O list

You can save and check-in the safety I/O list. By performing this operation, the safety communication I/O list is stored in the AD project.

Saving the safety communication I/O list

Follow these steps to save the safety communication I/O list:

1. Select Safety Communication I/O Editor.
2. On the tool bar of AD Organizer, click [Save].

TIP

- When the I/O module assignment information of the safety communication I/O list is edited, the safety communication I/O list (Comm_I/O) under the SCS of the assignment destination is automatically checked out and the content of the definition is reflected.
- When the Safety Communication I/O Editor is in the Deviation mode, you cannot save the safety communication I/O list.

Performing check-in of the safety communication I/O list

By using the Check-in window, check in the defined safety communication I/O list.

The icon shown for the item of [Checked-out Status] in the safety communication I/O list changes.

SEE ALSO For more information about operations for a check-in, refer to:

D2.8, “Saving and checking in the safety communication I/O list” on page D2-34

D2.9 Engineering after changing the safety communication I/O list

The user can proceed with the engineering by using the safety communication I/O list before the I/O information is fixed. Once the information is fixed, the changes can be reflected in the engineering data by loading the updated safety communication I/O list at a later stage.

If the safety communication I/O list is modified, you need to load the safety communication I/O list into Safety Communication I/O Editor, check the differences, and reflect them onto the database.

After the safety communication I/O list is imported, you need to use IOM Definition Editor to define the IOM.

After the changes are reflected to the SCS project, you must return to the previous step of engineering and proceed with the task according to the updated details.

D3. Input/output module configuration definition

The process of determining the IOM arrangement in SCS and the channel arrangement of IOM based on the I/O information list from the plant designer is referred to as I/O module assignment.

By using AD Organizer, you specify the SCS node and IOM relevant to each P&ID tag and their connection information based on the information that is displayed in Safety I/O Editor or Safety Communication I/O Editor.

For defining the I/O module configuration, the IOM Definition Editor is used to set the properties of the node and the I/O module (referred to as IOM).

The following types of properties are set.

- Node properties
- Basic IOM properties
  - IOM type
  - RS project name
  - Station name
  - Node number
  - Slot number
  - Other properties (redundancy, IOM comments, output type etc.)
- Advanced properties for each IOM type

D3.1 Overview of the node and I/O module creation

By using the IOM Definition Editor, you can assign nodes to the specified SCS, or assign I/O modules to the specified node. You can perform the following tasks with the IOM Definition Editor:

- Creating nodes and I/O modules based on the safety I/O list or safety communication I/O list
- Creating nodes and I/O modules without using the safety I/O list or safety communication I/O list
- Editing the node and I/O module

After creating nodes and I/O modules, save and check in them.

D3.2 Starting the IOM Definition Editor

Depending on the operation purpose, the method to start the IOM Definition Editor varies.

- Perform one of the following operations to start the Safety I/O Editor:
  - When creating or editing nodes and I/O modules of an RS project, right-click the target RS project in the System Structure Navigator and select [IOM Definition Editor].
  - When creating or editing nodes and I/O modules of an SCS, right-click the target SCS in the System Structure Navigator and select [IOM Definition Editor].
  - When editing a node, double-click [Node_definition] under the I/O module folder in the System Structure Navigator.
  - When editing a node, double-click [IOM_definition] under the I/O module folder in the System Structure Navigator.

  The IOM Definition Editor appears in the document window area of AD Organizer.

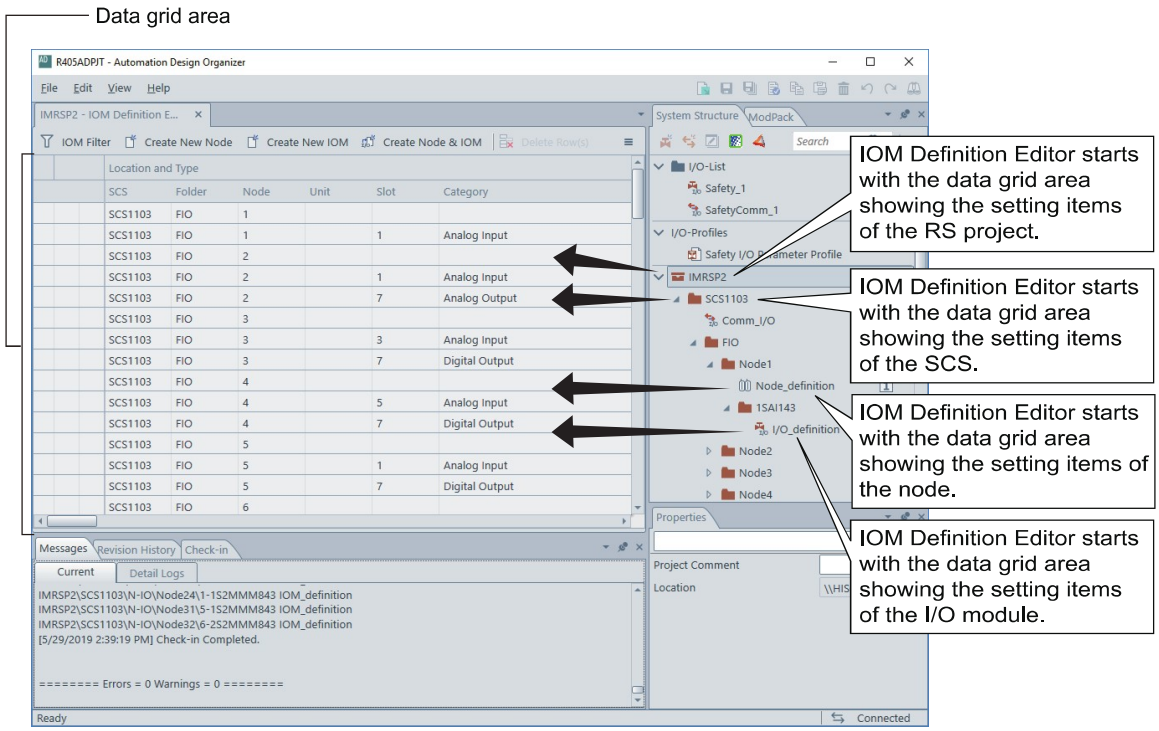


Figure D3.2-1 IOM Definition Editor

TIP

When the IOM Definition Editor is started, the source for which you have started the editor appears in the window title.

D3.3 Displaying for each specified setting item

You can switch the display of the data grid area of the IOM Definition Editor for each specified setting item. You need to perform the following operations to switch the display.

1. Click the [IOM Filter] button on the IOM Definition Editor tool bar.
   The Property Group Selection dialog box appears.

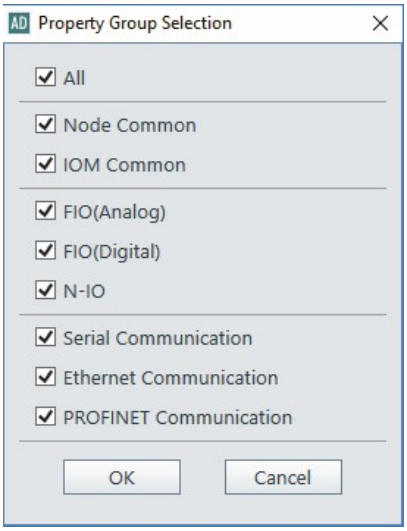


Figure D3.3-1 Property Group Selection dialog box

2. Select the check box of the setting item that needs to be displayed in the data grid area, and click the [OK] button.
   Only the selected setting item is displayed in the data grid area.

D3.4 Creating the node and I/O module

There are two ways to create the node and I/O module.

- Creating the node and I/O module based on safety I/O list
  You need to create the node and I/O module after defining the I/O module assignment information.
- Creating nodes and I/O modules without using the safety I/O list and safety communication I/O list
  You need to define the I/O module assignment information in the safety I/O list and safety communication I/O list after creating the nodes and I/O modules.

TIP

It is necessary to manually enter the settings of SEC401, SEC402, L1EC401, L1EC402, S2EN402, S2EN404, and the communication module based on the node settings.

It is also necessary to create the CPU node (FIO node number 1) manually even if you are creating nodes and I/O modules based on the safety communication I/O list.

Creating the node and I/O module based on safety I/O list

Follow these steps to create the node and I/O module based on the safety I/O list:

1. Click the [Create Node & IOM] button on the IOM Definition Editor tool bar.
   The Create Node & IOM window appears, and the I/O module assignment information is displayed in the list.

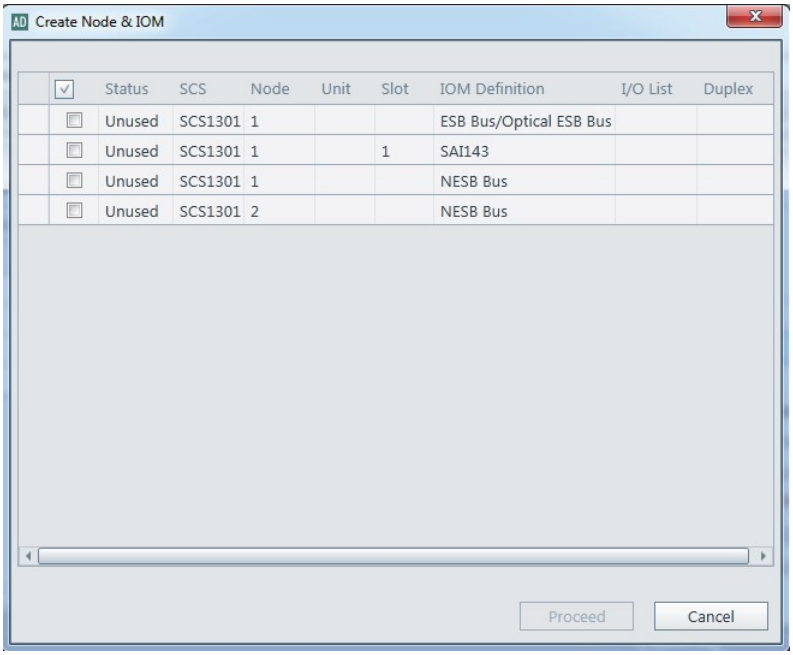


Figure D3.4-1 Create Node & IOM window

2. Select the check box of the assignment information of the node and I/O module that are to be created or deleted, and click [Proceed].
   The SCS name, node type, node number, slot number, unit number, I/O module category, and the I/O module type that are defined in the safety I/O list are assigned, and the node and I/O module are created.

   The node and I/O module that are created are added to the data grid area of the IOM Definition Editor.

TIP

- You can check whether the assignment information of the node and I/O module that are to be created is defined in the safety I/O list or not in Status.
- If the I/O module assignment information is defined in the safety I/O list, New is displayed. If the I/O module assignment information is not defined in the safety I/O list, and if the node and I/O module are created manually by using the IOM Definition Editor, Unused is displayed.
- When the check box of the assignment information of the node and I/O module, whose Status is Unused, is selected, and the [Proceed] button is clicked, the specified node and I/O module are deleted.

Setting items and status when creating nodes and IOMs based on the safety I/O list

The following table describes the setting items for creating nodes and IOMs based on the safety I/O list.

Table D3.4-1 Setting items for creating nodes and IOMs based on the safety I/O list

Setting item	Description
SCS	Location information of node or IOM
Node	Location information of node or IOM
Unit	Location information of node or IOM (Only N-IO)
Slot	Location information of node or IOM
IOM Definition	Detailed description is displayed in the tool tip
I/O List	Signal type of I/O
Duplex	Yes, for redundant Blank, for non-redundant

The following table describes the status when creating nodes and IOMs based on the safety I/O list.

Table D3.4-2 Status of the Create Node & IOM window

Status	Description
New	The I/O module assignment information is defined in the safety I/O list
Unused	The I/O module assignment information is not defined in the safety I/O list, and the node and I/O module are created manually by using the IOM Definition Editor

Creating a node

Follow these steps to create a node without using the safety I/O list:

1. Click the [Create New Node] button on the IOM Definition Editor tool bar.
   The Create Node dialog box appears.

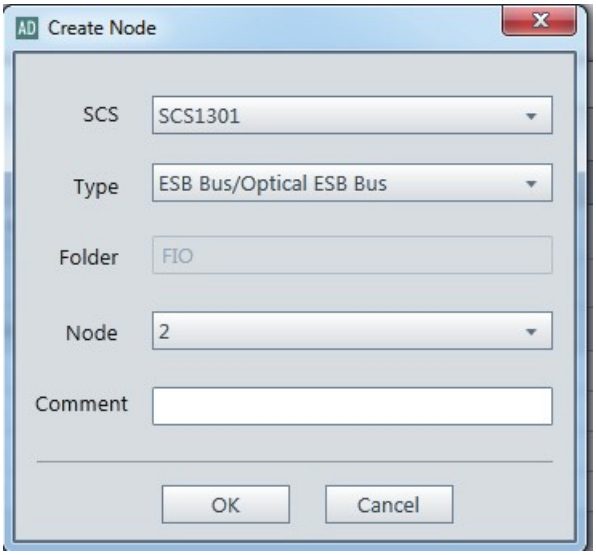


Figure D3.4-2 Create Node dialog box

2. Click the [OK] button after entering the setting items.
   The Create Node dialog box closes, and the node is added to the data grid area of the IOM Definition Editor.

Creating an I/O module

Follow these steps to create an I/O module without using the safety I/O list:

TIP

It is necessary to manually enter the settings of SEC401, SEC402, L1EC401, L1EC402, S2EN402, S2EN404, and the communication module based on the node settings.

1. Click the [Create New IOM] button on the IOM Definition Editor tool bar.
   The Create IOM dialog box appears.

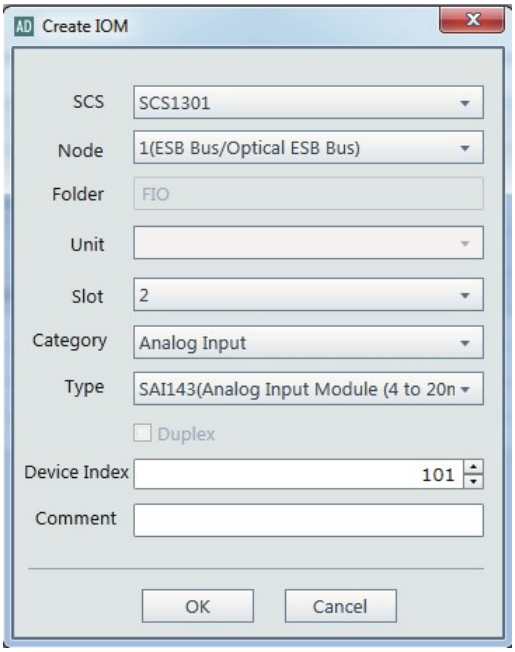


Figure D3.4-3 Create IOM dialog box

TIP

When [Duplex] check box is selected, the adjacent slot is occupied when the I/O module is created.

The initial values of [Device index] appear based on the node number, unit number, and slot number of the I/O module. The rules are as follows according to the I/O module type. The unit number of the I/O module installed in the FIO node is always 0.

- For FIO
  Rule: Node number + 0 + Slot number
  Example: For the module in node 10, slot 1: 1001
- For N-IO
  Rule: Node number + Unit number + Slot number
  Example: For the module in node 1, unit 1, slot 1: 111

An error occurs if you define duplicate values from other I/O modules as the device index.

2. Click the [OK] button after entering the setting items.
   The Create IOM dialog box will close, and the I/O module is added to the data grid area of the IOM Definition Editor.

Setting items when creating nodes and I/O modules without using the safety I/O list or safety communication I/O list

The types of I/O modules that you can add vary depending on the type of the node.

The following table shows the relationship between the SCS type and the node that can be added.

Table D3.4-3 Relationship between the SCS type and the node that can be added

Node type	Type of SCS (*1)					
	S2SC70x		L1SC70x	SSC60x	SSC50x	SSC57x
	FIO	N-IO	FIO	FIO	FIO	FIO
SNB10D	Yes	No	No	Yes	Yes	Yes
L1NB10D	No	No	Yes	No	No	No
S2NN30D	No	Yes	No	No	No	No

*1: Yes: Can be added.
No: Cannot be added.

The following table describes the setting items for creating a node.

Table D3.4-4 Setting items for creating a node

Setting item	Description
SCS	Name of the SCS in which the node is installed
Type	Type of the node that is added Set ESB Bus/Optical ESB Bus, or N-ESB Bus
Folder	IOM folder Set FIO, or N-IO
Node	Node number
Comment	Node related comments

The following table describes the setting items for creating an I/O module.

Table D3.4-5 Setting items for creating an I/O module

Setting item	Description
SCS	Name of the SCS in which the node is added
Node	Node number

Continues on the next page

Table D3.4-5 Setting items for creating an I/O module (Table continued)

Setting item	Description
Folder	Name of the folder in which the node is installed
Unit	Unit number
Slot	Slot number
Category	Category of the IOM that is added
Type	Type of the IOM that is added
Duplex	Make the adjacent IOM dual redundant
Device index	Device index of IOM
Comment	Node related comments

D3.5 Editing the setting items of the node and I/O module

Follow these steps to edit the setting items of the node and I/O module:

1. In the IOM Definition Editor list, double-click an editable cell.
   A dialog box appears, asking you to confirm the check-out.
2. Click [Yes].
   The corresponding node definitions and I/O module definitions are checked out, and check-out icons appear in the list.
3. In the cells of the IOM Definition Editor list, enter the values of the setting items of the node and I/O module.

TIP

If you select one or multiple columns of the device index, right-click, and select [Reset to Default], the values are reset to the initial values of the device index. The values of the node, unit, and slot on which the I/O module is installed are reflected on the initial values of the device index.

4. The Duplex setting of I/O modules must match the setting in the safety I/O list. To change the Duplex setting of the I/O module in the IOM Definition Editor, follow these steps:
   a. In the System Structure Navigator, select a file under the I/O-List folder and start the Safety I/O Editor. Clear [RS Project] of the definitions for which you want to change the Duplex setting and perform a check-in.
   b. In the list of the IOM Definition Editor, select the row of the target I/O module, change the [Duplex] setting, and then perform a check-in.
   c. In the System Structure Navigator, select a file under the I/O-List folder and start the Safety I/O Editor. Restore the [RS Project] that you cleared in step a and perform a check-in.

Bulk editing of the IOM definition

The user can perform bulk definition of multiple IOM definition elements by using the design results of Safety I/O Editor or Safety Communication I/O Editor.

Checking/resolving the issues in the I/O module assignment information

You can check the details of the I/O module assignment information by utilizing the check function of the grid rules by using Safety I/O Editor or Safety Communication I/O Editor.

If issues are found in the I/O module assignment information, you can correct the design related details by using Safety I/O Editor or Safety Communication I/O Editor, or create and edit the node and IOM which the design information requests by using IOM Definition Editor.

Generating the I/O module assignment information by using IOM

You need to perform the following procedure.

1. Click the [Create Node & IOM] button on the IOM Definition Editor.
   The generation and update process of the IOM are executed.

   Once the generation and update process of the IOM end, the IOM Definition Editor appears. The default value is applied to the properties of the node and IOM that are created based on the design information.
2. After setting the node and IOM properties, click [Save] in the IOM Definition Editor.
3. Check in the changes from the Check-in window.
   The editing is completed, and the details in the System Structure Navigator are updated.

D3.6 Deleting the node or I/O module

Follow these steps to delete the node or the I/O module:

1. Select the node or the I/O module in the IOM Definition Editor, and click the [Delete Row] button on the IOM Definition Editor tool bar.
   When the node is deleted, the IOM under the node is also deleted. When the IOM is deleted, the information is not deleted from the safety I/O list, and only the IOM data is deleted.
2. Check in the changes from the Check-in window.
   The details in the System Structure Navigator are updated.

D3.7 Exporting information from IOM Definition Editor

The definitions including the hidden columns and rows in IOM Definition Editor are exported to a CSV file.

Exporting the IOM definition information

Follow these steps to export the IOM Definition Editor definition:

1. From the sub menu of the IOM Definition Editor, select [Export].
   The Folder selection dialog box appears.
2. Enter the name of the file to be exported.
3. Specify the save destination and click [OK].

TIP

- If you export while editing, the edited contents are exported.
- While exporting, progress and result of the process is displayed in the Message Window.
- The file is exported in CSV format.

D3.8 Importing information to IOM Definition Editor

You can import the CSV file that you exported from IOM Definition Editor in to IOM Definition Editor. By importing, you can change the properties of existing nodes and I/O modules. You can change the properties only when defining nodes or I/O modules whose values match with those in the following columns: SCS, folder, node number, unit, slot, category, and type.

You cannot add nodes or I/O modules by importing. Also you cannot delete nodes or I/O modules by importing.

Importing the IOM definition information

Follow these steps to import a CSV file:

1. In IOM Definition editor, right-click a row to be imported, and select [Check-out].
2. From the sub menu of the IOM Definition Editor, select [Import].
   The Folder selection dialog box appears.
3. Select the file you want to import, and click [OK].

TIP

While importing, the progress and result of the process is displayed in the Message Window.

D3.9 Saving the node and I/O module and performing check-in

You can save the node and I/O module and perform a check-in. By doing this operation, the node and the I/O module are stored in the AD project.

Saving the node and I/O module

Follow this step to save the node and the I/O module:

- On the tool bar of AD Organizer, click [Save] while the focus is on the IOM Definition Editor.

Checking in the node and I/O module

- In the Check-in window, check in the created node and I/O module.

D4. Overview of RS generation

The reflection process and the SCS project build process are available as part of RS generation.

After creating engineering data by using iDefine, import the iDefine-config file with AD Organizer and check in before running the reflection process.

- Reflection process
  The safety I/O list, safety communication I/O list, and IOM information that were edited in AD Organizer and the iDefine-config file are acquired from the AD Server and converted into an SCS project file (hereinafter referred to as a conversion). Once the reflection process has been successfully completed, the data of the safety I/O list, safety communication I/O list, IOM information, and iDefine-config file are reflected onto the SCS database.

  The iDefine-config file is obtained when engineering is performed using iDefine.

- Build process of the SCS project
  You can run the SCS project build. If the reflection process is required, the build process is run after the reflection process is automatically run. The SCS project build process builds the entire SCS project while including the following engineering data in addition to the setting items related to the safety I/O list, safety communication I/O list, and IOM information:

  - Function blocks edited with SCS Manager or other builders
  - Subsystem settings
  - Engineering data in the iDefine-config file

  Be sure to perform the build process of the SCS project when downloading the data to SCS.

The target information for RS generation is as follows:

- Safety I/O list created by the Safety I/O Editor
- Safety communication I/O lists created with Safety Communication I/O Editor
- IOM information created by the IOM Definition Editor
- iDefine-config file

The related builders are as follows:

- Dictionary View (Variable)
- I/O Wiring View
- I/O Parameter Builder
- Tag Name Builder
- Link Architecture View
- Multi-Language Editor
- Communication I/O Builder

D4.1 Reflection process

Conversion and import are performed as part of the reflection process.

Conversion

When engineering is performed with the safety I/O list, safety communication I/O list, IOM information, and iDefine from AD Server, the iDefine-config file is also obtained and the file that is to be entered in SCS Manager and the builders is generated.

In the conversion process, you can perform the column check related to the FieldMate Validator or check the items added to the current setting information.

Column check related to the FieldMate Validator

You can check the details of the columns related to the FieldMate Validator of the safety I/O list. When the FieldMate Validation Status and Overwrite Status turn to the following, warning appears.

FieldMate Validation Status is Assigned, or Overwrite Status is Updated

The warning shows the channel in question. The user can verify the details and proceed with the conversion.

Checking added items in the Dictionary view

You can check the current setting information. If the user has defined the same variable name as the additional item, it will result in error. The following message appears and the check is terminated.

Dictionary View: Same variable name exists. (Variable name: xxxx)

Import

You can import the converted file to SCS Manager and the builder.

The contents that were defined in AD Organizer and iDefine are reflected in SCS Manager and the builders. During the import process, the operation history and changed files are not saved.

D4.2 Build process of the SCS project

The SCS project build process obtains the safety I/O list, safety communication I/O list, IOM information, and the iDefine-config file and then runs a build.

The iDefine-config file is obtained when engineering is performed with iDefine. If a reflection is required, you need to run the build after running the reflection.

If there is nothing in the modified list of Generation Manager, you cannot run the build.

After the build succeeds, you cannot run the reflection process and the build again.

■ Difference between the reflection process and the SCS project build process

The difference between the reflection process and the SCS project build process is that the reflection process does not run the SCS project build.

Even if the IOM definition or the assignment is not completed in AD Organizer, you can create the Program Organization Unit (POU). The reason for this is because it is possible to proceed with the creation of the application logic by using the I/O variables of the safety I/O list and safety communication I/O list.

The I/O variables are reflected onto Dictionary View when the reflection process is performed.

SEE ALSO For more information about items that should be configured in the safety I/O list and safety communication I/O list to run the reflection process, refer to:

"■ Handling of the safety I/O list and safety communication I/O list" on page C2-3

■ Build in Generation Manager and SCS Manager

Both the Generation Manager build and SCS Manager build create a database for SCS, but they have the following differences:

If the build succeeds in Generation Manager, the corresponding safety I/O list, safety communication I/O list, and IOM information of AD Organizer are reflected onto the SCS database via SCS Manager. When the safety I/O list, safety communication list, and IOM information are edited by using AD Organizer, the modifications are not imported into the SCS database. Therefore, it is necessary to perform the build with Generation Manager.

On the other hand, when performing a build by using SCS Manager, the status of the safety I/O list, safety communication I/O list, and IOM information of AD Organizer is not taken into account. When downloading to the SCS, the download cannot be done if the safety I/O list, safety communication I/O list, and IOM information of AD Organizer have not been reflected onto the SCS database. You can run the analyzer and launch the SCS simulator.

Therefore, when the safety I/O list, safety communication I/O list, and IOM information are edited, it is necessary to run the build successfully once in Generation Manager.

D4.3 Generation Manager window configuration

Generation Manager screen is shown in the following figure.

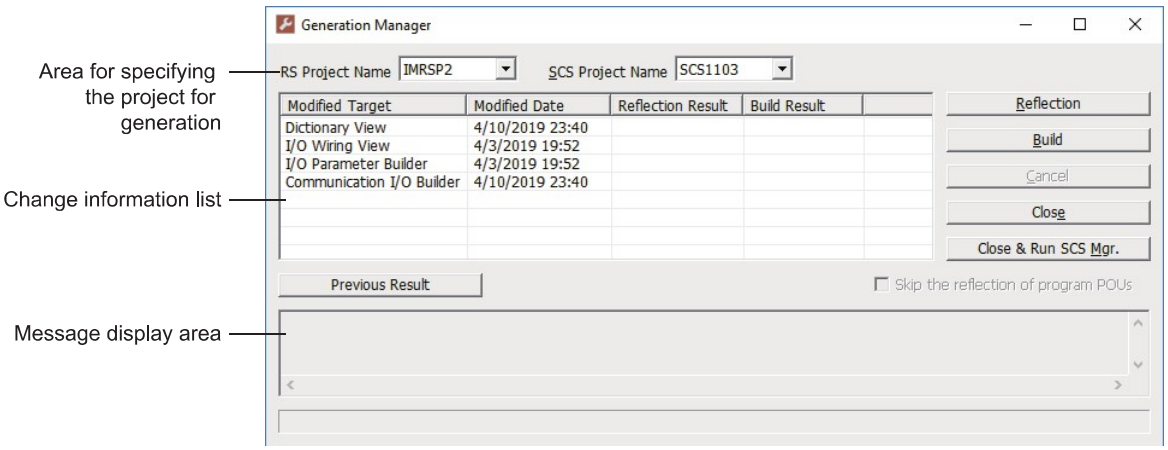


Figure D4.3-1 Generation Manager window configuration

RS project

The target RS project can be selected from the drop-down list box. You can select the RS project that is registered in the AD project.

SCS project

The SCS project that is defined in the RS project can be selected from the drop-down list. The SCS project that is displayed in the list box is the SCS project that is created by using the safety I/O list or safety communication I/O list of AD Organizer from the SCS project properties. The list is displayed in descending order sequence of the domain number and station number. If the RS project is switched in the drop-down list of the RS project, the station at the topmost position in the list will be in the selected state.

Change information list

Only the information related to the SCS project that is selected from the drop-down list box of the SCS project is displayed in the change Information list.

Soon after Generation Manager is started up, the RS project and the SCS project that were selected in the System Structure Navigator during start-up will be in selection status.

The details that are displayed in the change information list is shown in the following table.

Table D4.3-1 Column specification of the change information list

Item name	Description
Modified Target	Displays the name of the build which needs to be changed. When changes need to be made, the builders are shown in the order of Dictionary View, I/O Wiring View, I/O Parameter Builder, Communication I/O Builder, Dictionary View (iDefine), Tag Name Builder, and POU.
Modified Date	The date and time of file update are displayed.
Reflection Result	The results of reflection are displayed. • Succeed: Successful • Fail: Failure
Build Result	The results of the build are displayed. • Succeed: Successful • Fail: Failure

Previous result

The progress status message of the last RS generation is displayed.

Skipping reflection of a program POU

This option is used when the engineering is performed by using iDefine. This option is applicable to SCS projects that use subsystem communication or safety subsystem communication, and you can use the option as necessary when you change the POU included in an SCS for which downloading is already performed.

When the reflection process is performed after loading the iDefine-config file with AD Organizer, changes made to the POUs, variables, FB instances, and tag name information are all reflected together onto the SCS project.

For example, if any changes are made to a user-defined FB that uses a subsystem communication FB, you may want to download only the changed user-defined FB and the changes in the relevant subsystem communication to the SCS first and check the operation of the FB by using the program POU that is already downloaded.

In this case, when the reflection process is performed upon selecting this check box, changes will be reflected onto the SCS project except for the changes in the program POU and tag names in the iDefine-config file. However, even if user-defined FBs or user-defined FUs are deleted in iDefine, they will not be deleted from the SCS project. This is because, if such FBs or FUs are deleted from the SCS project, a build error will result when the FBs or FUs are used in the program POU that is already downloaded.

After testing of user-defined FBs that use a subsystem communication FB and other subsystem communication related functions is finished, clear the check box and run the reflection and build process again. By doing so, you can reflect all changes that were made with iDefine onto the SCS project.

The following table shows the changes of the status icon for the iDefine Configuration folder shown in System Structure Navigator after selecting the check box or clearing it and performing the build process:

Table D4.3-2 Status icon of the iDefine Configuration folder after the build process

Check box	Status icon after the build process
Selected	The work status is retained even if the build is successful. The work status icon remains shown next to the iDefine Configuration folder of System Structure Navigator. The user can continue to perform the reflection process.
Cleared	The work status icon next to the iDefine Configuration folder of System Structure Navigator disappears when the build process is successful.

Message display area

The message display area displays the execution result of RS generation.

Reflection button

When you click the Reflection button, conversion is run and the converted file is imported to SCS Manager and the builders.

While performing the conversion, the safety I/O list, safety communication I/O list, and IOM information file are acquired before the file for import is created. When engineering by using iDefine, the iDefine-config file is also required.

When importing, the file that was generated through conversion is imported to SCS Manager and the builders. The progress status appears in the message display area.

When there is nothing in the modified information, you cannot run the reflection process.

The successfully converted safety I/O list, safety communication I/O list, IOM information file, and iDefine-config file are imported to SCS Manager and the builders.

If the reflection process fails, you can run the reflection process once again. Run the process from the conversion stage again. When the reflection process is canceled by using the Cancel button, the result will be the same as the case when reflection fails.

- In the reflection process, the input/output modules are wired to the existing input/output variables. A check is then run to make sure that it is consistent with the IOM definition. Regardless of whether it is an input/output variable, the following values are compared in the iDefine-config file and AD Suite:
  - I/O Tag
  - I/O Type
  - Node
  - Unit
  - Slot
  - IOM Type
  - Terminal

  If the value is different, an error dialog box appears and the reflection process is stopped.
- If a tag name is included in the iDefine-config file and a CENTUM VP integration package or a CI Server integration package is not enabled, a message stating that the tag name definition is not reflected appears in the message display area.

Build button

This button runs the SCS project build process. After the reflection process succeeds, the SCS project build process is executed.

The safety I/O list, safety communication I/O list, and IOM information file, as well as the iDefine-config file when engineering by using iDefine, are all acquired from the AD Server, the reflection is performed when it is required, and then the SCS project build is run.

If there is nothing in the change information, you cannot run the SCS project build process.

Cancel button

This button cancels the reflection process and the SCS project build process. It is enabled only when the reflection process and the SCS project build process are executed. If the cancel button is clicked during the execution of the reflection process and the SCS project build process, the reflection process and the SCS project build process will be terminated.

When the cancel button is clicked, [Fail] is displayed in the [Reflection Result] or [Build Result] of the change information.

Once the import to SCS Manager and the build are executed, the cancel button will be disabled.

Close & Run SCS Mgr. button

After RS Generation Manager is closed, SCS Manager automatically starts for the corresponding SCS.

Process when the RS project and SCS project were switched in the RS Generation Manager

When the RS project and SCS project are switched in the Generation Manager dialog box, the screen is refreshed. The safety I/O list, safety communication I/O list, and IOM information file, and the iDefine-config file as well when engineering by using iDefine, of the SCS project that was newly selected are acquired from the AD Server, and the change information list shows which builder requires modifications.

D4.4 Operating procedure of RS generation

The RS generation flow is shown in the following figure.

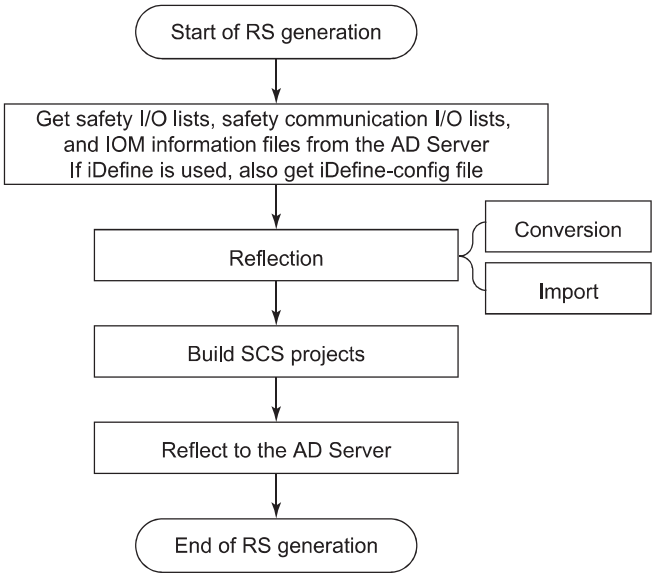


Figure D4.4-1 RS generation process

Starting Generation Manager

1. In the System Structure Navigator of AD Organizer, select SCS.
2. Perform either of the following operations:
   - Right-click and select [RS Generation Manager] from the context menu.
   - Form the sub menu of the System Structure Navigator, select [ProSafe-RS] > [RS Generation Manager].

   Generation Manager starts, and the builder that requires modifications is displayed in the change Information list.

Executing the reflection process

1. You need to select the target RS project and SCS project for RS generation.
2. Check the change information, and click the [Reflection] button.
   If the Access Control and Operation History Management Package is enabled, the Engineer Authentication dialog appears once the import starts.

   If the security of the SCS project is set, the Password Input dialog box appears for the project.
3. Enter the required fields in the Engineer Authentication dialog box and the Password Input dialog box of the SCS project. If the Engineer Authentication and the Password Input dialog boxes do not appear, no action is required.
   The conversion is performed, and the safety I/O list, safety communication I/O list, and IOM information are imported to the AD Server.

   If the reflection process succeeds, Succeed is displayed in Reflection Result.

   If the reflection process fails, Fail is displayed in Reflection Result.

TIP

When the reflection process is performed, you can only use the [Cancel] button.

Reflecting the POU that was defined by using iDefine

When running the reflection process, the POU that was defined by using iDefine is reflected in SCS Manager. The run sequence of the POUs that were defined by using iDefine and SCS Manager is sorted in the Link Architecture View of SCS Manager. POUs that were defined in SCS Manager are not reflected in iDefine. In iDefine, only the run sequence of the POUs that were defined in iDefine is shown.

This section describes the rules for reflecting POUs in SCS Manager after running the reflection process after adding, switching, or deleting POUs in iDefine.

- When POU was added by using iDefine
  POUs that were defined in iDefine and the following POUs that were defined in SCS Manager are treated as a series of the same run sequence; POUs that were added by using iDefine are added below that.

  Example:

  The following example shows how A1, UD1, and UD2 are treated as a series of the same run sequence and A2 is added below that.

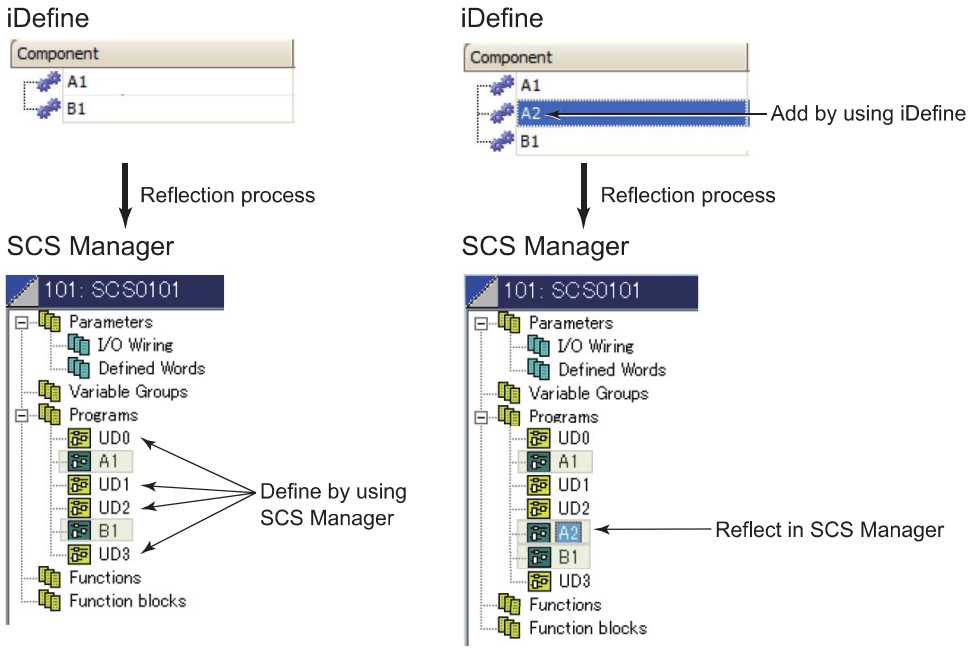


Figure D4.4-2 Reflecting POUs that were added by using iDefine in SCS Manager

- When the POU sequence was changed by using iDefine
  POUs that have had their sequence changed in iDefine and the following POUs that were defined in SCS Manager are treated as a series of the same run sequence, and their sequence in SCS Manager is also changed.

  Example:

  The following example shows how A1, UD1, and UD2, and B1 and UD3 are treated as a series of the same run sequence and how their run sequence is changed.

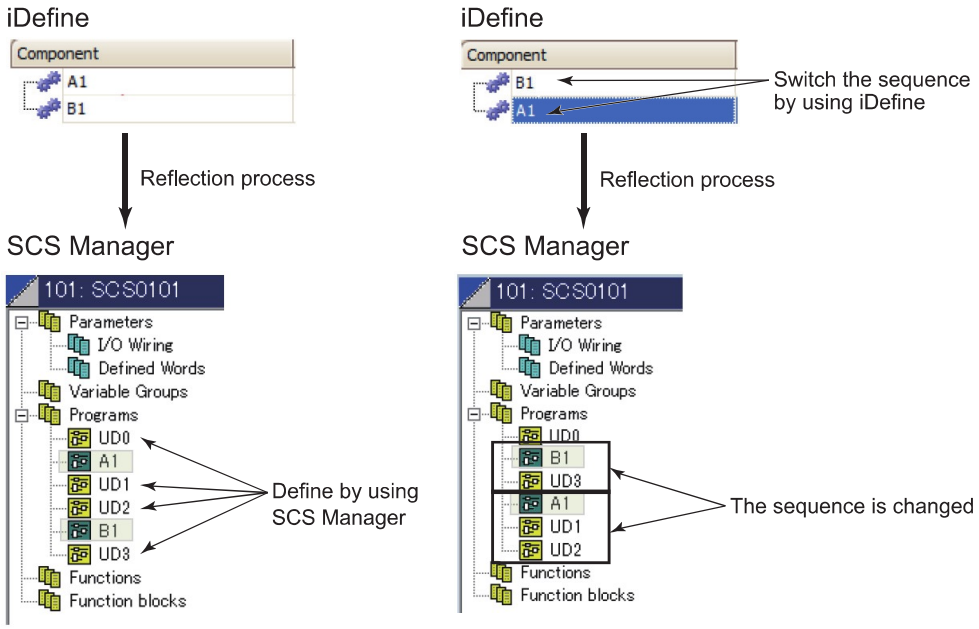


Figure D4.4-3 Reflecting POUs that have had their sequence changed by using iDefine in SCS Manager

- When POU was deleted by using iDefine
  POUs that were deleted by using iDefine are deleted in SCS Manager.

TIP

POUs that were imported from iDefine become read-only in SCS Manager and are displayed with a green icon.

Reflecting the ANN and ANN_FUP tag names that were defined by using iDefine

When running the reflection process, configurations related to the tag names corresponding to the ANN and ANN_FUP instances that were configured by using iDefine are reflected in the Tag Name Builder. Once the instance name has been reflected, it is reflected in the same Element Name in the Tag Name Builder for as long as it exists. New instances that were added by using iDefine are reflected in the unused Element Names in ascending order.

Running the SCS project build process

1. Click the [Build] button in Generation Manager.
   The safety I/O list, safety communication I/O list, and IOM information, as well as the iDefine-config file when engineering by using iDefine, are all acquired from the AD Server, the reflection is performed when it is required, and then the SCS project build process is run.

   The results of the SCS project build process is displayed in the message display area.

   - If the SCS project build process succeeds, Succeed is displayed in Build Result of the change information list. The safety I/O list, safety communication I/O list, IOM information file, and iDefine-config file for which the build is successful are reflected onto the AD Server. You cannot run the reflection process and the build again.
   - If the SCS project build process fails, Fail is displayed in Build Result of the change list. Even if the build fails, the safety I/O list, safety communication I/O list, IOM information, and iDefine-config file are reflected onto SCS Manager as long as the reflection process is successful.

D4.5 Error messages in Generation Manager

This section describes the error messages in Generation Manager.

Error during startup

An error message appears when a communication error occurs during startup. Generation Manager will not start up.

Error during check-out

If the check-out of the safety I/O list, safety communication I/O list, and IOM information file from the AD Server fails when the conversion begins, the name of the file that failed check-out is shown in the message display area.

When a communication error occurs during check-out, the following message is displayed in the message display area.

[Cannot connect to the server.]

Error during unlock

An error message is displayed if a communication error occurs when the reflection process or SCS project build process fails and the check-out is canceled. To release the lock, restart Generation Manager after connecting to the server.

Error during check-in

An error message is displayed if a communication error occurs during check-in to the AD Server after the reflection process and SCS project build process have succeeded. To perform a check-in, restart Generation Manager after connecting to the server.

Error when there is no conversion object

If the reflection button is clicked even though there is nothing in the change information list, the following messages are displayed.

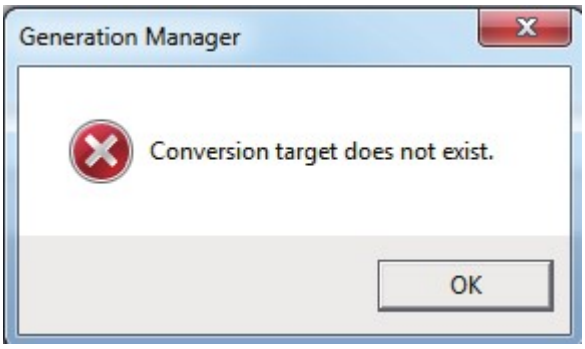


Figure D4.5-1 Error during conversion

After the build has succeeded, this error is displayed when the reflection is performed once again.

Engineer authentication error

When the User Authentication screen of the Access Control and Operation History Management Package appears, and if the engineer group associated with the engineer does not have the required access rights for Dictionary View, I/O Wiring View, I/O Parameter Builder and the

build, the following message appears in the message display area and the reflection process results in an error.

[ERROR: Don't have access right for the operation.]

SCS project security error

If three failed password entry are made for the project in the SCS project security, the following message is displayed in the message display area. Then, the reflection will result in error.

[ERROR: Cannot open the project.]

Error during the reflection process and the SCS project build process

If SCS Manager is started during the reflection process and SCS project build, the following error message is displayed and the processing is terminated.

SCS Manager is being executed.

D4.6 Engineering after changing the safety I/O list and safety communication I/O list

The user can proceed with engineering by using the safety I/O list or safety communication I/O list before the I/O information is fixed. Once the information is fixed, the changes can be reflected in the engineering data by loading the updated safety I/O list or safety communication I/O list at a later stage.

If the safety I/O list is modified, you need to load the safety I/O list into the Safety I/O Editor, check the differences, and reflect them to the database. Once the safety I/O list is imported, you need to use the IOM Definition Editor to define the IOM.

If the safety communication I/O list is modified, you need to load the safety communication I/O list into Safety Communication I/O Editor, check the differences, and reflect them onto the database. Once the safety communication I/O list is imported, you need to use IOM Definition Editor to define the IOM.

When the safety I/O list has been changed, if the engineered results are exported to FieldMate Validator to be tested and are modified, you must import the updated I/O list and reflect the changes onto the SCS project. Once the changes are reflected to the SCS project, you must return to the previous step of engineering and proceed with the task according to the updated details.

D5. Engineering by using iDefine

The following methods are available for engineering by using iDefine:

- Engineering when starting iDefine from AD Organizer
- Engineering when starting iDefine directly

This section describes the engineering steps for each method.

IMPORTANT

When using ProSafe-RS and iDefine, use ProSafe-RS R4.02 to R4.08.

If you want to use SENG to edit engineering data created with iDefine, contact YOKOGAWA.

D5.1 Engineering steps when starting iDefine from AD Organizer

This section describes the engineering steps when starting iDefine from AD Organizer, separately explaining operations in AD Organizer, in iDefine, and in RS Generation Manager.

IMPORTANT

If you are starting iDefine from AD Organizer, install AD Organizer and iDefine on the same computer.

D5.1.1 Operations in AD Organizer

Follow these steps to operate AD Organizer when starting iDefine from AD Organizer:

1. Specify the parameters for input/output and I/O modules.
2. In the System Structure Navigator, click the iDefine for ProSafe-RS icon.
   iDefine starts.

TIP

iDefine starts with the previously loaded iDefine project selected.

IMPORTANT

When performing engineering with starting iDefine from AD Organizer, the iDefine-config file is automatically imported during [Build All] in iDefine. If you want to select an FB with an instance name, do so before running [Build All] in iDefine.

SEE ALSO

For more information about I/O parameter definitions, refer to:

- D1., “Engineering based on the safety I/O list” on page D1-1
- D2., “Engineering based on the safety communication I/O list” on page D2-1

For more information about I/O module parameter definitions, refer to:

D3., “Input/output module configuration definition” on page D3-1

Selecting a FB with an instance name

The instance names of all the FBs that are used in application logics that were created by using iDefine are configured separately. Using this dialog box, you can select whether to assign instance names to the FBs to be reflected in SCS projects for each FB type.

Change the setting to use SCS Manager to assign instance names to any unique FB types that do not have an instance name configured by default or to reduce the number of variables that are registered in the Dictionary View.

Follow these steps to change the settings for FB with an instance name.

1. In System Structure Navigator, right-click with an SCS node selected and select [FB Selection...].
   The FB Selection dialog box appears.

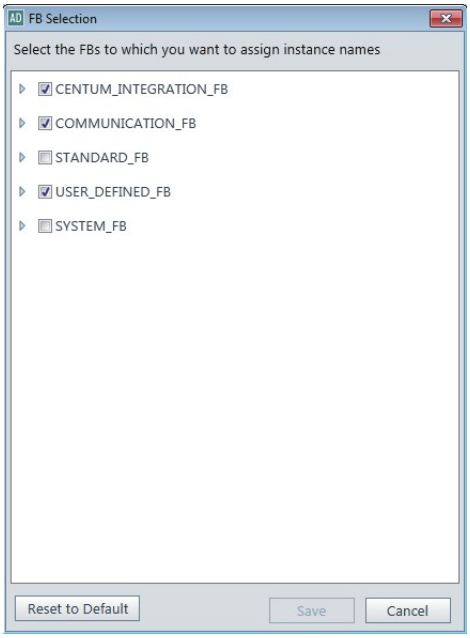


Figure D5.1.1-1 FB Selection dialog box

2. Select the FB with an instance name check box.
   - The function block is categorized; clicking the triangle on the left-hand of a category shows the function blocks contained within that category. You can select all of the check boxes of the function blocks that are contained within a category at the same time by selecting the check box for that category.
   - Clicking [Reset to Default] returns the FB selection status to its initial state.
3. Click [Save].

TIP

The selection of an FB with an instance name can also be done through the Import dialog box.

In the Import dialog box, select the [Show advanced setting] check box and click [Instances].

D5.1.2 Operations in iDefine

Follow these steps to operate iDefine when starting iDefine from AD Organizer:

1. Select an iDefine project and log in.
   iDefine runs in integration mode with AD Suite.

IMPORTANT

iDefine runs in integration mode only if you have started iDefine from AD Organizer. You cannot use the integrated functions of iDefine and AD Organizer if you started iDefine directly.

2. In iDefine Import from AD Suite, select one of the following range for importing I/O and IOM from AD Suite, and import them:
   - Entire AD project
   - RS project
   - SCS project
3. Create an application.
4. In Output Configuration, select the SCS that is the destination for the import of the iDefine-config file, and run [Build] and [Build All].
   Once the iDefine Output Configuration has been built and the iDefine-config file has been imported to AD Organizer successfully, RS Generation Manager starts automatically.

IMPORTANT

- iDefine has an automatic check-in option that runs after creating an iDefine-config file by using [Build All] and importing it to AD Organizer. If you enable this option, you can automatically start RS Generation Manager from iDefine.
- If RS Generation Manager is already running, it cannot be started from iDefine.

SEE ALSO For more information about specific operations in iDefine, refer to:

- iDefine User Guide (PR03076-MAN-970_01)
- iDefine User Guide (Yokogawa Extensions) (PR12002-MAN-980_01)

Creating applications by using iDefine

Follow these steps to create applications by using iDefine:

1. Import the ProSafe-RS I/O file.
   If a value has been entered in the column for iDefine reference, such as Typical, in Safety I/O Editor and Safety Communication I/O Editor, you can view the value for reference purposes in iDefine.
2. Use the following logic editor to create an application template.
   This task can be performed at the same time as the engineering of the I/O list by using AD Organizer, so you can perform this task before importing the ProSafe-RS I/O file.
   - Function Block / Function
   - Typical

   a. In the ProSafe-RS IO Tag Name window, create the parameter pattern for each type to define the tag name.

b. From the variables or function block instances that were defined in Typical, set the created parameter pattern to the one that you wish to assign a tag name.

3. For each I/O Tag, assign the corresponding Typical.
4. Use the following logic editor to create an application logic:
   - Group Typical
   - Cause and Effect module
   - State Analysis module
5. Build by using the Output Configuration and create the variables, tags and an executable program in FBD format.

SEE ALSO For more information about the procedure to import ProSafe-RS I/O files to iDefine, refer to:

10., "IMPORT FROM AD SUITE" in iDefine User Guide (Yokogawa Extensions) (PR12002-MAN-980_01)

D5.1.3 Operations in RS Generation Manager

Follow these steps to operate RS Generation Manager when starting iDefine from AD Organizer:

1. In RS Generation Manager, run the reflection process and the SCS project build process.
2. Click [Close & Run SCS Mgr.].
   RS Generation Manager closes and SCS Manager starts.
3. In SCS Manager, run Safety Analyzer and download to the SCS.
   We recommend that you back up the iDefine project at this step.

SEE ALSO

For more information about RS Generation Manager window configuration, refer to:

D4.3, “Generation Manager window configuration” on page D4-4

For more information about the reflection process and the SCS project build process, refer to:

D4.4, “Operating procedure of RS generation” on page D4-8

For more information about the analysis of SCS projects, refer to:

C5., “Testing with the Safety Analyzers” on page C5-1

For more information about download to the SCS, refer to:

C7., “Offline download to the target SCS” on page C7-1

D5.2 Engineering steps when starting iDefine directly

This section describes the engineering steps when starting iDefine directly.

Engineering is performed in iDefine after creating an iDefine project by using iDefine and using the file exported for iDefine from AD Organizer.

1. Export the ProSafe-RS I/O file from AD Organizer.
2. Import the ProSafe-RS I/O file by using iDefine and create an application. Export the result as an iDefine-config file.
3. Import the iDefine-config file by using AD Organizer. It is recommended that you back up the iDefine project at this step.

SEE ALSO

For more information about the procedures to export files for iDefine from AD Organizer, refer to:

D5.2.1, “Exporting the ProSafe-RS I/O file from AD Organizer” on page D5-9

For more information about the engineering flow when using iDefine, refer to:

C2.2, “Work flow of I/O list engineering with iDefine” on page C2-11

For more information about specific operations in iDefine, refer to:

- iDefine User Guide (PR03076-MAN-970_01)
- iDefine User Guide (Yokogawa Extensions) (PR12002-MAN-980_01)

For more information about tests that are run using iDefine test functions, refer to:

6., “Using iDefine in tests” in Test Function Guide (IM 32P04B30-01EN)

D5.2.1 Exporting the ProSafe-RS I/O file from AD Organizer

If you are using iDefine, export the safety I/O list, safety communication I/O list, and I/O module configurations as a ProSafe-RS I/O file in AD Organizer. The exported file is known as ProSafe-RS I/O file. A ProSafe-RS I/O file is created for each SCS project.

Follow these steps to export the ProSafe-RS I/O file:

If there are any files being edited in Safety I/O Editor, Safety Communication I/O Editor, or IOM Definition Editor, check in the files and export them. Contents that are being edited are not exported.

1. In the System Structure Navigator of AD Organizer, right-click the SCS project to be exported in the System Structure Navigator and select [Safety I/O Editor] or [Safety Communication I/O Editor].

TIP

If you start the Safety I/O Editor in the following ways, you cannot export the ProSafe-RS I/O file.

- Double-clicking the [I/O definition] under the module folder.
- In the Change Set Detail dialog box, right-clicking the file and selecting [Launch Editor] from the context menu.
- Launching the editor in read-only mode.

2. Select [Export to iDefine] from the sub-menu of Safety I/O Editor or Safety Communication I/O Editor.
   The File Selection dialog box appears.
3. Specify the export location, and click [OK].
   The ProSafe-RS I/O file is exported.

TIP

The same data is exported whether you use Safety I/O Editor or Safety Communication I/O Editor. However, different data will be exported depending on what is selected when you start the editor. The relationship between the selection and exported data is as follows:

- When an I/O list is selected
  Safety I/O of all P&ID groups

  Safety communication I/O of all P&ID groups

  Node and I/O module data for all P&ID groups

  Safety I/O parameter profile
- When an RS project is selected
  Safety I/O of all SCSs included in the selected RS project

  Safety communication I/O of all SCSs included in the selected RS project

  Node and I/O module data for all SCSs included in the selected RS project

  Safety I/O parameter profile
- When an SCS project is selected
  Safety I/O of the selected SCS

  Safety communication I/O of the selected SCS

  Node and I/O module data for the selected SCS

  Safety I/O parameter profile

D5.2.2 Operations in iDefine

Follow these steps to create applications by using iDefine:

1. Import the ProSafe-RS I/O file.
2. Use the logic editor to create an application template.
3. For each I/O Tag, assign the corresponding Typical.
4. Use the logic editor to create an application logic.
5. Build by using the Output Configuration and create the variables, tags and an executable program in FBD format.
6. Export the result as an iDefine-config file.

SEE ALSO For more information about creating applications by using iDefine, refer to:

"■ Creating applications by using iDefine" on page D5-5

D5.2.3 Import the iDefine-config file by using AD Organizer

Import the iDefine-config file that was exported from iDefine to AD Organizer. The iDefine-config file contains the POU, I/O Tag, and variables that were defined in iDefine.

Follow these steps to import the iDefine-config file:

1. In the System Structure Navigator of AD Organizer, select the SCS project for which you want to import the file, and select [Import iDefine configuration] from the context menu. The Import dialog box appears.

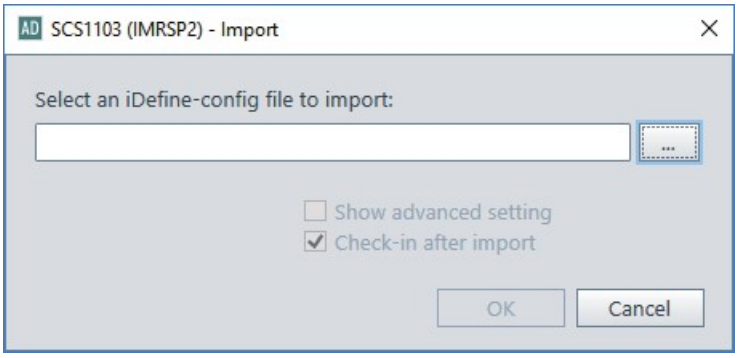


Figure D5.2.3-1 Import dialog box of the iDefine-config file

TIP

If you select an SCS project with a folder that has an exclamation mark, multiple SCS projects, or an SCS project that was created in RS original engineering, you cannot select [Import iDefine configuration].

2. Specify the iDefine-config file that will serve as the import source.
3. Perform either of the following operations:
   - If you do not want to change the settings for FBs with an instance name, skip to step 4.
   - If you want to change the settings for FBs with an instance name, follow the steps described in the next section "■ Selecting a FB with an instance name."
4. In the Import dialog box, click [OK].
   The iDefine-config file is checked out.
5. On the Check-in window, check in the iDefine-config file.
   The iDefine-config file is imported. If you select the [Check-in after import] check box, the iDefine-config file is automatically checked in to AD Server after it has been imported to AD Organizer.
6. Start RS Generation Manager and run the reflection process and the SCS project build process.
7. From AD Organizer, start SCS Manager.
8. In SCS Manager, run Safety Analyzer and download to the SCS.

TIP

Regardless of whether the settings for FBs with an instance name are changed, the FB instance setting file is checked out and checked in together with the iDefine-config file.

SEE ALSO For more information about the reflect, build, and start of RS Generation Manager, refer to:

D4.4, “Operating procedure of RS generation” on page D4-8

For more information about starting SCS Manager, refer to:

A10.2, “SCS Manager” on page A10-3

For more information about the analysis of SCS projects, refer to:

C5., “Testing with the Safety Analyzers” on page C5-1

For more information about download to the SCS, refer to:

C7., “Offline download to the target SCS” on page C7-1

■ Selecting an FB with an instance name

The instance names of all the FBs that are used in application logics that were created by using iDefine are configured separately. Using this dialog box, you can select whether to assign instance names to the FBs to be reflected in SCS projects for each FB type.

Change the setting to use SCS Manager to assign instance names to any unique FB types that do not have an instance name configured by default or to reduce the number of variables that are registered in the Dictionary View.

SEE ALSO For more information about the selection of an FB with an instance name, refer to:

“■ Selecting a FB with an instance name” on page D5-3

D5.3 Precautions when performing engineering by using iDefine

This section describes the terms used in ProSafe-RS and iDefine and the setting items that have any difference in specifications as the precautions for using iDefine in the engineering work.

You must understand these precautions before you start engineering.

IMPORTANT

If iDefine that was started by AD Organizer is operating, a dialog box appears and AD Organizer cannot be ended.

I/O Wiring

The following table compares the I/O Wiring information that is displayed in ProSafe-RS and iDefine.

Table D5.3-1 Comparison of terms between ProSafe-RS and iDefine (I/O Wiring information)

iDefine term	ProSafe-RS term	Description
Ch - Chassis	Node	iDefine identifies if the Node is for N-IO or FIO by adding a prefix. Format: [F/N][Node no.] F: Indicator for FIO, N: Indicator for N-IO
Sl - Slot	Unit	iDefine combines the information for Unit and Slot in the case of N-IO. Format for FIO: [Slot no.] Format for N-IO: [Unit no.][Slot no.]
	Slot	
Pt - Point	Channel or Terminal	Channel in the I/O Parameter Builder, and Terminal in AD Organizer

Variables

The following table compares the variables terms displayed in ProSafe-RS and iDefine.

Table D5.3-2 Comparison of terms between ProSafe-RS and iDefine (Variables)

iDefine term	ProSafe-RS term	Description
Tag	Variable (Global Scope)	Global variables of ProSafe-RS are called "Tag" or "TriTag" in iDefine. In iDefine, Tags are defined in Client IO Table and Typical. The defined Tags are reflected in Dictionary View of ProSafe-RS as variables.
Variable	Variable (Local Scope) Parameter	In ProSafe-RS, variables and parameters are defined by Dictionary View. In iDefine, those are defined by Typical, Function Block, or Structured Text. Local variables and parameters of ProSafe-RS are called “Variable” in iDefine.

Variable types

In iDefine, Tag types are specified in Client IO Table. The Tags will be reflected in Dictionary View as global variables. The following table shows the mapping between Tag types in iDefine and variable types in ProSafe-RS.

Table D5.3-3 Mapping of terms between ProSafe-RS and iDefine (Tag types in iDefine and variable types in ProSafe-RS)

Tag type in iDefine	Variable type in ProSafe-RS	Description
RI	IO_REAL	-
RO	IO_REAL	-
DI	IO_BOOL	-
DO	IO_BOOL	-
IM	DINT	-
DM	BOOL	-
RM	REAL	-
DEVICE	N/A	Variable will not be created in Dictionary View of ProSafe-RS for Tags of this type. This Tag type is used to assign a Typical to a Tag and instantiate the Typical.
IC	COM_DINT	Binding variable for inter-SCS safety communication
RC	COM_REAL	Binding variable for inter-SCS safety communication
DC	COM_BOOL	Binding variable for inter-SCS safety communication

Functions and function blocks

The following table shows the functions and function blocks that have different names in iDefine and ProSafe-RS, or those available only in either of them.

Table D5.3-4 Mapping of functions and function blocks between iDefine and ProSafe-RS

Category	iDefine name	ProSafe-RS name	Description
IEC61131-3 standard functions	ADD	+	Supported parameter data types are different between iDefine and ProSafe-RS. When you perform engineering by using iDefine, use parameters of the data type DINT, REAL, STRING, or TIME, which are supported by ProSafe-RS. If parameters of types other than DINT, REAL, STRING, and TIME are used, a build error will occur.
	DIV	/	-
	GE	>=	-
	GT	>	-
	LE	<=	-
	LT	<	-
	MOVE	1 GAIN	-
	MUL	*	-
	NE	<>	-
	SUB	-	-
TIS function	NUMBITS	-	Exported as user-defined function (ST) NUMBITS8 or NUMBITS16.

Continues on the next page

Table D5.3-4 Mapping of functions and function blocks between iDefine and ProSafe-RS (Table continued)

Category	iDefine name	ProSafe-RS name	Description
StateModule function blocks (*1)	TIS_CALCST	-	Exported as user-defined function block (ST).
	TIS_COND2	-	Exported as user-defined function block (ST).
	TIS_COND3	-	
	TIS_GST	-	Exported as user-defined function block (FBD).
	TIS_SE	-	Exported as user-defined function block (ST).
	TIS_SE_FIRST	-	
	TIS_SE_NT	-	
	TIS_SEP4	-	Exported as user-defined function block (ST). This creates AND_DWORD and OR_DWORD user-defined functions (ST) together.
	TIS_TMR	-	Exported as user-defined function block (ST).
StateModule functions (*2)	TIS_SEP1	-	Exported as user-defined function (ST).
Gas flow rate calculation function blocks (Interference-free)	-	ACCUM	Not supported in iDefine.
	-	AGA_3	
	-	AGA_7	
	-	AGA_R	
	-	ECWR_B	
	-	ECWR_I	
	-	ECWR_R	
Data buffering function blocks (Interference-free)	-	BUF_DIF_B	Not supported in iDefine.
	-	BUF_DIF_I	
	-	BUF_DIF_R	
	-	BUF_TIM_I	
	-	BUF_TIM_R	
	-	BUF_TRIG_B	
	-	BUF_TRIG_I	
	-	BUF_TRIG_R	
DNP3 communication function blocks (Interference-free)	-	DNP3_AI_16	Not supported in iDefine.
	-	DNP3_AI_32	
	-	DNP3_AI_SF	
	-	DNP3_AO_16	
	-	DNP3_AO_32	
	-	DNP3_AO_SF	
	-	DNP3_BI	
	-	DNP3_BO	
	-	DNP3_CT_16	
	-	DNP3_CT_32	

*1: Function blocks that are created when an SA module is converted to FBD
*2: Functions that are created when an SA module is converted to FBD

Differences of terminology during test operations

The terminology during test operations vary between iDefine and ProSafe-RS. The following table shows the correspondence between the varying terminologies.

Table D5.3-5 Correspondence chart for test operation terminology of iDefine and ProSafe-RS

iDefine Terminology	ProSafe-RS Terminology
Disable	Lock
Enable	Unlock
Set	Write
Single Step	One Cycle
Start Debug	Start Debug Mode
Stop Debug	Stop Debug Mode
Start Target	Simulation
Stop Simulator	Stop Simulation Mode
Cycle Scan Time	Cycle Timing

Notes on the reflection process for the iDefine-Config file

When the reflection process is performed after loading the iDefine-config file including subsystem communication FB or safety subsystem communication FB with AD Organizer, the POU and FB are all downloaded together onto the SCS project. In order to verify the subsystem communication FB or safety subsystem communication FB alone before downloading the application, use the function for skipping reflection of the program POU onto the SCS project.

SEE ALSO For more information about how to skip reflection of a program POU onto an SCS project, refer to:

"■ Skipping reflection of a program POU" on page D4-5

Cautionary notes on the use of the POWE/LOGE function

When using the POWE/LOGE function with the iDefine-config file that the reflection process is performed, POWE/LOGE is handled as either a safety function or an interference-free function, depending on the revision of the new SCS project created by SENG. The logic behavior of POWE/LOGE remains unchanged.

The following table describes the revision of the new SCS project created by SENG and the handling of POWE/LOGE.

Table D5.3-6 Revision of new SCS project created by SENG and handling of POWE/LOGE

Revision of new SCS project created by SENG	Handling of POWE/LOGE
Earlier than R4.07	Interference-free function
R4.07 or later	Safety function

E. Changing application

This section describes the procedure for online change of applications, procedure of import/ export, and the procedure to reuse SCS project database.

E1. Online change of applications

This chapter describes the procedure for online change of applications.

E1.1 Online change download

Online change download changes a part of an application without interrupting SCS functions. In SCS, the data stored in main memory of the CPU module is updated and changes are stored in flash memory of the CPU module as well. When performing online change download of I/O definitions, changes are also reflected in the non-volatile memory of the input/output modules. Data downloaded to an SCS is also saved in the master database on the SENG.

TIP

The SCS operating mode will not be changed when online-change downloading is performed.

Items for which online change download is allowed

SCS engineering tasks may include items for which online change download is allowed and items for which offline download is necessary.

IMPORTANT

- If the variable cannot be added by online change download depending on the state of free memory space, Clean Project and Offline Download are required. However, if you review and delete unused I/O modules and variables, you may be able to add new variables via online change download.
- Builders allow generating parts of database where online change download is not allowed.
  If you make changes exceeding the range where online change is possible, you will be notified that the downloading is impossible after performing the download operation.

  If it is notified that online change download is not possible, close SCS Manager once and use Master Database Restoring Function to revert the modified data to the same status as the data in the SCS.
- When engineering by using iDefine, you cannot check whether you can make changes online in iDefine. As such, make sure you confirm which items to change before changing anything. You will not be able to perform changes online after the changes have been reflected in SCS Manager; if you use the Master Database Restoring Function, the iDefine project database must also be restored to its previous state. As such, it is recommended that you back up the iDefine project database before making changes in iDefine.
- When modifying the logic, the related output channels should be locked-out on the I/O Lock window. However, locked channels cannot output values in response to demand. Analyze the impact of locking channels on the system in advance and implement the necessary measures before locking channels.
- When performing online changes for POUs, make sure to consider the items related to "Miscellaneous limitations" of the "Online changes" description in the "Debug" section of the "Workbench" chapter in the Workbench User's Guide.

Procedure for online change download

This section describes procedures from building application logic to storing SCS project after an online change download.

What to do before online change download

Build the application logic and analyze it by using Integrity Analyzer and Cross Reference Analyzer.

TIP

The items that may require retesting but not detected by Cross Reference Analyzer must be checked by the user.

IMPORTANT

Call up the SCS Information dialog box and confirm that the number of logical I/O points in use does not exceed the number of granted I/O licenses.

Use the SCS security level operation function to set the SCS security level to Level 1.

After that, open the I/O Lock window and lock the input and output modules to be affected by online change downloading.

Start the online change download

1. From the [Debug] menu in SCS Manager, select [Online Change: Download]. Alternatively, click the [Online change download] button on the toolbar.
   The Online Change Download Confirmation dialog box appears.

TIP

- If Integrity Analyzer or Cross Reference Analyzer has already been launched when you start online download, a message prompting to close the analyzer is notified and the download ends with an error.
- If the SCS security level is set to Level 2 when the online change download starts, a message prompting you to change the security level appears and the program aborts. Set the security level to Level 1 and start an online change download.
- If the I/O Lock window or Inter-SCS Communication Lock window is left open when you start online change download, an error message appears and the download processing stops.

2. Click [OK].
   A dialog box prompting to confirm the version control appears.

When the Scan period of the application logic is changed

If the scan period of the application logic has been changed, a confirmation dialog box appears when you start online change download. If there are any changes that take long time in downloading, another confirmation dialog box appears.

Check the application logic and end online change download

Using SCS Manager, change the SCS mode to Target test mode and test the changes you made. After the test, unlock the input and output modules which were previously locked using the I/O Lock window. And perform the output enable operation.
From the Set SCS Security Level dialog box, change the security level to Level 2. After that, save the SCS project using the Version Control Tool.

E1.2 Entire procedure of online change of application

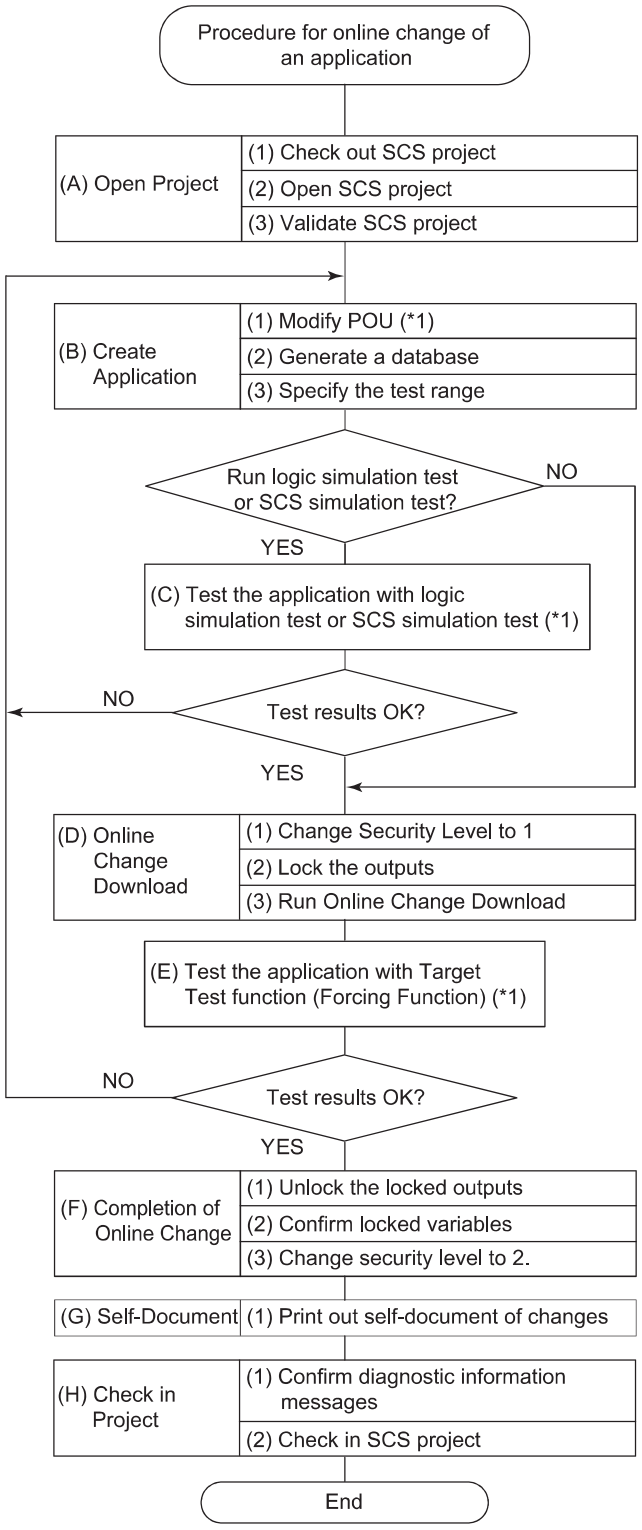
This section describes a procedure for online change of an application.

Procedure for online change of an application

Before performing an online change of an application, you need to analyze possible effects caused by the change carefully and take the appropriate measures. This section describes procedures for online change of application for both the following cases: online change of applications with addition or change of I/O modules, and online change of applications without addition or change of I/O modules.

Online change of applications with addition or change of I/O modules

The following describes the procedure for online change of applications without addition or change I/O modules.



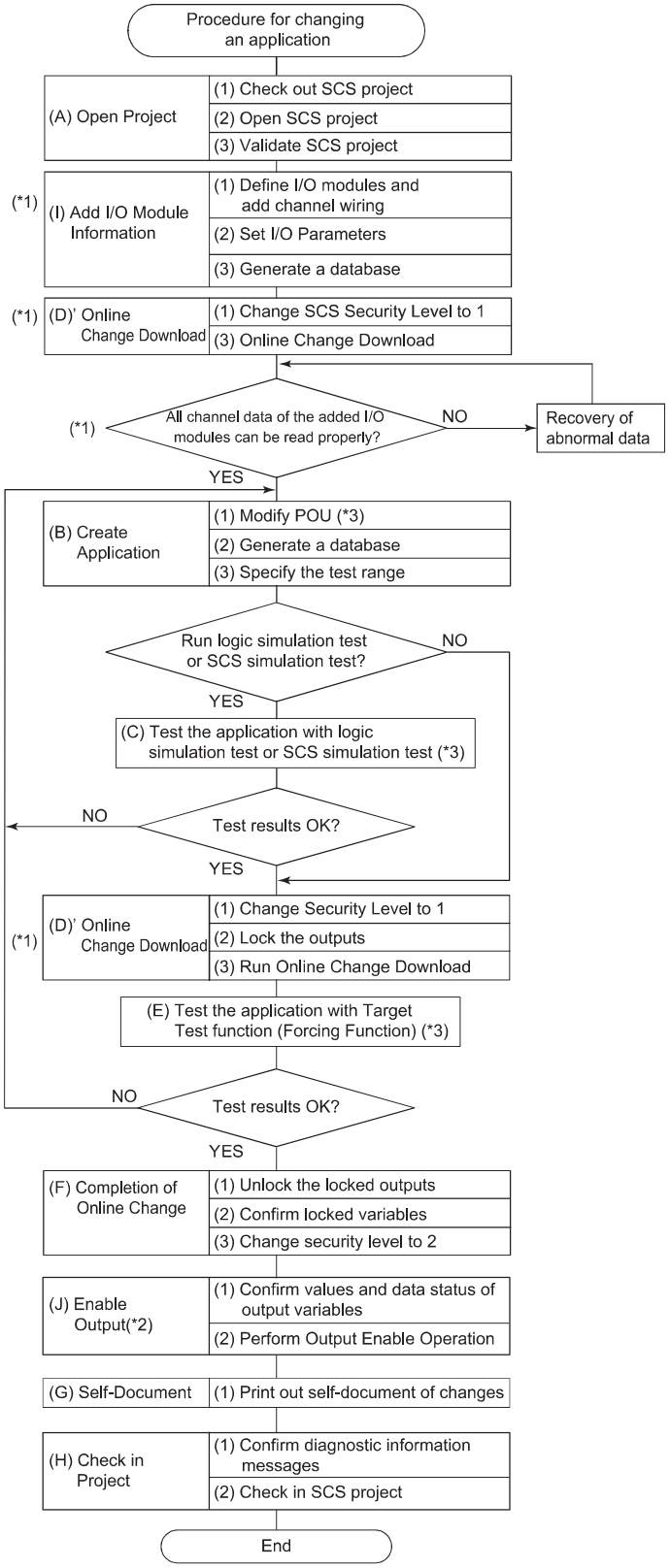
*1: You can use iDefine functions when you use I/O list engineering with iDefine.

Figure E1.2-1 Procedure for online change of an application

Online change of applications with addition or change of I/O modules

The following describes the procedure for online change of applications with addition or change I/O modules.
Before performing the following procedure, you need to install the I/O modules in the nodes and complete the required hardware setups such as field wiring and connection of power sup-

ply. Then, by using the following procedure, you need to make sure that all data of the added channels are normal, and generate the application or implement the changes.



*1: These steps are different from the procedure for online change without adding input/output modules.
*2: This is required only when you add output channels or output modules.
*3: You can use iDefine functions when you use I/O list engineering with iDefine.

Figure E1.2-2 Procedure for online change of an application (with addition and change of I/O modules)

SEE ALSO For more information about changing hardware, refer to:

E., “Maintaining the SCS” in Hardware User's Guide (IM 32P06C10-01EN)

(A) Opening the project

Table E1.2-1 Procedure for opening a project

Item	Description
(1) Check out SCS project	• Check out the existing SCS project with the Version Control Tool.
(2) Open SCS project	• Start SCS Manager from AD Organizer. • Open the SCS project. • Enter the password for the SCS project.
(3) Validate SCS project	• Run the Database Validity Check Tool and check that the CRC codes and generation times of the databases are consistent between the SCS and SCS project. • Repair a database if there is a discrepancy in the database.

SEE ALSO For more information about precautions for handling an SCS project engineered by I/O list engineering that was checked in with Version Control Tool of a revision earlier than R4.03.10, refer to:

“■ Precautions for handling an SCS project that was checked in with Version Control Tool of a revision earlier than R4.03.10” on page C3-2

(B) Creating an application

Table E1.2-2 Procedure for creating an application

Items	Description
(1) Modify POU	If you are not using iDefine: • Open the POU that you want to change. • Edit POU. • Save POU. • Print POU. • Confirm that the logic entered in Multi-Language Editor is the same as the logic printed by using the self-document function. If you are using iDefine: • Export the ProSafe-RS I/O file from AD Organizer and import it in iDefine. • Change the POU, variables and tag-related definitions by using iDefine. • Export the iDefine-config file from iDefine and import it in AD Organizer. • Run Reflection by using RS Generation Manager. Confirm that the run sequence for FB and FU is correct.
(2) Generate database	• Perform Build. • Analyze and confirm that the safety applications such as FU/FB are correct in terms of safety by using the Integrity Analyzer. • Call up the SCS Information dialog box and confirm that the number of logical I/O points in use does not exceed the number of granted I/O licenses.

Continues on the next page

Table E1.2-2 Procedure for creating an application (Table continued)

Items	Description
(3) Specify the range of testing	• Check the modified POU and the affected POU with the Cross Reference Analyzer and then authorize them. For the POU detected by the Cross Reference Analyzer, check the contents of the change with the Project Comparing Tool, determine whether the change affects the behavior of the logic, and add to the test target if any effects are expected. • Use the Project Comparing Tool to confirm that the following settings (for which Cross Reference Analyzer cannot confirm the existence of changes, which are critical in terms of safety, and through which online change download is made possible) are not unintentionally changed: Item in Resource Properties window: • [Cycle Timing] Items in SCS Constants Builder: • [Extend Scan Period Automatically] (*1) • [Behavior at Abnormal Calculation] (*1) • [Automatic IOM Download] (*1) • [Locking of Internal Variables] (*1) (for SCSP3/SCSL2/SCSP2) • [Device Power-Off Period] (for SCSP3/SCSL2/SCSP2/SCSP1/SCSU1) • [Device Startup Waiting Period] (*1)(for SCSP3/SCSL2/SCSP2/SCSP1/SCSU1) • [Skip Password Dialog Box for Manual Operation FB] (*1)(for SCSP3/SCSL2/SCSP2/SCSP1) Items in I/O Parameter Builder • [Extends Node Bus] (*1) • [Extends To (km)] (*1)

*1: The corresponding item may not exist or the configurable value may be different depending on the software release number of the system or SCS type. Such items may therefore be picked up as discrepancies by the Project Comparing Tool.

(C) Testing applications with logic simulation test functions and SCS simulation test functions

Test the user application with the logic simulation test functions or SCS simulation test functions.

SEE ALSO For more information about details of logic simulation test and SCS simulation test, refer to:

C6., “Simulation tests” on page C6-1

(D) (D’) Online change download

Table E1.2-3 Procedure for online change download

Items	Description
(1) Change SCS Security Level	• Start the SCS Maintenance Support Tool which monitors the SCS from the SCS Manager. • Set the security level to 1. Entering a password is required. • Confirm that the SCS Security Level is 1 on the SCS State Management window of SCS Maintenance Support Tool. • Confirm the diagnostic information message indicating the security level at 1 with the SCS Maintenance Support Tool.
(2) Fix the output	• Locks all the channels of the output modules connected to the modified POU or to be modified POU. • Use the SCS Maintenance Support Tool to confirm that a diagnostic information message is output, indicating that the abovementioned modules have been locked.

Continues on the next page

Table E1.2-3 Procedure for online change download (Table continued)

Items	Description
(3) Online Change Download	• Perform online change download. • Establish a communication. Confirm that no communication error occurs. • Confirm that the diagnostic information message is not issued, which is caused by a write error to the flash memory of SCS. If it is issued, perform Offline download. • Use the Database Validity Tool to confirm that CRC and generation time of four kinds of databases for SCS project databases are correct. Confirm that CRC of four kinds of databases and generation time are correct. • Repair a database if there is a discrepancy in the database. • Confirm that the total number of POU notified in the diagnostic information message about the change of resources (No.4172) is identical to the total number of POU shown in the Database Validity Tool. • If downloaded to Output module, validate the output after the download.

CAUTION

I/O Lock is a function to prevent unnecessary shutdowns in the following conditions:

- System malfunction caused by unintended errors in application programs
- Temporary halt of the I/O module when the I/O module settings are changed

If you lock the output, you can conduct target tests to check the behavior of a modified logic. However, if you are sure in advance that the above mentioned system malfunction or temporary halt does not occur, or that the occurrence causes no problem, you do not need to lock I/O. Furthermore, locked channels cannot output values in response to demand. Analyze the impact of locking channels on the system in advance and implement the necessary measures before locking channels.

The explanations in Instruction Manuals (IM) for ProSafe-RS rest on the premise that you use the I/O Lock function.

SEE ALSO For more information about repairing a database, refer to:

"■ Repair database" in F3., "Database Validity Check Tool" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about precautions for online change, refer to:

E1.5, "Precautions for online change" on page E1-20

For more information about precautions related to locks, refer to:

2.6, "Forcing" in Safety Manual (IM 32P01S10-01EN)

(E) Target test functions

Perform the output enable operation and test the user application on the target SCS.

SEE ALSO For more information about details of target test, refer to:

C9., "Target tests" on page C9-1

(F) Completion of online change

Table E1.2-4 Procedure for completion of online change

Items	Description
(1) Unlock the locked outputs	• Confirm that, for the digital output modules concerned, the values and statuses of logical data agree with those of physical data. • Unlock the output modules concerned. • Confirm that the diagnostic information message which indicates the output modules concerned have been unlocked is output with the SCS Maintenance Support Tool. • Disable the bypass to the actuator.
(2) Confirm locked variables	• Confirm the number of locked variables is 0 with the SCS Maintenance Support Tool. • Confirm that no diagnostic information message is issued except for one you confirmed, with the SCS Maintenance Support Tool.
(3) Change the security level to 2	• Set the security level to 2. • Confirm that the security level is 2 in the SCS State Management window of the SCS Maintenance Support Tool. • Confirm the diagnostic information message which indicates that the security level went back to 2 with the SCS Maintenance Support Tool.

(G) Self-document

Table E1.2-5 Procedure for Self-document

Items	Description
(1) Print out modified parts of the project using self-document	• In preparation for the desk check performed at application software changes in the future, print out the latest SCS project database as self-documents.

(H) Check in project

Table E1.2-6 Procedure for checking in a project

Items	Description
(1) Confirm the diagnostic information message	• Confirm that diagnostic information message other than one you confirmed is not issued with the SCS Maintenance Support Tool.
(2) Check in the SCS project	• Close the SCS Manager. • Check in the SCS project.

(I) Adding I/O module information

Table E1.2-7 Procedure for adding I/O module information

Items	Description
(1) Define I/O modules and add channel assignment	For I/O list engineering • Obtain the latest safety I/O list and import it by using Safety I/O Editor. Alternatively, obtain the latest safety communication I/O list and import it by using Safety Communication I/O Editor. • Use Safety I/O Editor, Safety Communication I/O Editor, and IOM Definition Editor to define I/O modules and I/O parameters. • If this affects the applications created by using iDefine, export the ProSafe-RS I/O file from AD Organizer and import it in iDefine to repair the iDefine application. For RS original engineering • Define I/O variables with the Dictionary. • Add I/O module definitions and define parameters. • Connect I/O variables to channels.

Continues on the next page

Table E1.2-7 Procedure for adding I/O module information (Table continued)

Items	Description
(2) Specification of I/O parameter	For RS original engineering • Define all parameters of nodes, units, modules, and channels.
(3) Generate a database	• For I/O list engineering After changing the application by using iDefine, export the iDefine-config file from iDefine and import it to AD Organizer. Start the Generation Manager from AD Organizer and execute reflection or RS generation process. • For RS original engineering Perform Build. • Analyze and confirm that the safety applications such as FU/FB are correct in terms of safety by using the Integrity Analyzer. • Use the SCS Information dialog to confirm that I/O license is available.

(J) Enabling output

Table E1.2-8 Procedure for enabling output

Items	Description
(1) Confirm values and data status of output variables	• Confirm which output channels are disabled on the SCS State Management window of SCS Maintenance Support Tool. • Start the I/O Lock Window.(This can be performed at security level 2.) • Confirm that values and statuses of logical data and physical data for output variables are correct.
(2) Operate “Enable Output”	• Perform the Output Enable Operation for output modules on the SCS State Management window of SCS Maintenance Support Tool. • Confirm that the diagnostic information message on the Output Enable Operation for output modules is displayed. • Confirm that Output Channels are enabled on the SCS State Management window. • Confirm that the SCS operating mode is "Running" on the SCS State Management window.

SEE ALSO For more information about details of the enable output operation, refer to:

“■ Enable Output operation” on page C8-2

E1.3 List of applicable items for online change

This section describes the items for which you can perform online change download and those which require offline download. If stopping SCS control is not allowed, setting items that require offline download must not be changed.

IMPORTANT

If you change setting items that require offline download, even if you reverse the change, online change download is not allowed. If this happens, use Master Database Restoring tool to recover the database to a state where online change download is allowed. When engineering by using iDefine, you must restore the iDefine project database as well.

SEE ALSO

For more information about online change availability for SCS operating on a SCS system program revision of R2.02 or earlier, refer to:

"■ Possibilities of online change download" on page App.3-5

For more information about operations of the Master Database Restoring function, refer to:

F4., "Master Database Restoring Function" in Engineer's Reference Manual (IM 32P04B10-01EN)

■ Online change of POU information

There are changes that enables you to execute online change download or offline download according to each POU type.

● Changing POU

The following table shows whether POU can be changed online. For an SCS project newly created with SENG R4.09.00 or later or when clean project is executed for an SCS project earlier than R4.09.00, online change download is available when newly creating, deleting, or renaming all program, user-defined FU, and user-defined FB POUs.

Table E1.3-1 Whether or not online change can be used for POU operations

Type of POU	Changing a name	Creating, deleting
Program	Yes	Yes
User-defined FU	Yes	Yes
User-defined FB	Yes	Yes

● Changing POU logic

When you perform a change operation on POU described in the following table, you can perform an online change download to SCS.

Table E1.3-2 Logic change operations that can be changed online on POU

Corrected item	Description
Adding/deleting the standard FU call	-
Adding/deleting the user-defined FU call	Including FU defined in the library. A project that is created with the revision earlier than R3.02.00 will be in the same condition as R3.02.00 when clean project is executed. Therefore, you can perform an online change download.
Changing logic	-

Changing a library

For an SCS project newly created with SENG R4.09.00 or later or when clean project is executed for an SCS project earlier than R4.09.00, online change download is available when adding or deleting a library from SCS project or renaming a library.

Changing program

The following table shows the operations that can perform online change download to SCS for global variables, global instances, local variables, and local instances that are used in Program.

Table E1.3-3 Operations that can be changed online for variables and instances used in program

Corrected item	Description
Adding/deleting a variable	-
Deleting variables and adding variables with the same names as the deleted variables	-
Changing the types of variables	-
Changing attributes of variables	-
Adding/deleting I/O variables	-
Adding/deleting the standard FB instances	-
Adding/deleting the user-defined FB instances	Including FB defined in the library. A project that is created with the revision earlier than R3.02.00 will be in the same condition as R3.02.00 when clean project is executed. Therefore, you can perform online change download.
Deleting FB instances and adding FB instances with the same names as the deleted ones	
Changing the types of FB instances	

Changing user-defined FB

The following table shows the corrections that need offline download to SCS for the parameters of user-defined FB. A warning is displayed at the build operation when performing the correction in the table. An error occurs at online change download operations.

However, if the user-defined FB to be changed meets the following conditions, no warning or error will occur and the online change can be made.

- User-defined FB instances are not defined in Dictionary.
- Instances without name are not used in Program.

Table E1.3-4 Operation of parameters that need offline download in user-defined FB

Modification	Description
Adding/deleting a parameter (*1)	-
Deleting parameters and adding parameters with the same names as the deleted parameters (*1)	-
Changing the types of parameter (*1)	-
Changing the attributes of parameter (*1)	As the attributes of user-defined FB parameters, the following items cannot be changed online. Direction, () (specification of the number of characters for STRING variables: [Not supported]), Dimension
Adding/deleting the standard FB instances (*1)	If you add FB instances without names (not appearing in the Dictionary) in user-defined FB, the FB instances become parameters and thus cannot be changed online.
Adding/deleting the user-defined FB instances (*1)	
Deleting FB instances and adding FB instances with the same names as the deleted ones (*1)	
Changing the types of FB instances (*1)	-

*1: Online change download is available by deleting the user-defined FB and creating a new user-defined FB with the same name. However, in this case, the created user-defined FB instance operates as a new instance that is different from the user-defined FB before deletion, regardless of whether there are differences in parameter definitions. Even if the parameters are the same in the definition, values are not inherited.

The following table shows the corrections that you can execute online change download to SCS for the global variables and the global instances used in user-defined FBs.

TIP

Normally, global variables and global instances are not used in user-defined FBs.

Table E1.3-5 Operations that can be changed online for global variables and global instances used in user-defined FB

Modification	Description
Adding/deleting a variable	-
Deleting variables and adding variables with the same names as the deleted variables	-
Changing the types of variables	-
Changing the attributes of variables	-
Adding/deleting the standard FB instances	-
Adding/deleting the user-defined FB instances	Including FB defined in the library. A project that is created with the revision earlier than R3.02.00 will be in the same condition as R3.02.00 when clean project is executed. Therefore, you can perform online change download. When adding user-defined FU/FB, the added user-defined FU/FB must be tested. When adding pre-validated user-defined FB, testing of the FB itself is not required.
Deleting FB instances and adding FB instances with the same names as the deleted ones	Including FB defined in the library. A project that is created with the revision earlier than R3.02.00 is in the same state as R3.02.00 when clean project is executed. Therefore, it can perform online change download.
Changing the types of FB instances	

Changing user-defined FU

The corrections that you can execute online change download for parameters or local variables in user-defined FU are as follows:

- Adding/deleting
- Deleting variables and adding variables with the same names as the deleted variables
- Changing the types of variables
  However, when the type of output parameter is changed, offline download is required.
- Changing attributes of local variables

SEE ALSO

For more information about the precautions that should be taken when deleting a variable or function block and then adding it again, refer to:

"Declared Variables" in "Variables" in "Online Change" in "Debug" in "Workbench" of "Workbench User's Guide"

I/O module information that is changeable online

The following table shows whether each item of I/O module related information can be changed by online change downloading.

Table E1.3-6 I/O module

Modification	Online change (*1)
Adding nodes	Yes
Deleting nodes	Yes
Changing parameters of nodes	Yes
Adding a unit	Yes
Deleting a unit	Yes
Adding I/O modules	Yes
Deleting I/O modules	Yes
Changing redundant I/O modules	Yes
Changing parameters of I/O modules	Yes
Change in the mounting position (node, unit, and slot) of N-IO I/O module	Yes
Change in the signal category of N-IO I/O modules.	Yes
Changing parameters of channels	Yes
Change in parameters of serial communication modules or Ethernet communication modules	Yes
Defining wiring between a variable and an idle channel	Yes
Deleting wiring between a channel and a variable	Yes
Changing wiring between a channel and a variable	Yes
Addition, change or deletion of subsystem communication definitions	Yes
Changing wiring of communication input/output FBs	Yes
Addition or deletion of ESB bus coupler modules	Yes
Add, change or delete a fire and gas communication definition	Yes
Changing a fire and gas communication FB wiring	Yes

*1: Yes: Online change download is possible.

SEE ALSO For more information about changing hardware, refer to:

- E4., “Replacing FIO node components” in Hardware User's Guide (IM 32P06C10-01EN)
- E5., “Replacing N-IO node components” in Hardware User's Guide (IM 32P06C10-01EN)

Constants and network information that are changeable with online

The following table shows whether the setting can be changed by online change downloading in the constant and network related items.

Table E1.3-7 Constant and network

Classification	Modification	Online Change (*1)
Configuration	Name	No
	Password	No (*2)
Resource	Name	No
	Resource Number	No
	Cycle Timing	Yes
	Memory size for online changes	No
	Memory size for temporary variable	No

Continues on the next page

Table E1.3-7 Constant and network (Table continued)

Classification	Modification	Online Change (*1)
Network	IP address	No
	Station address	No
	Inter-SCS safety Communication (Binding)	No

*1: Yes: Online change download is possible.
No: Offline download is required.
*2: Setting and changing passwords is ignored.

Builder definitions that are changeable with online

The following table shows whether online change download is possible after definition information has been changed using builders.

Table E1.3-8 Builder definitions that are changeable with online

Item	Online Change (*1)
SCS Constants Builder	Yes (*2)
I/O Parameter Builder	Yes
Communication I/O Builder	Yes
SCS Link Transmission Builder	Yes
Modbus Address Builder	Yes
DNP3 Communication Builder (*3)	Yes (*4)
Tag Name Builder	Yes
Alarm Priority Builder	No
Alarm Processing Table Builder	No

*1: Yes: Online change download is possible.
No: Offline download is required.
*2: Some items can be changed online. "Table of SCS Constants Builder online change" shows which items can or cannot be changed online.
*3: Usable only for SCSU1
*4: Some items can be changed online. "Table of DNP3 Communication Builder online change" shows which items can or cannot be changed online.

Table E1.3-9 SCS Constants Builder online change

Item	Online Change (*1)
Interval of Repeated Warning Alarms	No
Synchronous Mode	No
Scan Period for External System	No
Modbus Word Order	No
16-bit Modbus master support mode	No
Alarm Notify Action when AOF Released	No
PV Status of S_ANLG_S	No
The first number of annunciator messages with tag name	No
DNP3 Slave Function (*2)	No
Skip Password Dialog Box for Manual Operation FB (*3)	Yes
Optical ESB Bus Repeater	No
Maximum Extension Distance	No
Extend Scan Period Automatically	Yes

Continues on the next page

Table E1.3-9 SCS Constants Builder online change (Table continued)

Item	Online Change (*1)
Behavior at Abnormal Calculation	Yes
Locking of Internal Variables (*4)	Yes
Automatic IOM Download	Yes
Device Power-Off Period (*5)	Yes
Device Startup Waiting Period (*5)	Yes
Alarm Suppression During Device Reset (*3)	No
Command Line	No

*1: Yes: Online change download is possible.
No: Offline download is required.
*2: Displayed for SCSU1
*3: Displayed for SCSP3/SCSL2/SCSP2/SCSP1.
*4: Displayed for SCSP3/SCSL2/SCSP2.
*5: Displayed for SCSP3/SCSL2/SCSP2/SCSP1/SCSU1.

Table E1.3-10 DNP3 Communication Builder online change

Items	Online Change (*1)
DNP3 slave station address	Yes
DNP3 master station address	Yes
Timeout value for Select Before Operate (sec)	Yes
Binary Input event buffer size	No
Binary Output event buffer size	No
Binary Counter event buffer size	No
Frozen Counter event buffer size	No
Analog Input event buffer size	No
Analog Output event buffer size	No
Event to be removed when event buffer overflows	Yes
Generate an event when Freeze and Clear command changes data values	Yes
Include Frozen Counters in Class 0 response	Yes
Type of response message fragmentation	Yes

*1: Yes: Online change download is possible.
No: Offline download is required.

E1.4 Online change of scan period of the application logic execution function

The scan period of the application logic execution function can be changed online in the case of SCS with SCS system program R2.03 or later.

Overview of scan period online change

Change the scan period of the application logic execution function with SCS Manager and execute online change download under security level 1 or lower. The SCS will then operate with the specified scan period after download completes. If automatic extension of scan period has been enabled on the SCS, the automatic scan period extension status is cancelled after the completion of online change download and the SCS resumes operation with the scan period specified with the online change.

Limitations on online change

The allowable range of change is the same as the allowable range of specification, i.e., from 50 ms to 1000 ms in increments of 10 ms. Note that in online change, it is not allowed to set a scan period longer than the scan period before change by more than 250 ms. If such changes are made, an error occurs at online change download.

Example:

It is possible to change the scan period from 250 ms to 500 ms. Change from 250 ms to 550 ms is not allowed because it represents an increase of 300 ms.

When changing to a shorter scan period, a dialog box appears, showing the expected CPU idle time after the scan period is changed. You cannot download if the expected CPU idle time is 0 second.

TIP

On the SCS Simulator, the expected CPU idle time is not estimated. Only a dialog box is displayed, informing that the scan period has been changed.

Occurrence of IOM download at online change download

If the scan period defined before or after execution of online change is longer than 250 ms, IOM download processing is executed for all AIO/DIO modules used in the given SCS to notify the change of fallback time. In this case, a confirmation dialog box appears at the start of online change download.

- There is no influence on control operation during online change download because the control of AIO/DIO modules continues.
- Online change download on SENG is completed after the completion of IOM download to all AIO/DIO modules. IOM download takes approximately 5 seconds per module.

If an online change download that changes the scan period is executed, IOM download is executed for all N-IO modules used in the SCS.

- While IOM continuous download is in progress for N-IO modules, control of the N-IO modules continue. Safety loops will not be affected by the execution of IOM downloads.
- After the IOM downloads for all N-IO modules are completed, the online change download is regarded as completed on the SENG. The IOM download for N-IO modules takes about two seconds per module.

SEE ALSO

For more information about the results of analysis by Cross Reference Analyzer when the scan period is changed, refer to:

"● Changing Scan period" on page C5-38

Notification of scan period online change

When online change download performed at scan period change is completed, the diagnostic information message of scan period online change (No. 4152) is notified, in addition to the diagnostic information message of online change download completion.

E1.5 Precautions for online change

This section describes precautions for online change of an application.

Cross Reference Analyzer

- User should confirm locations required for a retest by checking the output of Cross Reference Analyzer.
- For interference -free applications, it is also required to analyze and test parts that are potentially affected by application modifications as with safety applications.

Online change download

- When Online Change Download is executed on I/O modules, confirm that download is executed on the correct I/O modules by checking the diagnostic information message from SCS.
- In CENTUM Integration engineering, even if the correspondence of an instance name and tag name is changed, the modified location may not be displayed in the Cross Reference Analyzer nor in the diagnostic information message. Users must conduct tests very carefully.
- After performing an online change, confirm that the CPU idle time of SCS is sufficient and the scan timing is appropriate.
- When the CPU module is in a dual-redundant configuration, avoid performing online change download during APC (All Program Copy) whenever possible. If online change is executed during APC, the APC is interrupted and starts over again after the online change is finished, which requires longer time to complete APC. This prolongs the duration of operation with a single CPU. This behavior has no impact on safety. The status of APC operation can be confirmed with LED on CPU, SCS State Management window of SENG or Status Display View of HIS. The start and end of APC are notified by diagnostic information messages.
- The maximum number of tag names that can be assigned for monitoring to the annunciators (ANN/ANN_FUP) and function blocks (such as ANLG_S and PASSWD) that allow the assignment of mapping blocks are as follows:
  - Up to 2600 tag names can be assigned when using SCSP1/SCSV1
  - When SCSP3/SCSL2/SCSP2 is used, a maximum of 4500 tag names can be assigned.

  The maximum number of online changes that can be made to these tag names and parameters of the mapping blocks and elements at one time is 200. However, online change download may not succeed even if the above condition is met. In this case, the following error message appears in the message display area of SCS Manager.

  ```
  Too much modified data. Make fewer changes, then load.
  ```

  The limit on the number of function blocks when using SCSP1/SCSV1 is as follows:

  (Number of mapping blocks) + (number of annunciator blocks with tag names) + (total number of mapping blocks/elements changed online at one time) ≤ 2800

  When using SCSP3/SCSL2/SCSP2, the minimum number is as follows:

  (Number of mapping blocks) + (number of annunciator blocks with tag names) + (total number of mapping blocks/elements changed online at one time) ≤ 4700

  If this condition is not met, an error occurs in the check performed before online change and the following error code is displayed in the message display area of the SCS Manager.

```
Error Code:0x9443:0x8ec9
```

or

```
Error Code:0x9448:0x8ec9
```

Note that tag names are not mandatory for annunciators. It is recommended to set tag names only for those that are referenced by tag names.

- If online change download is executed while the Communication I/O Lock Window is open, close the Communication I/O Lock Window after the completion of the online change download. Then, open the Communication I/O Lock Window again. A database mismatch error may occur if the Communication I/O Lock Window is not closed.
- If you change the range of an input channel that is defined in I/O parameters and execute an online change download, the input value on that channel changes during the download and IOP may occur.
- While an Output value at fault is being output, if you change any I/O parameter related to the Output value at fault and execute an online change download, the output value on the channel to which the change was made may change during the download.

SCS actions after changing the types of FB instances

The SCS actions during online change download after the types of FB instances or variables are changed are as follows:

- CENTUM integration configuration
  SCS data keeps the values before online change download. When reading with the Tag Name interface from CENTUM station, the read values are the values before executing online change download. Values cannot be written from CENTUM station.
- Modbus Slave Communication
  Loading/writing values from the Modbus master causes an error. The error code is 13 (hexadecimal).

SEE ALSO For more information about the error code in Modbus slave communication, refer to:

"● Response message under abnormal conditions" in "■ Response message from SCS" in F1.7, "Messages communication" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Precautions for changing instance name in online change

If you add/change/delete Instance name(s) to/in/from a function block used in POU and online change download, it affects the behavior of the changed function block.(*1) Do not make unnecessary changes to Instance name(s). Adding of Instance name(s) to a function block is required only if External communication function is used.

*1: Each function block is affected differently by online change. Adding/changing/deleting Instance name(s) involves deleting the existing Instance name(s) together with its previous input/output value and internal status, which affects the behavior of FB. Function Blocks that require measures against instance name changes are as follows:

Table E1.5-1 Impact of instance name change(s)

Function Block	Impact	How to Recover/Avoid
OVR_B, OVR_I, OVR_R, OVR_IB, OVR_IR, GOV_B, GOV_IB	If Override is on, it turns off.	Override is repeated from HIS.
PASSWD	If activated, it gets deactivated.	Activate it again from HIS.
PROD_B, PROD_I, PROD_R	An Inter-SCS communication error and recovers later.	Before online change download, lock the output of Consume side.

Continues on the next page

Table E1.5-1 Impact of instance name change(s) (Table continued)

Function Block	Impact	How to Recover/Avoid
MOB_11, MOB_21, MOA	If Data Manual Operation is enabled, output gets FALSE or “0.”	Before online change download, lock the variable of OUT connected to MOB_* or MOA.

Precautions for reusing instances

If you delete an instance of an FB or instance of a variable from a Program and perform online change downloading without deleting it (instance of FB or variable) from the Dictionary and then add it again to the Program, the data in the instance are those before the deletion. If you need to initialize the instance data, restart the SCS.

Precautions related to initial values of variables

Initial values of variables and FB instance parameters are used when fixing values without rewriting them via logic and specifying values before execution of the first scan after starting SCS.

If Type, Dimension, Scope, and Direction, among types and attributes of variables, are changed online, the values are initialized to the initial values specified by Init.Value of the Dictionary. Changes to values are not reflected if only Init.Value of the Dictionary is changed and online change is executed in order to change the initial values.

If you wish to change only the initial values of variables or FB instance parameters via online changes, change the variable names or delete the variables or FB instances once, perform online change download and then perform online change download to add them again.

Writing to flash memory of SCS

- If an error occurs during writing operation to a flash memory, offline download is required.
- If writing operation to the flash memory is interrupted by pulling out the CPU module or cutting off the power, hardware of the flash memory may fail. Before removing the CPU module or cutting off power, confirm that the LED on the CPU module indicating the flash memory writing status, is lit up (not writing).

Online change of scan period

- You can change the scan period of the application logic execution function by using the online change download. When you shorten the scan period, a confirmation dialog box displays the estimated CPU idle time of the SCS after changing the scan period during performing online change download. For the estimated idle time that is displayed, only the change in scan period is considered and the impact due to application change is not considered.
- Do not change both the scan period of the application logic execution function and applications (e.g., addition of logics and I/O modules) at the same time in a single online change download operation. First, change the scan period and perform online change download, check the CPU load of SCS and then change applications.

Reception Interval Timeout Value (OUTT) for Inter-SCS safety communication

In principle, if you set a longer scan period, the transmission interval of inter-SCS safety communication becomes longer. When you change the scan period by online change download, you need to re-adjust the reception interval timeout values (OUTT) of the SCSs that communicate, by inter-SCS safety communication with the SCS for which the scan period is changed.

(This includes the case where the SCS for which the scan period is changed receives data by inter-SCS communication.)

SEE ALSO For more information about precautions when setting OUTT, refer to:

"● OUTT (reception interval timeout value) setting" in "■ Definition of receive data" in A6.2, "Data structure and definition of the SCS link transmission" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Reception Interval Timeout Value (OUTT) for SCS link transmission safety communication

If you set a longer scan period, the transmission interval of SCS link transmission safety communication becomes longer. Therefore, you also need to re-adjust the OUTT for SCS link transmission safety communication, as should be done for inter-SCS safety communication.

SEE ALSO For more information about precautions when setting OUTT, refer to:

"● OUTT (reception interval timeout value) setting" in "■ Definition of receive data" in A6.2, "Data structure and definition of the SCS link transmission" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Online change of single/dual-redundant specification of AIO/DIO modules

You need to perform the following procedure to change two adjacent AIO/DIO modules in single configuration implemented in FIO node into dual-redundant configuration by using online change download.

1. Disconnect the I/O cables (or terminal blocks) of the modules.
2. If you change two adjacent existing single modules into dual-redundant configuration, pull out one of the modules and then insert it again.
3. Change the definition of dual redundancy specification, and perform online change download.
4. Connect the I/O cables (or terminal blocks).

Immediately after the online change download, the AIO/DIO modules go into the status described in the following warning; however, the state is restored when I/O cables (or terminal blocks) are connected.

CAUTION

- Input module
  An IOM fail occurs and the "input values at error occurrence" specified as the I/O parameters are set to all input channels. The data status changes to BAD.
- Output module
  An IOM fail occurs and the "Output value at fault" specified as the I/O parameters are set to the physical data of all output channels. The module goes to an output disable status.

Online change of I/O module device index

In order to change the device index of an I/O module, you must delete the I/O module and define it again. At the point I/O modules are deleted, the lock status of each channel of the modules is also canceled.
If you change a device index for a module of the same model installed in the same position by online change download, in the case of input modules, 0s (0 for DI and 0.0 for AI) are input to

the application logic at first and then the values from the field are input. In the case of output modules, the channels' outputs are disabled. FALSE for DO and tight-shut value for AO are output. After performing “output enabled operation”, the modules start to output the values of application logic.

Online change of the device index and element numbers for a fire and gas communication module

If you change the device index of a fire and gas communication module (model: S2LP131) and execute online change download, the S2LP131 restarts. The target S2LP131 will be unlocked upon executing the online change download even if you lock the S2LP131 before executing the online change download. Take appropriate measures against restarting of the communication module, such as to lock the outputs of the application logic that is using the data obtained through the target S2LP131.

When you change the element number of a %XW element, lock the outputs of the application logic that is using the FB wired to the element for which the element number will be changed. This is because if you change the element number of a %XW, an unknown value will be input to the FB that is wired to that element.

Online change of channel wirings

This section explains the system behavior when channel assignment is added, deleted, or changed and then online change download is executed. Note that the following cases are also included, in addition to simply adding, deleting, or changing channel assignments.

- When AIO/DIO module definitions are added, channel assignments are also performed at the same time
- When AIO/DIO module definitions are deleted, channel assignments are deleted
- When AIO/DIO module models are changed (when AIO/DIO module definitions are deleted once, then new AIO/DIO module definitions are added, and channel assignments are also performed at the same time)

IMPORTANT

- If you change the channel assignment and download the change, IOM downloading will not start automatically. However, if the I/O parameters are also changed, IOM downloading may automatically start depending on which parameters have been changed.
- When using S2MMM843 or S2MDV843 in an explosion protection system, refer to the following document without fail because the approved values of the explosion protection parameters are different depending on the signal type.

  ProSafe-RS/ProSafe-RS Lite Explosion Protection (TI 32S01J30-01E)

Online change of input channels

After online changing the input channel assignments, the logical data values of the assigned input variables will be set with the initial value of 0 (DI:FALSE; AI:0.0).Then, the values from the I/O modules will be used.

IMPORTANT

If you add the input channel assignment and the application accessing the input variable, and then the two are online change downloaded at once to SCS, 0 is set to the input variable for an instant before the actual values.

In this case, do the online change according to the procedure below:

1. Run online change downloading right after adding input channels.
2. Lock input variables.
3. Run online change downloading right after changing applications.

When the variable names of the previously assigned input variables are changed and online change downloaded, the input variables will immediately take the values from the I/O modules.

Online change of output channels

When the output channel assignments are added online, the added channels will not be able to output the logic values. The logic values can be output only after performing the "Output enable operation."
When the output channel assignments are changed, after online change downloading, the output values may be different from the previous values.

In this case, do the online change downloading according to the procedure below:

1. Lock the output variables.
2. Run online change downloading.
3. Unlock

When the variable names of the previously assigned output variables are changed and online change downloaded, the output channels will continuous to output the values through I/O modules.

Lock status at online changing of channels

When a locked channel is deleted from the assignment, the lock status of that channel will be released and deleted from the total number of locked channels of the whole station. Once a locked channel is deleted from the assignment and online change downloaded, the lock status of the channel will not be kept even when the channel is added to the assignment and online downloaded again.

Channel status at online changing

If the definition of assigned channels is deleted in online change to make them unassigned, the changed channels behave same as the other channels that are unassigned. As the result, channel status outputs for the system function block (such as CHn of SYS_OUTST or Q of SYS_CHST) become FALSE. Also the changed channels are excluded from representative alarm for the system function block (such as NRAL of SYS_OUTST, NRO of SYS_IOALLST, IOER of SYS_DIAG) and are not considered for diagnostic information marks on the SCS State Management window.

System alarm messages at online changing

When a channel that is causing an error is deleted from the assignment and online change downloaded, the recovery message for the channel will not be raised.

Operating mode at online changing

When an output disabled channel is deleted from the assignment and then online change downloaded, and the operating mode of the station may become Running due to the station does not have any output disabled channel. When an output channel is added to a station that in Running mode, and then online change downloaded the assignment, the status of the station may become Waiting due to the added channel is started in the output disabled status.

Online change of SCS link transmission

- Sequence of Adding and Deleting
  When adding a new data, it should be added first on the sender station. When deleting a data, it should be deleted from the receiver station. Doing this way is to avoid the application to access the deleted data.
- Lock the Link Transmission Data
  The link transmission data can only be locked together for the whole station. Locking one link transmission data, all the link transmission data in the station will be locked.

  Thus, when performing online change (adding or deleting) for link transmission data, the influence of the change to the logics should be properly checked, and then lock the proper variables at the proper places (such as link transmission data of sender station, link transmission data of receiver station or other individual internal variables).

IMPORTANT

For applications that require individual lock, connect the internal variable to lock them as follows:

- On Sender Station: Connect an internal variable to the input parameter of the link transmission output FB, and then lock it.

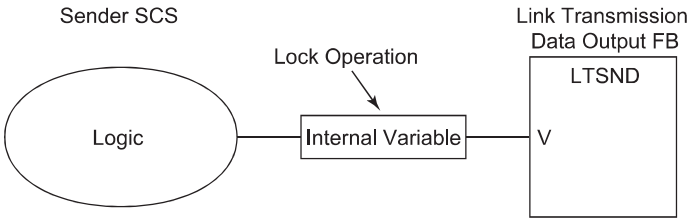


Figure E1.5-1 Lock on sender station

- On Receiver Station: Connect an internal variable to the output parameter of the link transmission input FB, and then lock it.

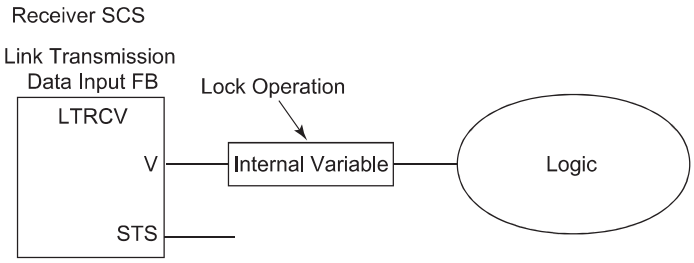


Figure E1.5-2 Lock on receiver station

- Add a logic that uses a link transmission data input FB

IMPORTANT

Do not add a link transmission data input FB and the logics connected to the FB at the same time during the online change. The influence to other logics may occur even if the link transmission received data are properly locked.

In this case, do the online change according to the procedure below:

1. Create a link transmission data input FB.
2. Online Change Download
3. Add a logic connecting to the link transmission data input FB.

- Change the Link Transmission Data Input FB Instance Name
  When a link transmission data input FB instance name is online changed, note that the output of the FB may become different.

  When changing the instance name online is necessary, do it according to the procedure below:

  1. Lock the internal variable that connected to the link transmission data input FB.
  2. Online Change Download

  If you cannot find a proper internal variable to lock, you need to add an internal variable to the output parameter of the link transmission data input FB, and then lock the variable. Then you can online change the instance name.

- Delete Link Transmission Data Output FB
  When a Link Transmission Data Output FB is deleted, the output data will be reset to 0. Even if the local station is locked to avoid bad influence, the receiver side is still affected since the linked data is reset to 0. Therefore, the FB in the receiver side should be deleted first.

- When Sending Definition of the SCS Link Transmission is Disabled
  When sending definition of the SCS link transmission is disabled during online change, data sending to other stations will stop. If another station is receiving data from the stopped station, the actions are shown as follows.

Table E1.5-2 Actions of Receiver Station

Receiver Station	Description
SCS	Since the updating of the safety information (such as sequence numbers or transmission timestamps) sent through the link transmission are stopped, an error will be indicated. The statuses of related input data will become BAD.
FCS	The last received data will be kept. The statuses of the related data will not become BAD.

Moreover, when the transmission size of the sender FCS is online changed to 0, the receiver station on SCS side will keep the last received data values. The data statuses will not become BAD.

Locking Inter-SCS safety communication and SCS link transmission data at online change

False trips caused by online changes can be prevented by locking inter-SCS safety communication data or link transmission data on the station where online change is performed. It is not necessary to lock data on the stations that receive data from the station where online change is performed.

The following figure illustrates an overview and the procedure for performing online changes.

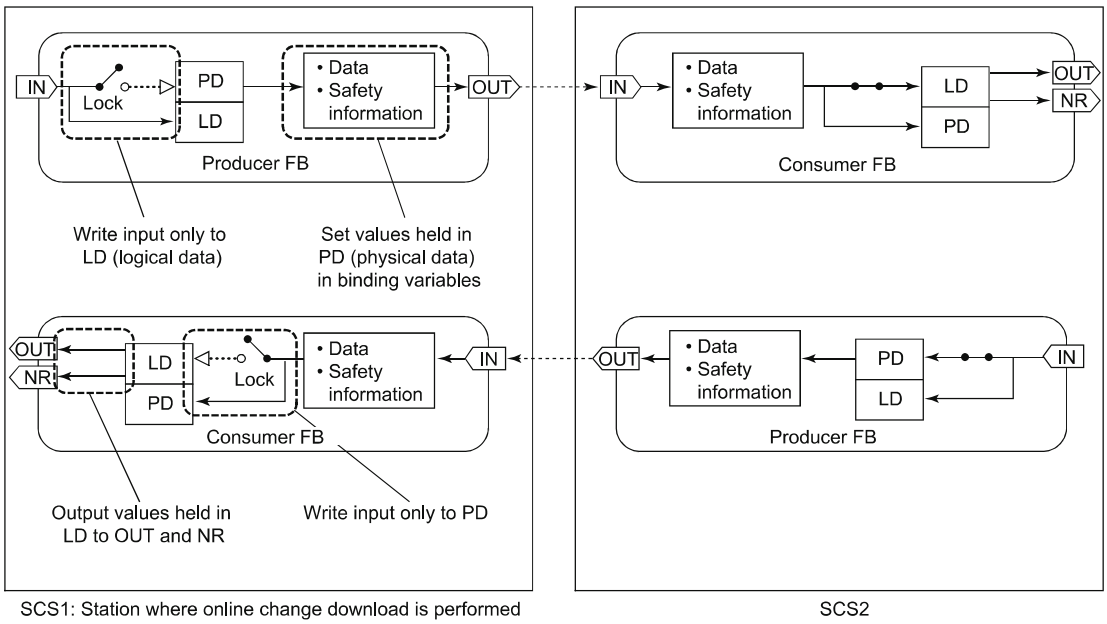


Figure E1.5-3 Example of locking Inter-SCS safety communication at online change

Follow these steps to perform online changes:

1. Set the security level of the SCS for which online change is to be performed to 1.

   Check that the SCS's security level has changed to 1 with diagnostic information messages.

2. Open the Inter-SCS Communication Lock Window or SCS Link Transmission Window of the SCS for which online change is to be performed and lock the sending and receiving data.

   Check that inter-SCS safety communication or link transmission safety communication has been locked with diagnostic information messages.

3. Execute online change download.

4. Check that the logical data and physical data match and that the data status is GOOD in the Inter-SCS Communication Lock window or SCS Link Transmission Lock window.

5. Unlock the sending and receiving data in the SCS in the Inter-SCS Communication Lock window or SCS Link Transmission Lock window.

   Check that the inter-SCS safety communication is unlocked with diagnostic information messages.

6. Set the security level of the SCS for which online change has been performed to 2.

   Check that the SCS's security level has changed to 2 with diagnostic information messages.

Online change download of input/output modules

In the online change download, you can perform changes in the redundant configuration, addition and deletion of I/O modules. If I/O modules are added through online change download, diagnostic information messages are issued to notify failure of I/O modules (No. 0081) and normal recovery of I/O modules (No. 0082).

Online change download of AIO/DIO module settings

When you perform online change download after you have made changes to the settings related to I/O parameter of AIO/DIO modules, IOM download may also take place depending on

the setting items you have changed. The AIO/DIO module continues its I/O operations when IOM download also takes place along with the online change download. The behavior of the SCS is as follows:

- The target modules continue their input/output operations.
- For AIO/DIO modules in redundant configuration, control rights are retained.
- The diagnostic information message of IOM Fail is not output.

Precautions related to fire and gas communication modules when downloading an online change onto SCS

Before online change downloading onto SCS, a dialog box asking the lock of S2LP131 may appear. In such case, before online change downloading onto the SCS, lock the S2LP131 shown in the dialog box. Lock by locking all inputs or by locking all communication definitions.

When not locking all inputs or all communication definitions, the following phenomenon will occur:

- The status of the LD (logical data) of Safety and Non-Safety data obtained via S2LP131 changes to Error.
- The locks of communication definitions partially locked may be released.

As these issues will lead to an unnecessary shutdown of the plant, lock S2LP131 before on-line change downloading.

E1.6 Precautions for online change download of N-IO

This section describes the I/O operation and extent of impact when online change is performed for definitions related to N-IO. Other than the online change of definitions in regard to N-IO, precautions are the same as those for online change download of FIO.

IMPORTANT

When using S2MMM843 or S2MDV843 in an explosion protection system, refer to the following document without fail because the approved values of the explosion protection parameters are different depending on the signal type.

ProSafe-RS/ProSafe-RS Lite Explosion Protection (TI 32S01J30-01E)

SEE ALSO For more information about precautions for online change download of FIO, refer to:

E1.5, “Precautions for online change” on page E1-20

Changing N-ESB bus coupler modules

When you add/delete N-ESB bus coupler module to/from the CPU node, the I/O operations at the I/O modules, other than the N-IO nodes at the connection destination, remain unaffected.

Changing N-IO nodes

When you add or delete an N-IO node, the I/O operations at the I/O modules, other than the related nodes, remain unaffected.

Even when you perform online change for the setting values of N-IO nodes, I/O of the related nodes remain unaffected.

Changing I/O modules of N-IO nodes

The configuration information of an I/O module is downloaded in either of the following ways:

- IOM continuous download: A download wherein the I/O operations at the points other than the changed points continue.
- IOM initialization download: A download wherein the I/O operations of all points of changed I/O modules stop.

In the online change with IOM download, IOM continuous download is executed. During the IOM continuous download, the I/O operations continue.

When you add an I/O module, IOM initialization download is executed. After the IOM initial download, the operation at the IOM startup is executed.

When you add or delete an I/O module, only the I/O operations of the related I/O module are affected.

The deleted I/O module will be in the fall-back state due to being separated from the CPU. This is the same as when the I/O module of the FIO node is deleted.

■ Changing the channels of the I/O module of the N-IO node

When changing the signal type of the channels of the universal type I/O module, you need to reassign I/O variables that are appropriate for the type of signal to which the change is being made.

When the channel being deleted (subject to deletion of variable assignment) is locked, the locked status will be released after the channel is deleted.

Changing the channel assignment is the same as with the I/O module of the FIO node with the exception of the status of the deleted channel.

TIP

The deleted channel will be in an undefined state with the universal type I/O module.

SEE ALSO

For more information about change of channel wirings, refer to:

"■ Online change of channel wirings" on page E1-24

■ Changing the signal category of channels (only for universal type I/O modules)

When changing the signal category of the channels of the I/O module, you need to reassign I/O variables that are appropriate for the category of signal the change is being made to. When you have changed the signal category of channels, IOM download is executed. The operation of the I/O module after download is completed is as follows:

● Changing to a different signal category input

When you change the channel of I/O module to input of a different signal category, after the internal change process in the I/O module completes, the values are newly read from the fields.

TIP

The logical data that is configured to the channel will differ depending on the signal category before and after the change.

- When changing from AO to DI, DO to AI, AI to DI, or DI to AI
  After "0" (FALSE for DI, 0.0 for AI) is configured for the logical data, the input value from the channel is reflected.
- When changing from AO to AI, DO to DI, AI to AI, or DI to DI
  After the value from before the change is configured for the logical data, the input value from the channel is reflected.

When you change the signal category from current input (AI) to current input with HART (AI_HART), or, from current input with HART (AI_HART) to current input (AI), the channels continue their operation even during IOM download. In this case, you do not need to reassign the I/O variables.

● Changing to a different signal category output

When you change the channel of I/O module to output of a different signal category, after internal change process in the I/O module completes, DO outputs 0 and AO outputs tight-shut output value to the field. The output values from the application logic will be output to the field after you perform the output enable operation.

When you change the signal category from current output (AO) to current output with HART (AO_HART), or, from current output with HART (AO_HART) to current output (AO), the channels continue their operation even during IOM download. In this case, you do not need to reassign the I/O variables.

Changing to a high current output

You can change from a high current output type signal to a signal of other type or category by online change.

- When changing from status output (DO) to high current output (DO_1.3A or 2A), or, from high current output (DO_1.3A or 2A) to status output (DO), you do not need to reassign the I/O variables.
- When changing from the output other than status output (AI, AO, DI) to high current output (DO_1.3A or 2A), or, from high current output (DO_1.3A or 2A) to the output other than status output (AI, AO, DI), you must reassign the I/O variables.

IMPORTANT

If the second and the third channel of the channels that you try to define in DO of high current output are already defined as a different channel, the intended channels cannot be defined in the high current output.

The channels that are changed to high current output (DO_1.3A or 2A) will output 0 and go into output disable status. The output values from the application logic will be output to the field after you perform the output enable operation. Only the channels that are targeted for online change are affected.

Operating mode upon online change of the channel signal category

The changes of the operating mode upon online change of the channel signal category are as follows:

- When changing to AO or DO
  The change is the same as when an output channel assignment is added. As the channel for which assignment has been changed will start in a state where output is disabled, the operating mode will be Waiting.
- When changing to AI or DI
  The change is the same as when an output channel assignment is deleted. When output disabled channels no longer exist in the station, the operating mode becomes Running.

SEE ALSO For more information about operating mode upon change of channel wirings, refer to:

"● Operating mode at online changing" on page E1-25

E1.6.1 Procedure for online change download of signal category of channels

There are the following three cases for online change download of the signal category (AI, AO, DI, DO) of channels in the universal type I/O module:

- Change from other than DO to other than DO
- Change from other than DO to DO
- Change from DO to other than DO

IMPORTANT

- You must follow this procedure when performing online change download of the signal category of channels. Otherwise, it may lead to the failure of field devices at the connection destination.
- When you change the signal category from/to DO for a module that is installed on a base plate with disconnecting terminal, disable the ON pulse diagnosis (pulse test (ON) or low voltage pulse test (ON)), set the DO to OFF, and then open or close the disconnecting terminal.
- In the Zone2/Div2 area, removal or installation of barrier cards while they are powered is prohibited. Do not remove or install barrier cards.

Changing the signal category from other than DO to other than DO

Follow these steps to change and online change download the signal category of channels from other than DO to other than DO:

1. Lock the channels to be changed.
2. Perform the following operation based on the type of the base plate used:
   - For base plate with disconnecting terminal
     Open the disconnecting terminals of the channels to be changed.
   - For a base plate with barrier
     Remove the barriers of the channels to be changed from the base plate.
3. On SENG, change the signal category of the channels.
4. Run online change download from SENG.
   When the download is successful, confirm that no abnormality is found in the I/O modules by checking the SCS status display or the LED lamps of the I/O modules.
5. Replace the field devices that are connected to the channels that have been changed.
6. Perform the following operation based on the type of the base plate used:
   - For base plate with disconnecting terminal
     Close the disconnecting terminals of the channels that have been changed.
   - For a base plate with barrier
     Install the barriers of the channels that have been changed on the base plate.
7. Unlock the locked channels.
8. For an output channel, perform output enable operation.

Changing the signal category from other than DO to DO

Follow these steps to change and online change download the signal category of channels from other than DO to DO:

1. Lock the channels to be changed.
2. Perform the following operation based on the type of the base plate used:
   - For base plate with disconnecting terminal
     Open the disconnecting terminals of the channels to be changed.
   - For a base plate with barrier
     Remove the barriers of the channels to be changed from the base plate.
3. On SENG, change the signal category of the channels to DO. At the same time, disable the ON pulse diagnosis of the channels.
4. Execute online change download from SENG.
   When the download is successful, confirm that no abnormality is found in the I/O modules by checking the SCS status display or the LED lamps of the I/O modules.
5. Replace the field devices that are connected to the channels that have been changed.
6. Perform the following operation based on the type of the base plate used:
   - For base plate with disconnecting terminal
     Close the disconnecting terminals of the channels that have been changed.
   - For a base plate with barrier
     Install the barriers of the channels that have been changed on the base plate.
7. As necessary, enable ON pulse diagnosis.
8. Execute online change download from SENG.
9. Unlock the locked channels.
10. Perform the output enable operation.

Changing the signal category from DO to other than DO

Follow these steps to change and online change download the signal category of channels from DO to other than DO:

1. Lock the channels to be changed. When the high current output is set, you need to lock the primary channel only.
2. Perform the following operation based on the type of the base plate used:
   - For base plate with disconnecting terminal
     a. Disable the ON pulse diagnosis of the DO channels.
     b. Execute online change download from SENG.
        When the download is successful, confirm that no abnormality is found in the I/O modules by checking the SCS status display or the LED lamps of the I/O modules.
     c. Perform the output enable operation for the channels that have been changed
     d. Open the disconnecting terminals of the channels to be changed. When the high current output is set, you need to perform the operation for all target channels.
   - For a base plate with barrier
     Remove the barriers of the channels to be changed from the base plate.
3. On SENG, change the signal category of the channels.

4. Run online change download from SENG.
   When the download is successful, confirm that no abnormality is found in the I/O modules by checking the SCS status display or the LED lamps of the I/O modules.
5. Replace the field devices that are connected to the channels that have been changed.
6. Perform the following operation based on the type of the base plate used:
   - For base plate with disconnecting terminal
     Close the disconnecting terminals of the channels that have been changed.
   - For a base plate with barrier
     Install the barriers of the channels that have been changed on the base plate.
7. Unlock the locked channels.
8. For an output channel, perform output enable operation.

E1.7 Online change of subsystem communication modules

This section describes online changes such as the addition/deletion/dual-redundancy specification of subsystem communication modules, changes to settings relating to communication inputs and outputs, the addition/deletion of subsystem communication I/O FBs, and changes to wiring for subsystem communication I/O FBs.

SEE ALSO For more information about precautions during online changes of a subsystem communication module, refer to:

"■ Precautions related to fire and gas communication modules when downloading an online change onto SCS" on page E1-29

■ Locking of subsystem communication data

By locking subsystem communication data, you can reduce the impact of online changes on the application logic or prevent erroneous outputs to subsystems resulting from application logic correction errors.
Subsystem communication data cannot be locked once an online change download is started. Lock subsystem communication data before starting an online change download.

To change a communication input/output definition from any SCS Manager window or builder, close the Communication I/O Lock window first. After the online change is completed, display the Communication I/O Lock window again, if necessary.

Table E1.7-1 Relationship of online changes and locking of communication modules

Content of change	Lock
Change a transmission definition	Required (inputs/outputs need to be locked).
Add, change or delete a communication definition	
Add a subsystem communication I/O FB	
Change the wiring of a subsystem communication I/O FB	
Change an error handling action(*1)	
Delete a subsystem communication I/O FB	Not required.

*1: If a setting is changed while an error occurs, input values will change. Subsystem communication outputs are not affected.

■ Online change procedure

The procedure for making an online change is as follows:

1. Change the application logic and perform build.
2. Check the application logic for consistency using Integrity Analyzer.
3. Check the range to be tested using Cross Reference Analyzer.
4. Change the SCS's security level to Level 1.
5. Lock the inputs/outputs of subsystem communication data in accordance with what you have changed.
6. Close the Communication I/O Lock window.
7. Perform an online change download.
8. Open the Communication I/O Lock window.
9. Test the modified application logic.

10. Unlock the inputs/outputs of subsystem communication data.
11. Reset the SCS's security level to Level 2.
12. Save the SCS project using Version Control Tool.

Addition, deletion, and dual-redundant specifications of subsystem communication modules

Addition, deletion, and dual-redundant specifications of subsystem communication modules can be changed online.

Online changes relating to communication inputs/outputs

When changing a communication I/O setting in the Communication I/O Builder or Safety Communication I/O Editor, also change the wiring of the subsystem communication I/O FB affected by the change.

Online change download

If an online change download is to be performed after a communication input/output data or subsystem communication module setting has been changed, the subsystem communication data of the target subsystem communication module needs to be locked before commencing the online change download. If the subsystem communication data of the target module is not locked, the application logic will be affected by a restart of the subsystem communication module.

The subsystem communication module will restart after the online change download is completed. After the subsystem communication module has been restarted, unlock the subsystem communication data of the module.

Online changes relating to subsystem communication I/O FBs

Adding a subsystem communication I/O FB

If a subsystem communication I/O FB is added, the FB also needs to be wired. If the FB is not wired, a build error will occur.

Before performing an online change download to add a subsystem communication I/O FB, the communication I/O data of the target subsystem communication module needs to be locked.

An online change download to add a subsystem communication I/O FB is performed as a series of multiple scans. Specifically, the subsystem communication I/O FB is added first, and then the wiring is changed. As a result, the added FB is not wired while the online change download is in progress. The subsystem communication I/O FB temporarily assumes the following status during the download:

- Subsystem communication input FB: The data value is 0. The data status is FALSE.
- Subsystem communication output FB: The data value is ignored. The data status is FALSE.

The subsystem communication module will restart after the online change download is completed. Once the subsystem communication module has been restarted, unlock the subsystem communication data of the module.

Deleting a subsystem communication I/O FB

When deleting a subsystem communication I/O FB, also delete the wiring of the FB.

Changing a wiring

Before performing an online change download, the subsystem communication data of the target subsystem communication module needs to be locked. To change the wiring of a subsystem communication I/O FB between two subsystem communication modules, subsystem communication data needs to be locked for the subsystem communication module that contains the wired communication data before the change, as well as the subsystem communication module that will contain the wired communication data after the change. If the data of both modules is not locked, subsystem communication data will be immediately input to the application logic after the online change download is completed, and outputs from the application logic will also be output to subsystems immediately after the download.

Each subsystem communication module will restart after the online change download is completed. Once the subsystem communication module has been restarted, unlock the subsystem communication data of the module.

Changing a POU that includes subsystem communication output FB

To change a POU containing a subsystem communication output FB, the communication output data of the subsystem communication module wired to the applicable subsystem communication output FB needs to be locked.

E2. Import/Export function

The application data of a project can be exported to an external file, and the application data in an exported file can also be imported to a project. This function can be used when diverting or regenerating SCS projects during SCS expansion or reformation.

This function cannot be used together with iDefine projects. Application data that was created by using iDefine need to be controlled under the project management by iDefine.

E2.1 Precautions concerning import/export

This section summarizes the precautions to take when you perform an import or export. You must observe these precautions when carrying out the actual operation.

Outline of import/export

The import/export functions support modifying and reusing SCS project databases. Import/export should be executed from AD Organizer or SCS Manager, depending on the purpose. For example, execute import/export by using SCS Manager for data that is managed by SCS Manager.

However, some of the targets of import/export using SCS Manager will differ depending on the engineering method.

Precautions on compatibility (including import from builders)

- When importing the files created in the previous software release number of SENG, the setting values for the new items supported only in the newer software release number of SENG will be the default values.
- The files exported from the project created on newer software release number SENG cannot be imported to the project opened on the older software release number SENG.

Precautions on password

When importing a project to replace an old project, the passwords of project and POUs are also imported and the old passwords will be replaced.

Therefore, when using export and import, you should manage the project password and the passwords of POUs for exported project.

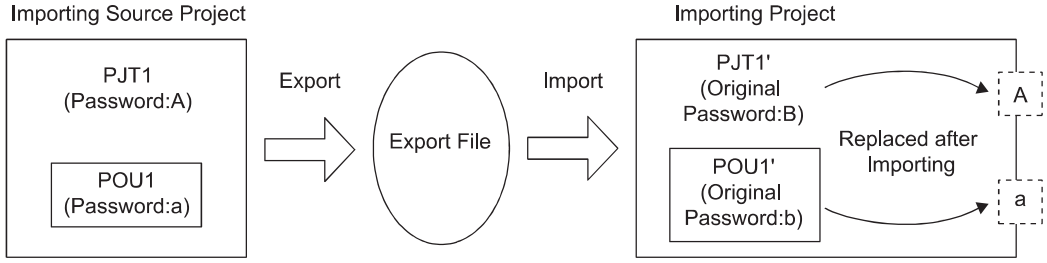


Figure E2.1-1 Passwords replaced after importing

The effects regarding passwords after importing are shown as follows:

- When importing the exported project files with passwords, the passwords of exported project and POUs are also imported and the existing passwords will be replaced. After importing, the passwords of the imported project will be required to open the project, without the passwords, the imported project cannot be opened for editing.
- When importing those POUs that are protected by passwords, the passwords of the existing POUs will be replaced by the passwords of the imported POUs. So, after importing, the passwords of the imported POUs will be required to open the POUs, without the passwords, the imported POUs cannot be opened for editing.

How imported POUs are handled in Cross Reference Analyzer

If the POU to be imported has an identical name with an existing POU, the Cross Reference Analyzer will act as follows:

If the POU to be imported is exactly the same as the existing POU, the Cross Reference Analyzer will mark the POU as "Unchanged POU" and display it in green icon. If the POU to be imported is discrepant from the existing POU, the Cross Reference Analyzer will mark the POU as "Changed POU" and display it in red (Modified) icon.

How to check when project data is migrated by export or import

How to check differences in the imported data after migration of project data by import/export is as follows:

Table E2.1-1 Builder definitions and how to verify

Builder	Data	How to Verify
SCS Manager	POU	Cross Reference Analyzer
	I/O Wiring	Cross Reference Analyzer
	Binding	Cross Reference Analyzer
SCS Project Properties	Domain/Station number	Project Comparing Tool
	CENTUM Project Folder	Project Comparing Tool
Configuration Properties	Target	Project Comparing Tool
	Memory size for temporary variables	Project Comparing Tool
Connections	IP Address	Project Comparing Tool
Resource Properties	Resource Number	Project Comparing Tool
	Cycle Timing	Project Comparing Tool
	Memory size for online changes-Code	(Fixed value) (*1)
	Memory size for online changes-User variable size	Project Comparing Tool
SCS Constants Builder	Interval of Repeated Warning Alarms	Project Comparing Tool
	Synchronous Mode	Project Comparing Tool
	Scan Period for External System	Project Comparing Tool
	Modbus Word Order	Project Comparing Tool
	Alarm Notify Action when AOF Released	Project Comparing Tool
	PV Status of S_ANLG_S	Project Comparing Tool
	Optical ESB Bus Repeater/Maximum Extension Distance (*1) SCS Constants Builder	Project Comparing Tool
	Extend Scan Period Automatically (*1)	Project Comparing Tool
	Behavior at Abnormal Calculation (*1)	Project Comparing Tool
	Automatic IOM Download (*1)	Project Comparing Tool
	Locking of Internal Variables (*1)	Project Comparing Tool
	Device Power-Off Period (*1)	Project Comparing Tool
	Device Startup Waiting Period (*1)	Project Comparing Tool
	Alarm Suppression During Device Reset (*1)	Project Comparing Tool
	16-bit Modbus master support mode	Project Comparing Tool
	DNP3 Slave Function (*1)	Project Comparing Tool
	Skip Password Dialog Box for Manual Operation FB (*1)	Project Comparing Tool

Continues on the next page

Table E2.1-1 Builder definitions and how to verify (Table continued)

Builder	Data	How to Verify
I/O Parameter Builder	Node parameter (Extends Node Bus/ Extends To (Km) for Optical ESB Bus Repeater) (*1)	Project Comparing Tool
	Module parameter	Cross Reference Analyzer
	Channel parameter	Cross Reference Analyzer
Communication I/O Builder	Communication I/O definition	Cross Reference Analyzer
	Communication I/O wiring	Cross Reference Analyzer
SCS Link Transmission Builder	SCS Link transmission data definition	Cross Reference Analyzer
	Wiring definition	Cross Reference Analyzer
Modbus Address Builder	-	Project Comparing Tool
DNP3 Communication Builder (*1)	-	Project Comparing Tool
Tag Name Builder	-	Project Comparing Tool
Alarm Priority Builder	-	Project Comparing Tool
Alarm Processing Table Builder	-	Project Comparing Tool

*1: The corresponding item may not exist or the configurable value may be different depending on the software release number of the system or SCS type. Such items may therefore be picked up as discrepancies by the Project Comparing Tool.

E2.2 Export/import using AD Organizer

This section describes the procedures for exporting/importing SCS project data by using AD Organizer and the procedure for deleting an SCS project by using AD Organizer.

TIP

When engineering by using iDefine, the engineering data that was defined by using iDefine is also imported and exported to SCS projects. In addition, the setting information on FB types to be converted to instances is also included. The iDefine project itself is not imported or exported.

Exporting SCS projects

You can export SCS projects to a specified location. The export file includes SCS project information defined in SCS Manager, the safety I/O, safety communication I/O, nodes, and IOM definitions under the corresponding SCS project in AD Organizer but does not include history information. Follow these steps to export an SCS project:

1. On the System Structure Navigator, select one or multiple SCS projects.
2. Right-click and select [Export SCS].
   The Select Folder dialog box appears.
3. Specify the folder to which the project is to be exported and click [OK].
   When the export is complete, the following result appears.
   - All exported SCS projects
   - List of files at the export destination
   - List of SCS projects for which export failed and reasons of failure

Importing SCS projects

You can import the exported SCS projects. You can specify the SCS projects that were exported from the same AD project or different AD projects, and import them into the RS project.

You need to perform the following procedure to import the project:

1. On the System Structure Navigator, select the RS project folder.
2. Right-click and select [Import SCS].
   The Import SCS dialog box appears.

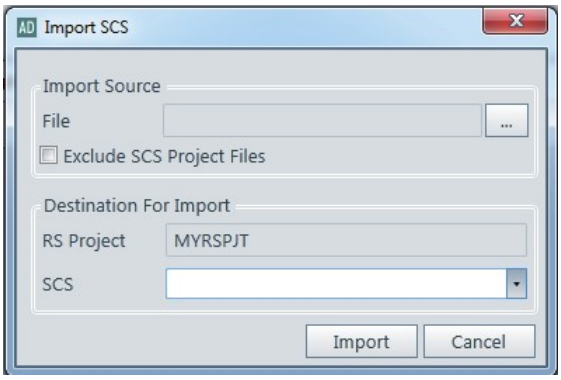


Figure E2.2-1 Example of SCS project import settings

3. Click the […] button on the right side of [File] text entry box and select one SCS project to be imported.
   If you want to import the SCS data other than the data of the SCS project in the specified folder, select the [Exclude SCS Project Files] check box.
4. Perform either of the following operations:
   - From the [SCS] drop-down list, select the SCS name of the import destination.

- Enter a new SCS name.

5. Click the [Import] button.

   If you selected an SCS name from the [SCS] drop-down list, the existing SCS project is overwritten.

   If you entered a new SCS name, a new SCS project is created. Using SCS Manager, change the setting items of the new SCS project to the appropriate values.

Responding to an error when importing an SCS project

- If an error occurs when you import an SCS project, do the following:
  - If the error is due to duplicate P&ID tags, the corresponding safety I/O list and safety communication I/O list are imported in a checked-out state. Start Safety I/O Editor or Safety Communication I/O Editor, correct the P&ID tag, and then perform a check-in.
  - If the error is due to a missing P&ID group, create a safety I/O list or safety communication I/O list with the name of the P&ID group that you want to set under the [I/O-List] folder in System Structure Navigator.

SEE ALSO For more information about precautions for importing an SCS project including the safety I/O list with the safety I/O parameter profile assigned, refer to:

"■ Importing SCS" on page D1-40

Deleting SCS projects

You need to perform the following procedure to delete the SCS project:

1. Use the Windows function to delete the SCS project data to be deleted from the RS project folder.
2. From the menu bar of the System Structure Navigator in AD Organizer, select [Display] > [Update].
   The status of the target SCS is updated. The SCS projects created with RS original engineering are deleted.
3. To delete the SCS project created with I/O list engineering, specify the target SCS project under the RS project in the System Structure Navigator and click [Delete] on the toolbar.
   All the data under the deleted project of the RS project database is deleted, and the IOM definition information related to the deleted project is deleted from AD Organizer.

E2.3 Importing and exporting data that is managed by SCS Manager

By using SCS Manager, you can export/import the application data that is managed in SCS Manager to/from external files. In addition to SCS Manager, some builders also support exporting to and importing from external files.

TIP

In I/O list engineering, both SCS Manager and AD Organizer are used to import/export project data.

This section describes the importable and exportable files, and whether online change download is possible after the import.

SCS project application data exportable by SCS Manager

The units of application data of an SCS project that can be exported by the SCS Manager and the menu item names displayed under [Export] of the [File] menu are as follows.

Table E2.3-1 Specifying export data and Export menu items

Specifiable export data		Menu item	Detailed menu item
Project	Entire SCS project	Project	Entire Project (*1)
	Defined words		Defined words
Resource	Resource properties	Resource	Properties
	I/O device instances (*2)		I/O Device Instances
	Global variables (*2)		Global Variables
	Wiring variables (*3)(*2)		Wiring Variables
	External bindings (*4)		External Binding
POU		POU	
Variables (*5)		Variables	
Defined words		Defined words	
SCS Project Properties		- (*6)	

*1: If you select this item, all the data shown in the table other than SCS project properties are exported.
*2: The function for exporting data in the format of a PXF file cannot be used while implementing I/O list engineering.
*3: Only wired variables among global and local variables are exportable.
*4: Only binding variables among global variables and binding groups are exportable.
*5: When I/O list engineering is being implemented and data is being exported in the CSV format, the variables reflected from Generation Manager will not be exported while all other variables will be exported.
*6: You cannot use the [File] menu to export SCS Project Properties. To export SCS Project Properties, start the Engineering Launcher in SCS Manager, and use the [Export] button in the SCS Project Properties dialog box.

Application data imported by SCS Manager

When you import data from data files of an SCS project using SCS Manager, you can import all of the exported data as a whole or selectively import data by specifying only the lower-level data units you want to import. When you import data from other data files, all of their exported data will be imported. However, if any of the project name, configuration name or resource name in the data file for import do not match their counterparts in the destination project, an error dialog box appears and the import ends up in a failure.

Table E2.3-2 Application data selectable for import

File format	Exported data file	Data unit selectable for import
Binary (PXF format)	Entire SCS project	Project
		POU (you can select multiple POUs)
	Defined words	Defined words
	Resource properties	Resource properties
	I/O device instances	I/O device instance (*1)
	Global variables	Global variable (*1)
	Wiring variables	Wiring variable (*1)
	External bindings	External bindings
	POU	POU
Text (CSV format)	Variables	Variable (*2)
	Defined words	Defined words
	SCS Project Properties (*3)	SCS Project Properties

*1: The import function cannot be used while implementing I/O list engineering.
*2: When performing I/O list engineering, variables of the same name as the variables reflected from Generation Manager will not be imported while all other variables will be imported.
*3: The operations to import SCS Project Properties differ from those for other data. Import using the [Import] button of the SCS Project Properties dialog box.

IMPORTANT

Files with the same software revision number for SENG can be imported. Using SENG to open an SCS project created with an earlier version will make it possible to import that file as well.

Availability of online change download is determined for the imported application data based on the same conditions as those for the change of application data without using an import.

Builders supporting import/export

The table below shows a list of builders that support Import/Export and whether the 'online change download' is allowed for the imported builder files.

Table E2.3-3 Builders supporting import/export and online-changeability of their files

Builders supporting Import/Export	Online change download (*1)
SCS Constants Builder	No (*2)
I/O Parameter Builder	Yes
Communication I/O Builder	Yes
SCS Link Transmission Builder	Yes
Modbus Address Builder	Yes
DNP3 Communication Builder (*3)	No (*4)
Tag Name Builder	Yes
Alarm Priority Builder	No
Alarm Processing Table Builder	No

*1: Yes: Online change downloading possible
No: Online change downloading not possible
*2: Items for which online change download can and cannot be performed both exist in items configured in the SCS Constants Builder. Check the link included at the end of this section.
*3: Export/Import is possible only for the SCS projects of SCSU1 that are created by the software version R3.02.20 or later.

*4: Items for which online change download can and cannot be performed both exist in items configured in the DNP3 Communication Builder. Check the link included at the end of this section.

IMPORTANT

If you import text files that were exported from builders, do not edit the exported files before you import them. Only the text files that were exported from builders are importable; do not import other files.

Exporting a Builder file: On the [File] menu, click [External File] and then click [Export]. The data of the Builder file of the currently opened Builder is exported to an external file.

Importing a Builder file: On the [File] menu, click [External File] and then click [Import]. The data that was exported to the external file is imported and the data of the imported Builder file is shown in the currently opened builder window.

SEE ALSO For more information about whether online change download is possible for each definition item in the builder, refer to:

"■ Builder definitions that are changeable with online" on page E1-16

■ Precautions on handling CSV files

Do not edit CSV files that are exported from SCS project data by using an editor. If you import an edited CSV file in SCS project data, the operations are not guaranteed.

■ Precautions on the importing sequence

When importing individual global variables or individual POUs, the sequence of importing is as follows:

1. POU (Function Block)
2. POU (Other than Function Block)
3. Global Variables

- If you import global variables before importing the POU (Function Block), the Type information regarding the imported global FB instance may be missing. As a result, "???" will be shown in the Type column of Dictionary.
- If you import POU (other than Function Block) before importing the POU (Function Block), the Type information regarding the imported local FB instance may be missing. As a result, "???" will be shown in the Type column of Dictionary.
- If a user-defined function block (such as FB1) is using another user-defined function block (FB2) as a local parameter and FB1 is imported before FB2, the Type information regarding the imported local parameter type may be missing. As a result, "???" will be shown in the Type column of the parameter in Dictionary. The function blocks used as parameters should be imported before.

If the above sequence is not observed when importing the individual global variables or POUs, a build error will occur. In this case, import again in the above-mentioned order.

■ Unit for exporting and sequence of importing

This section describes the file formats that are used when exporting SCS project data and actions that are carried out while importing. SCS projects can be exported as binary (PXF format) files. SCS project properties and SCS constant data can be exported in CSV files.

Import/export in PXF format

Even if you have exported data for individual SCS projects in binary (PXF format) files, you can import data selectively (you can import the POUs you need) from the exported data.

The actions during importing are shown in the following table.

Table E2.3-4 Actions during importing

Imported Contents	Actions during Importing
Project	Deletes the existing project first and then adds the imported project in PXF files. Importing projects is only possible when the project name, configuration name and resource name of the source project match with those of the existing project.(*1)
POU	• Deletes the existing POU with the identical name when adding the POUs from PXF files. • POU name can be changed during importing. • When you import multiple POUs at one time, you can choose whether to import them without changing their name (by deleting any existing POUs and adding them with the same name) or by automatically renaming any POUs with the same name to non-duplicate names. • When importing a local instance where the FB is not defined in the existing project, the variables with unknown types will be generated and build error will occur. To solve this problem, you can either define a new FB before importing or import the FB.
Resource properties	Overwrites all the existing properties of the resource.
I/O device instances (*2)	• If the imported I/O device has different index number with the existing I/O modules, the imported I/O device will be added as a new I/O module. • If the imported I/O device has an identical index number with the same type of existing I/O module, the IOM parameters (node address, slot numbers and redundancy setting) of the imported I/O device will be added to replace the existing I/O module. • If the imported I/O device has an identical index number with a different type of existing I/O module, a warning message will be displayed and the I/O device will not be imported. The existing I/O module will not be changed.
Global variables (*2)	• If the imported variable is different from the existing variable, the imported variable will be added as a new variable. • If the name and scope of the imported variable are identical with the existing variable, the imported variable will be added to replace the existing variable. • If the existing variable is wired with other variable in the same channel, the imported variable will replace the existing variable and be wired with the other variable. • When importing an instance where the FB is not defined in the existing project, the variable with an unknown type will be generated and a build error will occur. To solve this problem, you can either define a new FB before importing or import the FB.
Wiring variables (*2) (I/O variables)	• If the imported variable is different from the existing variable, the imported variable will be added as a new variable. • If the name and scope of the imported variable are identical with the existing variable, the imported variable will be added to replace the existing variable. • If the existing variable is wired with other variable in the same channel, the imported variable will replace the existing variable and be wired with the other variable. • When importing an instance where the FB is not defined in the existing project, the variable with an unknown type will be generated and a build error will occur. To solve this problem, you can either define a new FB before importing or import the FB.

Continues on the next page

Table E2.3-4 Actions during importing (Table continued)

Imported Contents	Actions during Importing
Binding	• If the imported binding group has a different group ID from the existing binding group (either Consumer Group or Producer Group), the imported group will be added as a new group. • If the imported binding group has an identical group ID to an existing binding group (either Consumer Group or Producer Group), the imported group will be added to replace the existing group. • If the imported binding variable has different name from the existing binding variable, the imported binding variable will be added in a binding group.
Defined words	• If the imported defined words have a different name from the existing defined words, the imported defined words will be added as a new defined words. • If the imported defined words have an identical name with the existing defined words, the imported defined words will be added to replace the existing defined words.

*1: When importing the entire projects, an error dialog box appears if any one of the project name, configuration name and resource name of the importing source project does not match with that of the existing project.
For instance, if the entire SCS project of SCS0101 is exported, it is not allowed to import the entire project as SCS0102. If you wish to export the entire project and import it to an SCS project with a different name, create a new project with the same name as the importing source project, perform import operation, and then change the project name, configuration name and resource name to the desired names before using the project.
*2: Cannot be imported when I/O list engineering is applied.

Import/export of SCS Project Properties

You can export SCS Project Properties as a CSV file, but this does not mean that all of the data will be applied when you import it. Actions during import are shown in the following table:

Table E2.3-5 Actions when importing SCS Project Properties

Items	Actions during Import
Station Type	Reflected only when importing during new project creation
Database Type	Not reflected
Station Address	Reflected
Domain Number	Reflected
Station Number	Reflected
IP Address	Not reflected
Component Number	Reflected
Version	Not reflected
CENTUM Project Folder	Reflected
SCS Project Attribute	Not reflected
Originally Created	Not reflected

Import/export of SCS constants

SCS constants can be exported in a CSV file. However, when you import the constants, the default value may be used if the setting does not exist, depending on the software release number of your system and the SCS type. If the settable values are different, they will need to be changed. If you do not change them, an error will occur at build time.

SEE ALSO For more information about importing or exporting PXF files and CSV files, refer to:

E2.3, “Importing and exporting data that is managed by SCS Manager” on page E2-7

E3. Modification and reuse of SCS project database

This section describes the procedures for expanding or remodeling an existing SCS project, recreating an SCS project, and so on by using the import/export functions.

The source project and the destination project for import must be registered in different AD projects.

E3.1 Data transfer procedure during expansions/remodeling in modifications where online change is possible

This section describes the procedure for applying the results of making a modification that can be changed online from a user-defined project to the current project. This procedure involves exporting the results from the user-defined project and only importing the data that has been modified into the current project.

TIP If all the changes were made by using iDefine and none was made by using SCS Manager when engineering by using iDefine, importing the same iDefine-config file to the current project reflects all the changes.

IMPORTANT

- Do not forget to import all the modified content.
- Confirm that the current project has not been changed manually before importing.

The overall flow of the procedure is as follows:

1. If a POU included in a library has been modified, first update the original library project with the modifications required, and then copy the modifications to the library of the current project.
2. If an SCS project has been modified, apply the modifications from the user-defined project to the current project.
3. Perform an online change download of the SCS project.

SEE ALSO For more information about importing or exporting PXF files and CSV files, refer to:

E2.3, “Importing and exporting data that is managed by SCS Manager” on page E2-7

Library POU data transfer in modifications where online change is possible

If you are using library POUs, use the Import/Export function to apply the modifications from the library in the user-defined project to the original library.

- By way of preparation, back up the original library using the Version Control Tool.

Exporting library POU source data where online change is possible

Export the library Program Organization Unit (POU) source data.

- Export the data from the library of the project at the origin of the import to create the following PXF file or CSV file.
  - A PXF file of the entire library project.
  - When reflecting the addition/modification of a global variable being used in the library project, create a PXF file or CSV file of the global variable. (*1)
  - When reflecting the addition/modification of a definition word being used in the library project, create a PXF file or CSV file of the global variable (*1)

*1: When performing RS original engineering, create a PXF file. When performing I/O list engineering, create a CSV file.

Importing library POU data where online change is possible

1. Open the original library with SCS Manager and import the required data from the exported PXF or CSV files.
   1-1 In the Import dialog, specify the PXF file containing the entire exported library project and import only the modified POUs (*1)
   1-2 When importing global variables, in the Import dialog box, specify the PXF file or CSV file (*2)that contains global variables and perform the import. Import the data upon making a specification in the import dialog box.
   1-3 When importing defined words, specify the PXF file or CSV file of the defined word in the import dialog box and import (*2)

   *1: In the course of importing, if the POU contains any FB that does not exists in the current project, the following warning message will be displayed. In such a case, a build error will occur when building the project.
   Warning: Type 'UFB' for symbol 'iUFB' was not found in this project.
   or
   Warning: Type 'UFB1' for Parameter 'iUFB1' was not found in this project.
   'UFB', 'UFB1': FB Name
   'iUFB', 'iUFB1': FB Instance Name
   *2: When performing RS original engineering, import the PXF file. When performing I/O list engineering, import the CSV file.
2. Delete any global variables and defined words that are not required after importing. The variables that are not used in POU can be checked in the Browser. Start the Browser and generate (or refresh) the cross-reference information for checking the unused variables.
3. Perform build.
4. Validate the contents on the Integrity Analyzer.
5. Copy the original library to the LIBRARIES folder of the current project.

SCS project data transfer in modifications where online change is possible

Apply the modifications from the modified user-defined project to the current project using the Import/Export function.

- By way of preparation, back up the current project using the Version Control Tool.

Exporting SCS project source data where online change is possible

Export the SCS project data from the import source project.

1. Using SCS Manager, export the data from the project at the origin of the import and create the following PXF file or CSV file.
   - A PXF file of the entire project
   - When reflecting the addition/modification of a global variable, create a PXF file or CSV file of the global variable. (*1)
   - When reflecting the addition/modification of a definition word, create a PXF file or CSV file of the global variable(*1)

   *1: When performing RS original engineering, create a PXF file. When performing I/O list engineering, create a CSV file.
2. If you have modified "Component Number" or "CENTUM Project Folder" in the SCS Project Properties, export the SCS Project Properties to a CSV file. Items other than "Component Number" and "CENTUM Project Folder" cannot be modified via an online change in SCS Project Properties.
3. When performing I/O list engineering, use AD Organizer to export the SCS project at the origin of the import.

SEE ALSO For more information about procedures for exporting an SCS project using System Structure Navigator of AD Organizer, refer to:

"■ Exporting SCS projects" on page E2-5

Importing SCS project data where online change is possible

1. Open the original current project with SCS Manager and import the required data from the exported PXF files.
   1-1. In the Import dialog, specify the PXF file containing the entire exported project and import only the modified POUs (*1)
   1-2. To import the global variables, in the import dialog box, specify the PXF file containing the global variables, and import.
   1-3. To import the defined-words, in the import dialog box, specify the PXF file containing the defined-words, and import.

   *1: In the course of importing, if the POU contains any FB that does not exists in the current project, the following warning message will be displayed. In such a case, a build error will occur when building the project.
   Warning: Type 'UFB' for symbol 'iUFB' was not found in this project.
   or
   Warning: Type 'UFB1' for Parameter 'iUFB1' was not found in this project.
   'UFB', 'UFB1 ': FB Name
   'iUFB', 'iUFB1': FB Instance Name

2. After importing, the unnecessary global variables and defined words should be deleted. The variables that are not used in POU can be checked on the Browser. Start the Browser and generate (or refresh) the cross-reference information to check the unused variables.
3. If you have modified "Extends Scan Period Automatically", "Behavior at Abnormal Calculation", "Locking of Internal Variables", "Automatic IOM Download", "Device Power-Off Period", or "Device Startup Waiting Period" of SCS Constants Builder, correct each of them in the builder. There are no other items in SCS Constants Builder that can be modified via an online change.
4. Regarding the following builders, import the builder files if required.

Table E3.1-1 Builder files for import (modifications where online change is possible)

Builder	Builder File Location (*1)
I/O Parameter Builder (*2)	SCS Project\YOKOGAWA_SCS\SAFETY\IOM\IOMDEFSB.edf
Communication I/O Builder (*2)	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\CommIO.edf
Link Transmission Builder	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\LinkTrans.edf
Modbus Address Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\ModbusDef.edf
DNP3 Communication Builder (*3)	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION \DNP3Def.edf
Tag Name Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\TAG\TAG.edf

*1: Relative path under SCS project top directory
*2: In the case of I/O list engineering, it is not necessary to import the builder files using I/O Parameter Builder and Communication I/O Builder.
*3: Because the event buffer size cannot be modified by an online change, import the event buffer size, and then restore and save the original value.

The builder files of the Alarm Priority Builder and Alarm Processing Table Builder cannot be modified by online change. Do not import them.

5. If "Component Number" or "CENTUM Project Folder" have been changed in the SCS Project Properties, import the CSV file that you exported to in advance.
6. Perform the following operations when performing I/O list engineering:

6-1 Run an SCS import using System Structure Navigator of AD Organizer to reflect the safety I/O list, safety communication I/O list, and IOM information onto the SCS project at the destination of the import.

In the SCS Import dialog box, select the [Exclude SCS Project Files] check box and perform the import.

6-2 If changes have been made with the safety I/O list, safety communication I/O list, and IOM information, perform the build process with RS Generation Manager.

SEE ALSO For more information about build processes of SCS project using Generation Manager, refer to:

D4.4, “Operating procedure of RS generation” on page D4-8

For more information about importing an SCS project using System Structure Navigator of AD Organizer, refer to:

“■ Importing SCS projects” on page E2-5

● Online change downloads during SCS project expansions/remodeling

When you have applied the library POU data and SCS project data to the current project, run the online change download.

1. Perform build.
2. Use the Project Comparing Tool to check that the original project after import is the same as the source user-defined project.
   a. Launch the Project Comparing Tool and clear the [compare imported project] check box to compare the original project after import and the source user-defined project and check that there are no discrepancies. When you do so, check the project path display area of the Project Comparing Tool or the printed discrepancies summary report to make sure that the project paths that you are comparing are correct.
   b. If a discrepancy is found, check that it is appropriate.
3. On Integrity Analyzer, validate the contents.
4. On Cross Reference Analyzer, validate the modified contents. Modifications must also be tested after download.
5. Perform online change downloading.

SEE ALSO For more information about procedures for an online change download, refer to:

E1., “Online change of applications” on page E1-1

E3.2 Data transfer procedure during expansions/remodeling in modifications requiring offline download

This section describes the procedure for making a modification that requires offline download and importing the results of testing in the import source project into the current project on a project-by-project basis. Offline download is necessary because the entire project is being imported.

The overall flow of the procedure is as follows:

1. If a POU included in a library has been modified, first apply the modifications to the library project to the original library project, and then copy the modifications to the library of the current project.
2. If the import source project has been modified, apply the modifications to the current project.
3. Download the SCS project offline.

Library POU data transfer in modifications requiring offline download

Apply the modifications from the library in the import source project to the original library and copy it to the LIBRARIES folder of the current project.

- By way of preparation, back up the original library using the Version Control Tool.

1. Open the library of the importing source project side on the SCS Manager, and change the target name to SCS_TARGET and then save the change.
2. Export the entire project containing the library to PXF files.
3. Use the SCS Manager to open the original library, specify the PXF files thus created in the Import dialog, and then import the whole project containing the library.
4. Execute the build of the original library.
5. Check the integrity of the original library using the Integrity Analyzer.
6. Copy the original library to the LIBRARIES folder of the current project.

SCS project data transfer in modifications requiring offline download

Reflect the modifications on the current project from the modified importing source project.

- By way of preparation, back up the current project using the Version Control Tool.

Exporting SCS project source data requiring offline download

1. Open the importing source project on the SCS Manager, and change the target name to SCS_TARGET and then save the change.
2. Export the entire source project to PXF files.
3. If you have modified "Component Number" or "CENTUM Project Folder" in the SCS Project Properties of the import source project, export the SCS Project Properties to a CSV file.
4. If you have modified SCS Constants Builder in the import source project, export it to a CSV file.

Importing source SCS project data that requires offline download

1. In SCS Manager, open the current project, import the whole project specifying the PXF file exported from the source project.
2. Redefine the library path to the current project.
3. Import the CSV file if there is an exported CSV file of the SCS Constants Builder.
4. Import the builder files if required.

Table E3.2-1 Builder files for import

Builder	Builder File Location (*1)
I/O Parameter Builder (*2)	SCS Project\YOKOGAWA_SCS\SAFETY\IOM\IOMDEFSB.edf
Communication I/O Builder (*2)	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\CommIO.edf
Link Transmission Builder	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\LinkTrans.edf
Modbus Address Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\Modbus-Def.edf
DNP3 Communication Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION \DNP3Def.edf
Tag Name Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\TAG\TAG.edf
Alarm Priority Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\Alm-Pri.edf
Alarm Processing Table Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION \AlmTbl.edf

*1: (relative path under SCS project top directory).
*2: In the case of I/O list engineering, it is not necessary to import the builder files using I/O Parameter Builder and Communication I/O Builder.

5. Import the CSV file if there is an exported CSV file of the SCS Project Properties of source SCS project.
6. Perform the following operations when performing I/O list engineering:
   a. Using AD Organizer, reflect the safety I/O list, safety communication I/O list, and IOM information onto the SCS project at the destination of the import.
   b. If changes have been made with the safety I/O list, safety communication I/O list, and IOM information, perform the build process with RS Generation Manager.

SEE ALSO

For more information about build processes of SCS project using Generation Manager, refer to:

D4.4, “Operating procedure of RS generation” on page D4-8

For more information about importing an SCS using System Structure Navigator of AD Organizer, refer to:

“■ Importing SCS projects” on page E2-5

Offline download during expansions/remodeling

Execute offline download in an SCS project that you have finished importing.

1. Perform build.
2. Use the Project Comparing Tool to check that the original project after import is the same as the source user-defined project.
   2-1. Launch the Project Comparing Tool and clear the [compare imported project] check box to compare the original project after import and the source user-defined project and check that there are no discrepancies. When you do so, check the project path

display area of the Project Comparing Tool or the printed discrepancies summary report to make sure that the project paths that you are comparing are correct.

2-2. If a discrepancy is found, check that it is appropriate.

3. Validate the contents on the Integrity Analyzer.
4. Validate the modified contents on the Cross Reference Analyzer. Modifications must also be tested after download.
5. Perform offline download.

TIP

- Possibilities of online change download
  Whether or not it is possible to perform online change download when the current project has been modified by import is the same as when the same modifications are made manually on the current project. Therefore, in some cases, online change download is possible even when the entire project has been imported. Whether or not it is possible to perform online change download is found when you run a build or try to run online change download after importing.

E3.3 Data transfer procedure during SCS project regeneration

In order to apply the new features on the newer SENG software release number to the existing SCS project or to reuse the existing project, the existing project needs to be ported (or regenerated).

When porting (or regenerating) a project, the original project needs to be entirely exported into PXF format binary files. Then import the PXF files into a new project.

When performing I/O list engineering, in addition to using SCS Manager, it is necessary to export/import the SCS project by using AD Organizer.

The overall flow of the procedure is as follows:

1. If the library needs to be regenerated, regenerate the library first.
2. Regenerate the SCS project.
3. Check that the regenerated project is equivalent to the original project.

SEE ALSO For more information about importing or exporting PXF files and CSV files, refer to:

E2.3, “Importing and exporting data that is managed by SCS Manager” on page E2-7

Regenerating library data when regenerating an SCS project

Implement the following procedure if you need to regenerate a library as part of regenerating an SCS project.

1. Back up the original library on the Version Control Tool if necessary.
2. Open the source library in SCS Manager and export the whole project containing the library to PXF files.
3. In Windows Explorer, delete the original library, or move it to a different place.
4. Create a new library by using the same name as the source library, and change the related resource names and configuration names to the same names that are used in the source library.
5. In the SCS Manager, import the whole project containing the source library. In the Import dialog, specify the PXF files to which the project has been exported.
6. Build the library.
7. Check the integrity of the library using the Integrity Analyzer.

Regenerating an SCS project with the new revision

Follow these steps to regenerate an SCS project with the new revision:

1. Using SCS Manager, export all of the data in the source SCS project. More specific instructions are given later.
2. If you are upgrading an SCS project that was created by I/O list engineering with a software revision R4.01.00 through R4.03.00, create a safety communication I/O list for the target SCS by using Communication I/O List Output Tool.
3. In System Structure Navigator of AD Organizer, select the target SCS and execute an export of the SCS.
4. In Windows Explorer, move the source SCS project to a work folder.
5. From the menu bar of AD Organizer, select [View] > [Refresh].
   The display of System Structure Navigator is refreshed.

6. For I/O list engineering, in System Structure Navigator of AD Organizer, select the target SCS and start Safety I/O Editor, then delete all I/O rows, save, and check in.
7. If there is no Comm_I/O under the target SCS, proceed to the next step. If there is a Comm_I/O under the target SCS, select the Comm_I/O and start Safety Communication I/O Editor. Delete all rows of Program Definition, Communication Definition, and Signal Definition, save the list, and then check in.
8. In System Structure Navigator, select the target SCS and click [Delete].
9. Using SCS Manager, create a new SCS project by using the same SCS name and location as the source SCS project, and change the related resource names and configuration names to the same names that are used in the source project.
10. Copy any libraries used in the source SCS project to the LIBRARIES folder of the newly created SCS project. Also copy any libraries that you have regenerated.

TIP

When engineering by using iDefine, you do not need to copy the iDefine-config file.

11. In SCS Manager, open the newly created SCS project and import the data that you exported in step 1. More specific instructions are given later.
12. Import the builder files of the source project.
13. If the SCS project has been registered in AD Server, select [View] > [Refresh] from the menu bar of AD Organizer.
    The display of System Structure Navigator is refreshed.
14. When performing I/O list engineering, use System Structure Navigator of AD Organizer to select the target RS project and execute an import of the SCS.
    As the files to import, specify the files that you exported in step 3.

    In the SCS Import dialog box, select the [Exclude SCS Project Files] check box and perform the import.
15. If you are upgrading an SCS project that was created by I/O list engineering with a software revision R4.01.00 through R4.03.00, import the safety communication I/O list that you created in step 2.
16. Start the SCS project build process. In the case of I/O list engineering, run RS Generation from AD Organizer.

SEE ALSO

For more information about build processes of SCS project using Generation Manager, refer to:

D4.4, “Operating procedure of RS generation” on page D4-8

For more information about the procedure for exporting source SCS project data using SCS Manager, refer to:

“● Exporting SCS project data when regenerating an SCS project” on page E3-11

For more information about the procedure for exporting an SCS project using System Structure Navigator of AD Organizer, refer to:

“■ Exporting SCS projects” on page E2-5

For more information about the procedure to import source SCS project data by using SCS Manager, refer to:

“● Importing SCS project data when regenerating an SCS project” on page E3-11

For more information about the procedure for importing an SCS using System Structure Navigator of AD Organizer, refer to:

“■ Importing SCS projects” on page E2-5

For more information about Communication I/O List Output Tool, refer to:

“■ Communication I/O List Output Tool” on page App.3-16

Exporting SCS project data when regenerating an SCS project

1. Back up the original project on the Version Control Tool if necessary.
2. Open the original project on the SCS Manager, export the binding information, and create the PXF file.
3. Export the whole project from the original project and create the PXF file.
4. Export the SCS Project Properties from the source project to create a CSV file.
5. Export the SCS Constants Builder data from the source project to create a CSV file.

Importing SCS project data when regenerating an SCS project

Follow these steps to import data of the source SCS project to the destination SCS project:

1. In SCS Manager, open the newly created SCS project, specify the PXF file to which the binding information of the source project was exported, and import the binding information.
2. In SCS Manager, specify the PXF file to which the whole source project was exported, and import the whole project.
3. Open the SCS Constants Builder and import the exported CSV file in the source project.
4. Import the builder files of the builders that are shown in the following table:

Table E3.3-1 Builder files to be imported (project regeneration)

Builder	Builder File Location (*1)
I/O Parameter Builder (*2)	SCS Project\YOKOGAWA_SCS\SAFETY\IOM\IOMDEFSB.edf
Communication I/O Builder (*2)	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\CommIO.edf
Link Transmission Builder	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\LinkTrans.edf
Modbus Address Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\ModbusDef.edf
DNP3 Communication Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION \DNP3Def.edf
Tag Name Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\TAG\TAG.edf
Alarm Priority Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\AlmPri.edf
Alarm Processing Table Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION \AlmTbl.edf

*1: (relative path under the SCS project top directory)
*2: In the case of I/O list engineering, it is not necessary to import the builder files using I/O Parameter Builder and Communication I/O Builder.

5. Open SCS Project Properties and import the exported CSV file in the source project.

Regenerating an SCS project with a different station type

Follow these steps to regenerate an SCS project with a different station type.

TIP

If the source SCS project was created by I/O list engineering with a software version earlier than R4.03.10, create a safety communication I/O list of the source SCS by using Communication I/O List Output Tool and load it into Safety Communication I/O Editor in advance.

1. Using SCS Manager, export the entire source SCS project.

- When performing RS original engineering to change from SIL3 SCS to SIL2 SCS, or the other way around, keep a separate record of the definition details of I/O Wiring View and I/O Parameter Builder.

2. When performing I/O list engineering, follow these steps:

   a. In System Structure Navigator of AD Organizer, select the source SCS and start IOM Definition Editor.

   b. Export the defined contents.
   When changing from SIL3 SCS to SIL2 SCS, or the other way around, keep the record of IOM definition details. You can record them for example by copying the definition details and pasting them into a text editor.

   c. In System Structure Navigator of AD Organizer, select a file under the I/O-List folder, start Safety I/O Editor, perform a save after clearing the RS Project column of the I/O assigned to the target SCS, and check in.

   d. In System Structure Navigator of AD Organizer, if there is a Comm_I/O, select it and start Safety Communication I/O Editor, then clear the RS Project column of the program definitions assigned to the target SCS. Because fire and gas communication related definitions are allowed only for S2SC70, delete all such definitions, save the list, and check in.

3. When engineering by using iDefine, specify the iDefine-config file that was imported to the target SCS and save it.
   You can specify the iDefine-config file that was imported to the target SCS by using the revision management function of iDefine.

4. In Windows Explorer, move the source SCS project to a work folder.

5. From the menu bar of the System Structure Navigator in AD Organizer, select [Display] > [Update].
   The display of System Structure Navigator is refreshed.

6. Select the target SCS, and click the [Delete] button on the toolbar.

7. Because the type of SCS is being changed, re-assign licenses to the SCS.

8. In SCS Manager, create a new SCS project with the same SCS name under the original RS project. Definitions of the configuration name and resource number must be the same as the source station.

9. Copy any libraries used in the source SCS project to the LIBRARIES folder of the newly created SCS project. Also copy any libraries that you have regenerated.

TIP

When engineering by using iDefine, you do not need to copy the iDefine-config file.

10. Using SCS Manager, import the PXF files of the SCS that you exported in step 1 to the destination SCS project. Import the exported builder files as well. However, exclude the POUs that cannot be defined in the destination station.

    - When performing RS original engineering to change from SIL3 SCS to SIL2 SCS, or the other way around, change the I/O Wiring View information recorded in step 1 to be appropriate for the destination IOM and define it. Also, change the definition details of I/O Parameter Builder to the recorded details.

11. From the menu bar of the System Structure Navigator in AD Organizer, select [Display] > [Update].
    The display of System Structure Navigator is refreshed.

12. When performing I/O list engineering, in the System Structure Navigator, select a file under the I/O-List folder and start Safety I/O Editor, and then perform the following steps:
    a. In the RS Project column of the destination SCS project, enter the same data as that of the source SCS project. Delete the data that is not supported in the regenerated station, and save.
    b. When changing from SIL3 SCS to SIL2 SCS, or the other way around, change IOM Type to be appropriate for the destination.
    c. Check in the changed details.
13. If you are performing I/O list engineering, select Comm_I/O, if it is defined in the System Structure Navigator, and start Safety Communication I/O Editor, then perform the following operation:
    a. In the RS Project column of the program definition, enter the same data as that of the source SCS project. Delete the data that is not supported in the regenerated station, save the list, and check in.
14. If you are performing I/O list engineering, select the destination SCS in the System Structure Navigator and start IOM Definition Editor.
    a. Click the [Create Node & IOM] button, and create nodes and IOMs.
    b. Create ESB bus coupler modules or N-ESB bus coupler modules as necessary.
    c. Change the node and IOM definition details from the default values to the values defined in the source project. To do this, use IOM Definition Editor to import the file exported from IOM Definition Editor in step 2.
    d. When changing from SIL3 SCS to SIL2 SCS, or the other way around, change the IOM definition details to the values record in step 2-b.

IMPORTANT

- If you export the entire SCSP1/SCSV1 project and import it to a newly created project of SCSP3/SCSL2/SCSP2, the values of the source project are applied to the following definitions related to application capacity. After importing, you must change the values to the fixed values or default values of SCSP3/SCSL2/SCSP2.

Table E3.3-2 Definition items related to application capacity

Definition item	Value of SCSP1/SCSV1	Value of SCSP3/ SCSL2/SCSP2	Remarks
Online change code size (*1)	1700000 (fixed value)	2550000 (fixed value)	A build error will occur if the value is not changed after importing.
Online change user variable size (*2)	32768 (default) 8192 to 65536 (allowable specification range)	131072 (default) 8192 to 262144 (allowable specification range)	A value different from the default SCSP2 value is set after importing.
Constant/temporary variable size (*3)	32768 (default) 8192 to 65536 (allowable specification range)	131072 (default) 8192 to 262144 (allowable specification range)	A value different from the default SCSP2 value is set after importing.

*1: [Code size] in the Advance settings dialog box of the Settings tab in Resource Properties of the SCS Manager
*2: [User variable size] in the Advanced settings dialog box of the Settings tab in the Resource Properties of the SCS Manager
*3: [Memory size for temporary variables] in the Target tab of Resource Properties in the SCS Manager or [Memory size for temporary variables] in the Hardware tab of Configuration Properties in the SCS Manager

- If you are performing RS original engineering and have imported the project data of SCSP1/SCSV1 to an SCSP3/SCSL2/SCSP2 project that uses optical ESB bus repeater, configure the node settings of the I/O Parameter Builder for all FIO nodes connected to the CPU node through the optical ESB bus repeater modules. If [Extends Node Bus] is set to [No], change it to [Yes] and specify the actual node distance to [Extends To (Km)].
- If you import SCSP3/SCSL2/SCSP2 applications to an SCSP1/SCSV1 project, do not import the entire project. Instead, import the engineering data individually, for example, in POU units.

15. If you use iDefine for engineering to change from SIL3 SCS to SIL2 SCS, or the other way around, follow these steps:
    a. From AD Organizer, load the information of new node and IOM into iDefine.
    b. In the POU and tag information defined in iDefine, reflect the new information which was reflected in step a. Next, load the iDefine information by using System Structure Navigator of AD Organizer and reflect it in the new SCS again.
16. Start the SCS build process. In the case of I/O list engineering, run RS Generation from AD Organizer.

SEE ALSO

For more information about how to create nodes & IOM, refer to:

"■ Creating the node and I/O module based on safety I/O list" on page D3-5

For more information about build processes of SCS using Generation Manager, refer to:

D4.4, "Operating procedure of RS generation" on page D4-8

For more information about how to use Communication I/O List Output Tool, refer to:

"■ Communication I/O List Output Tool" on page App.3-16

For more information about the procedure to export SCS project data, refer to:

"● Exporting SCS project data when regenerating an SCS project" on page E3-11

For more information about the procedure to export SCS project data by using SCS Manager, refer to:

"● Importing SCS project data when regenerating an SCS project" on page E3-11

■ Confirming a regenerated project

Check that the regenerated project is equivalent to the original project using the following procedure.

1. Open the regenerated SCS project on the SCS Manager and perform build.
2. Check the validity using the Integrity Analyzer.
3. Using the function of Cross Reference Analyzer for comparison with the original project, check that all POUs are equivalent to those of the original project.
   Open the regenerated SCS project on the SCS Manager and compare it with the original SCS project using the Cross Reference Analyzer. Confirm that all POUs are displayed in green (retesting or review is not required). At this point, check whether the path in the title bar of Cross Reference Analyzer or in the report is correct.
4. For data that cannot be checked with Cross Reference Analyzer, use the Project Comparing Tool to ensure that the regenerated SCS project is equivalent to the original SCS project. When doing so, select the [compare imported project] check box of the Project Comparing Tool.
   Launch the Project Comparing Tool and compare the regenerated SCS project with the original SCS project, so that there is no difference in all items. When you do so, check that the project paths which you are comparing are correct in the project path display area of Project Comparing Tool or in the printed summary report of the discrepancies.
   - If no difference is detected with the Cross Reference Analyzer or the Project Comparing Tool, re-test of SCS application is not required.
   - If the following differences are detected with the Project Comparing Tool, check the details and modify as needed:
     - If you import an SCS project that is created using a SENG with an older software release number, definitions that do not exist in the original project are set to the default values in the regenerated project. These items are picked up as discrepancies by the Project Comparing Tool. When you change the default value, the items must be tested.
     - If you import an SCS project that is created for a different model, definitions that do not exist on the model used for the original project are set to the default values in the regenerated project. Moreover, definitions with different configurable values will produce an error at build in the regenerated project.
5. Perform an offline download to the SCS and make sure that the SCS starts.

TIP

If you have modified a regenerated project after verifying that the regenerated project is equivalent to the original project by using the Cross Reference Analyzer and Project Comparing Tool, ascertain the range for retesting in the usual manner by using the Cross Reference Analyzer, Project Comparing Tool, or the self-document printout, and conduct the tests.

SEE ALSO

For more information about how to check project data migrated by export or import, refer to:

"■ How to check when project data is migrated by export or import" on page E2-3

E3.4 Reusing SCS project data

This section describes the procedures of operations to perform with the SCS project in order to reuse an existing SCS project database. Do not use Windows Explorer to copy SCS projects because, if you do so, you can no longer register the SCS project in an AD project.

Duplicating an SCS project

Using AD Organizer, you can duplicate an SCS project by exporting the SCS project to be duplicated, changing the SCS name, and then importing that project. Follow these steps to duplicate an SCS project:

TIP

If the original SCS project was created by I/O list engineering with a software version earlier than R4.03.10, create a safety communication I/O list of the original SCS by using Communication I/O List Output Tool and load it into Safety Communication I/O Editor in advance.

1. Export an SCS project.
2. Import the exported SCS project. In the SCS name field of the Import SCS dialog box, enter a new name of the duplicate SCS.
3. If you are performing I/O list engineering, edit the imported safety I/O list and safety communication I/O list and check these in.
   a. You cannot check in a duplicated safety I/O list or safety communication I/O list because the P&ID Group names and P&ID Tags are the same as the original. You need to change the P&ID Tag names and P&ID Group names to separate the Group.
   b. You cannot check in the safety communication I/O list because the Program Group names are the same as the original. You need to change the Program Group names and reflect them into the signal definition and communication definition.
   However, for S2LP131, when changing the Program Group name, the corresponding communication group is automatically created. Copy the contents of the existing communication group to the created communication group, and delete the existing communication group.
   c. After making the change, you can check in the safety I/O list and safety communication I/O list by using the Check-in window.
4. Perform the following operations when engineering by using iDefine:
   a. Export the ProSafe-RS I/O file of the target SCS from AD Organizer.
   b. After the ProSafe-RS I/O file is imported in iDefine and the engineering is complete, export the created application as an iDefine-config file.
   c. Import the iDefine-config file to AD Organizer.
   d. Run the reflection process and the SCS project build process by using Generation Manager.
5. Using SCS Manager, open the SCS project that you have imported.
6. Change the following settings of the SCS project to the appropriate values.

Table E3.4-1 Settings that you need to change values

Dialog box	Tab	Setting item
Configuration Properties dialog box in Hardware Architecture View	General tab	Name
Connection Properties dialog box in Hardware Architecture View	Network Parameters tab	IP address

Continues on the next page

Table E3.4-1 Settings that you need to change values (Table continued)

Dialog box	Tab	Setting item
Resource Properties dialog box in Link Architecture View	General tab	Name, Resource number
SCS Project Properties dialog box	SCS tab	Domain number, Station number
	Project tab	CENTUM project folder
Add/Remove dependencies dialog box	-	Dependencies

TIP

When an SCS project is copied to another location, the library project will also be copied together. The SCS project at the copy destination will still reference the library at the copy source. For this reason, the dependency of the SCS project and library project will become inappropriate. It is necessary to reconfigure the path of the library project at the copy destination with the Add/Remove Dependencies dialog.

7. Save the SCS project.
8. Using Document Generator, change the title string for the cover page of the document to print.
   In the Customize dialog box that is opened from the [Option] menu of SCS Manager, clear the [Enhanced printing style] check box, change the title string, and then select the check box again.

SEE ALSO

For more information about the procedures for importing or exporting SCS project data, refer to:

E2., “Import/Export function” on page E2-1

For more information about how to use Communication I/O List Output Tool, refer to:

“■ Communication I/O List Output Tool” on page App.3-16

For more information about how to change the title string for the cover page of the document, refer to:

“● Header/Footer” in “■ Options tab” in F2.5, “Customizing print settings (backward-compatible mode)” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about the procedure to import ProSafe-RS I/O files to iDefine, refer to:

10., "IMPORT FROM AD SUITE" in iDefine User Guide (Yokogawa Extensions) (PR12002-MAN-980_01)

■ Modifying an application

The following modifications to the application are required on the copied station.

1. Modification of inter-SCS safety communication
   Modify the inter-SCS safety communication application.
   a. The domain number and station number on the consumer and producer will change. Modify the variable names accordingly.
   b. Delete the existing binding table and regenerate it.
2. Modification of SCS link transmission
   Modify the receiving station as appropriate.

■ Checking the projects that are created by reusing data

Check that the copied SCS project is equivalent to the original project.

1. Perform build for the copied SCS project.
2. Run the Integrity Analyzer to validate the contents.

3. Launch the Cross Reference Analyzer and check that all Program Organization Units (POU) are equivalent to those of the project before the project was copied. If you are comparing with a project with a different station address, proceed to step 4.

   a. Use the Cross Reference Analyzer's function for comparison with the original project to compare the copied SCS project with the original SCS project. Check that all POUs are displayed in green, excluding the sections in which you have modified the inter-SCS safety communication and related areas. At this point, check whether the path in the title bar of Cross Reference Analyzer or in the report is correct.

   b. Validate the modified content.
   Each modification must be tested at an appropriate timing.

4. For data that cannot be checked with the Cross Reference Analyzer, use the Project Comparing Tool to ensure that the copied SCS project is equivalent to the original SCS project.

   a. Launch the Project Comparing Tool, clear the [compare imported project] check box, and compare the copied SCS project with the original SCS project. Ensure that there are no discrepancies, except in sections that you have modified. When you do so, check in the results printed from the Project Comparing Tool for the project path display area and the summary of discrepancies to make sure that the project paths that you are comparing are correct.

   b. If a discrepancy is found, check that it is appropriate.

5. Perform an offline download to the SCS and make sure that the SCS starts.

TIP

If the copied SCS project contains any modifications, except those in inter-SCS safety communication and SCS link transmission, ascertain the range for retesting in the usual manner by using Cross Reference Analyzer, Project Comparing Tool, self-document printout, or other appropriate means.

F. Installation and start-up

This chapter describes the installation of ProSafe-RS system, the wiring to field devices, a procedure of start-up including tests, commissioning and precautions for the start-up.

F1. Procedure of installation and start-up

This section describes a general procedure of the start-up of ProSafe-RS system ranging from the installation of equipment to the completion of commissioning.

Installing and getting started with ProSafe-RS

The regular procedure from the installation of equipment to the completion of commissioning is as follows.

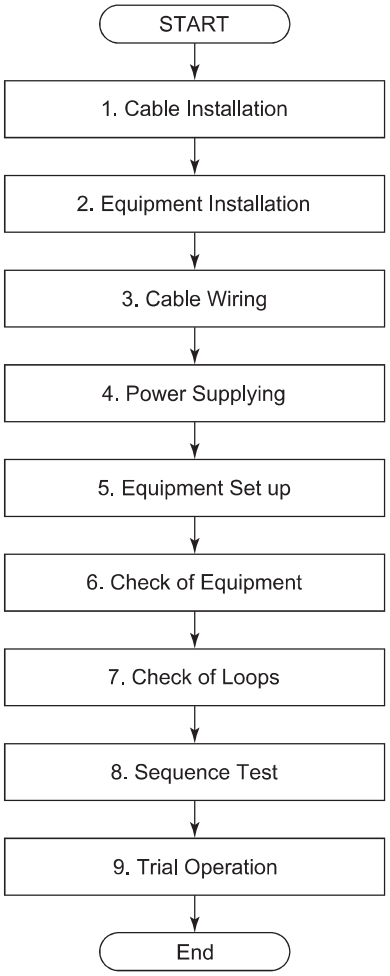


Figure F1-1 Workflow for installing and getting started with ProSafe-RS

1. Install control bus, optical cables and cables between panels.
2. Install ProSafe-RS and other equipment. When performing wireless communication with subsystems, configure the initial settings of the wireless devices on the subsystem side.
3. Wire for networks such as V net and ESB buses, as well as I/O modules and field devices.
4. Supply power to ProSafe-RS and other equipment.
5. Turn on ProSafe-RS and other equipment to start.
6. Check individual hardware of ProSafe-RS and other equipment (including I/O modules).
7. Check loops from the field to I/O modules.

8. Test application logic of ProSafe-RS.
9. Perform a trial operation for the entire system to confirm actions of the ProSafe-RS system itself.

SEE ALSO For more information about engineering of fire and gas communication, refer to:

E1.5, “Engineering for fire and gas communication” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Commissioning

In commissioning, procedures from No.6 “Check of Equipment” to No. 9 “Trial Operation” in the flowchart of “Installation and start-up” are performed. Confirm the following items in this series of procedures.

- All modules in SCS, wiring to field devices and wiring of power supply are correctly installed.
- All modules in SCS, field devices and power supply work without faults.
- Sensor measurement values are correct.
- Input values to SCS and output values from SCS are correct. (Including tests of high/low limits)
- Application logic works correctly according to changes of input values.
- Operations for failure occurrence take place as intended on the basis of each field device and SCS module.
- Safety application logic works correctly between actual SCSs when Inter-SCS safety communication is used.
- Confirm Demand Reaction Time.
- Confirm actions against a fault (a failure in SCS).

Precautions

- When executing offline download on a suspended SCS, confirm that the SCS is being suspended with the SCS State Management window in SENG so as not to download the database to a different SCS by mistake.
- Confirm that the SCS works normally after offline download with the SCS State Management window in SENG.
- Confirm that database is downloaded correctly with the Database Validity Check Tool in SENG.
- Set new passwords for security levels 0 and 1 after offline download.
- Precautions for LED display of CPU of SCS
  LEDs of CPU have a structure which switches between V net or Vnet/IP address display and SCS Status Display. Set LED to the SCS Status Display when SCS is in operation.
- When SDV526/L1DV526 is outputting Off signals, it takes max. 5 minutes to detect an open circuit. It takes max. 2 minutes to detect the recovery.
  Because of this, if any of the following events occur before the cause of open circuit error is eliminated after a diagnosis information message of an abnormal status caused by the open circuit is generated, a diagnosis information message of recovery is generated first. And after about 5 minutes, a diagnosis information message of an abnormal status is generated again.

TIP If you perform output enable operation before the abnormal status is re-detected, open circuit is detected about 5 minutes after a diagnosis information message of recovery is informed if the output signal is OFF. If the signal is ON, open circuit is immediately detected.

  - SDV526/L1DV526 recovers from power supply error. (The power to the I/O node or the field power supply is turned off and on.)
  - Dismounting and remounting of SDV526 or re-connection of a cable connector that was disconnected (both modules in redundant configuration.)
  - Recovery of ESB bus communication (SDV526/L1DV526 recovers from a state where it outputs fail-safe values.)

- In the case of SDV521 (style S3 or above)/L1DV521 and SDV53A (style S2 or above)/ L1DV53A, if a short circuit has occurred while the module is outputting an Off signal, it takes max. 10 seconds to detect the short circuit.
- In the case of SDV521 (style S3 or above)/L1DV521 and SDV53A (style S2 or above)/ L1DV53A, if a short circuit is detected while the module is outputting an Off signal and a diagnosis information message indicating abnormal status is generated, a diagnosis information message of recovery may be generated if either of the following events occurs before the short circuit is repaired:
  - The module is powered off and on (due to dismounting and remounting of the module or turning on and off the power to the I/O node)
  - Switch over to the standby module (when modules are in redundant configuration)

  Also note that if the module is powered on while it has a short circuit, the short circuit may not be detected. After the short circuit is repaired, it becomes possible to detect short circuits that occur afterward.
- In the case of SDV521/L1DV521 and SDV53A/L1DV53A, if a short circuit is detected while the module is outputting an On signal and a diagnosis information message indicating abnormal status is generated, a diagnosis information message of recovery may be generated before the short circuit is repaired. Even after the recovery message is generated, an Off signal is output to the channel and the channel remains in the output disabled status.

F2. Preparation before installation and start-up of N-IO nodes

You need set a node number for N-IO nodes by using the Node Number Setting Tool. When performing the I/O list engineering, you can connect the FieldMate Validator to N-IO nodes to perform connection tests between the devices and I/O modules in advance.

Preparing N-IO nodes earlier than the upper equipment

You can prepare N-IO nodes that contain N-IO I/O modules earlier than the upper equipment such as SENG, HIS, SCU.

1. Set the node numbers of all N-IO nodes.
2. Use the FieldMate Validator to perform the loop checking, to check the functionalities and to configure the field device and N-IO I/O module under the N-IO node.

F2.1 Configuring the N-IO node interface unit

For the N-IO node interface unit, you can set the node number by connecting the computer and maintenance port of the node interface unit. This section describes the tool to configure the node number.

F2.1.1 Using the Node Number Setting Tool

You can use the Node Number Setting Tool to set a node number for N-IO nodes. This section describes the Node Number Setting Tool.

Outline of the node number setting operation

Node number is not set for the N-ESB bus module that is installed in the node interface unit of the N-IO node when the module is shipped from the factory. You must set a node number for the N-ESB bus module before connecting it to the SCU.

You need to connect the computer to the maintenance port of N-ESB bus module to set the node number by using the software on the computer.

The software required to set the node number is available in the installation medium of ProSafe-RS.

Items to be prepared

The following items are required to set the node numbers:

Software medium of ProSafe-RS

It includes USB drivers and Node Number Setting Tool required to set the node number. You need to install this software on the computer that you use to set the node number.

Computer

The computer must have the following specifications:

- Hardware
  Compliant with the hardware requirement of Windows 10.
- Software
  Windows 10 Pro (64bit)

USB cable

Use the MicroUSB Micro-B connector for the N-ESB bus module side.

Preparing the computer that sets the node number

You need to install the required software on the computer that sets the node number.

Installing USB drivers

1. Insert ProSafe-RS installation medium in computer drive.
2. On the explorer, open the following folder of ProSafe-RS installation medium:
   `<ProSafe-RS software medium drive>:\ProSafe-RS\NIO_TOOLS`
3. Double click and run the `Setup.exe`.
   The User Account Control dialog box appears.
4. Click [Yes].
   A dialog box for confirming the setup details appears.
5. Select [Install] and click [OK].
   A dialog box for confirming the installation start appears.
6. Click [OK].
7. When the Windows Security dialog box appears, click [Install].
8. When the dialog box notifying the completion of installation appears, click [OK].

TIP

- When the dialog box prompting for computer restart appears, click [OK] to restart the computer.
- You can install the USB drivers after connecting the computer and N-ESB bus module.

Copying the Node Number Setting Tool

1. Insert the ProSafe-RS installation medium in the computer drive.
2. On the explorer, open the following folder of ProSafe-RS software medium:
   `<ProSafe-RS software medium drive>:\ProSafe-RS\NIO_TOOLS`
3. Copy `NodeNumSetting.exe` of the folder to any folder on the computer.

Setting node numbers

The procedure to set node numbers is as follows:

Checking before setting the node numbers

Before setting the node numbers, confirm that the status lamp of the N-ESB bus module is ON.

Remove all N-ESB bus cables and optical ESB bus cables from both N-ESB bus modules to disable the bus communication.

Removing the N-ESB bus modules

If the node numbers are already set in the N-ESB bus modules, remove one of the two N-ESB bus modules from the node interface unit. You can remove any of the two N-ESB bus modules.

If the node numbers are yet to be set (ADRS lamp is OFF), you do not need to remove the N-ESB bus module.

Connecting the computer and N-ESB bus module

With the USB cable, connect the USB port of the computer (which is used to set node numbers) and the maintenance port of the powered N-ESB bus module on the node interface unit.

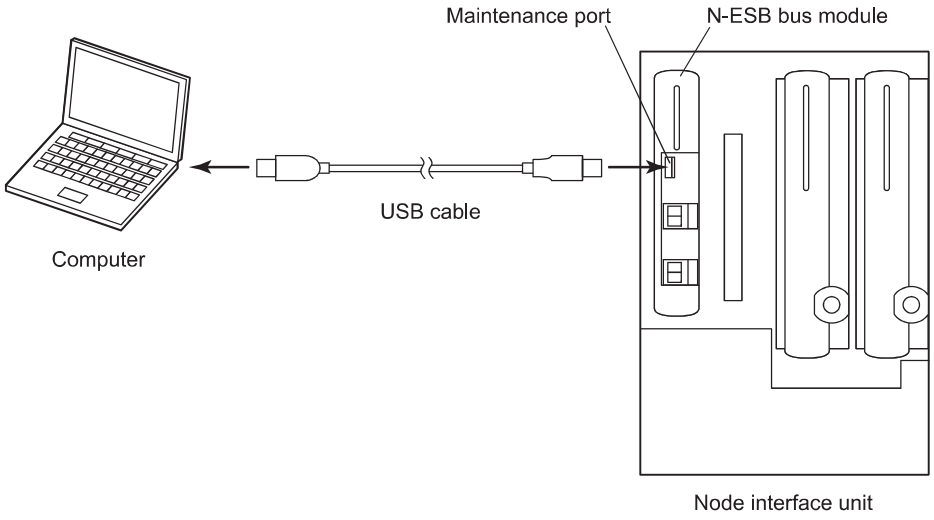


Figure F2.1.1-1 Connecting the computer and N-ESB bus module

Tool operation

1. Double click and run the `NodeNumSetting.exe` command on the computer.
   The Node Number Setting Tool window appears.

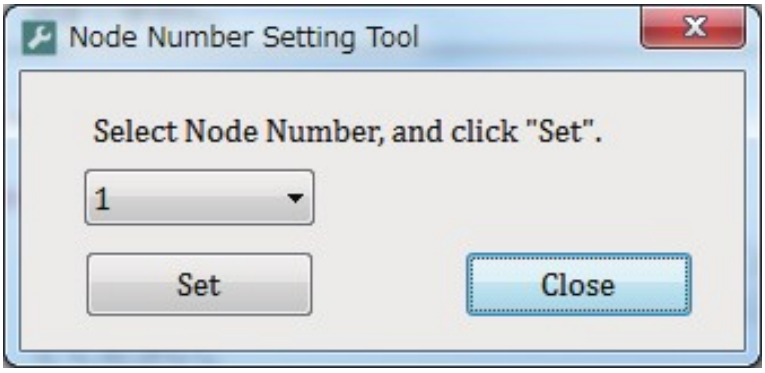


Figure F2.1.1-2 Node Number Setting Tool

2. Select a node number and click [Set].
   A confirmation dialog box appears, showing the currently set node number and node number to be set.
3. Click [Yes].
   The node number is set to the N-ESB bus module. A dialog box displaying setting completion appears.
4. Confirm the node numbers in the ADRS lamp of the N-ESB bus module.

Setting the node numbers of the other N-ESB bus module

If you removed the other N-ESB bus module, perform the following operations for the removed N-ESB bus module. If you did not remove the other N-ESB bus module, proceed to the next procedure.

1. Install the removed N-ESB bus module on the node interface unit.
   The node number is copied from the N-ESB bus module that was already installed.
2. You need to confirm the node numbers in the ADRS lamp of the N-ESB bus module.

Procedure after node number setting

1. Close the Node Number Setting Tool.
2. Remove the USB cable from the N-ESB bus module.
3. Connect all N-ESB bus cables and optical ESB bus cables to both N-ESB bus modules to enable the communication with the SCU.

TIP

The maintenance port of the N-ESB bus module is enabled when shipping. Before starting operation, you must disable the port by using the NIU maintenance port setting tool on SENG.

SEE ALSO

For more information about NIU maintenance port setting tool, refer to:

I4.5, “NIU maintenance port setting tool” on page I4-77

F2.2 Testing by using FieldMate Validator

You can use FieldMate Validator to test the N-IO modules that are defined in the safety I/O list, and import the information once again after testing. When using FieldMate Validator, you must enable the maintenance port and disable the maintenance port after use.

Outline of testing by using FieldMate Validator

Outline of testing by using FieldMate Validator is as follows:

1. Export the IOM information to be tested to FieldMate Validator.
   a. From the sub menu of the Safety I/O Editor, select [Export to FieldMate Validator] to export the data of each safety I/O list.
   b. Import the exported safety I/O list data into FieldMate Validator.

TIP

If the Field Commissioning Support Package is used, select [Export] in the submenu of the Safety I/O Editor.

2. Test the data by using FieldMate Validator.
3. Import the test results from FieldMate Validator.
   a. Export the information containing the test results from the FieldMate Validator in the safety I/O list format.
   b. From the sub menu of the Safety I/O Editor, select [Import from FieldMate Validator] to import the data exported from FieldMate Validator.

TIP

- If the Field Commissioning Support Package is used, select [Import] in the submenu of the Safety I/O Editor.
- In the Deviation setting page, select either or both [Remove Leading White-space of Import Value] and [Remove Trailing White-space of Import Value] check boxes as necessary. When importing, blank spaces in the specified location are removed.

4. Confirm that the status of test result has changed with the changes in the settings of the safety I/O list.
   When you change the IOM settings by using the Safety I/O Editor, it is indicated that that the I/O setting used for the previous test result is changed.

SEE ALSO

For more information about operating FieldMate Validator and linking with AD Suite, refer to:

manual of FieldMate Validator

For more information about operating the Field Commissioning Support Package and linking with AD Suite, refer to:

manual of Field Commissioning Support Package

F3. Overview of procedures to construct/maintain a stand-alone SCS configuration system

This section explains each of the main steps of constructing and maintaining a stand-alone SCS configuration system.

To do the following steps, you need to connect SENG to the Vnet/IP, but note that while a SENG is connected, one of the buses (bus 2) is in an error status.

- Startup of SCS
- Re-connection of SENG
- Disconnection of SENG
- Replacement of one of the redundant CPU modules.

IMPORTANT

Always connect a SENG during maintenance and make sure that you check the following before you disconnect it.

- SCS is normally started.
- SCS inputs and outputs are all normal.
- There is no diagnostic information message indicating errors of the SCS.

Getting started with SCS

The following information explains the procedure for starting SCS for the first time (offline download).

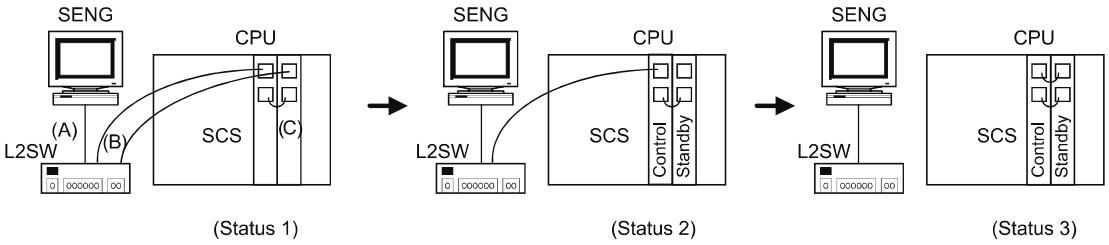


Figure F3-1 Getting started with SCS

1. Perform the following connections using network cables while the SCS is powered off. (Status 1)
   a. Connection between SENG and L2SW, and powering them on
   b. Connection of bus 1 connectors on both CPU modules to L2SW
   c. Connection between bus 2 connectors on both CPU modules
2. Turn on the power of the SCS and perform offline download from SENG.
3. After the offline download is completed, wait until one of the CPU module enters the control state and the other enters the standby state, and then remove the cable between the bus 1 connector of the standby-side CPU module and L2SW. (Status 2)

4. Disconnect the bus 1 cable of the control-side CPU module from L2SW and connect it to the bus 1 connector of the standby-side CPU module. (Status 3)

Reconnection of SENG

Use the following procedure to connect an SENG to an operating stand-alone SCS for the purpose of maintenance and so forth.

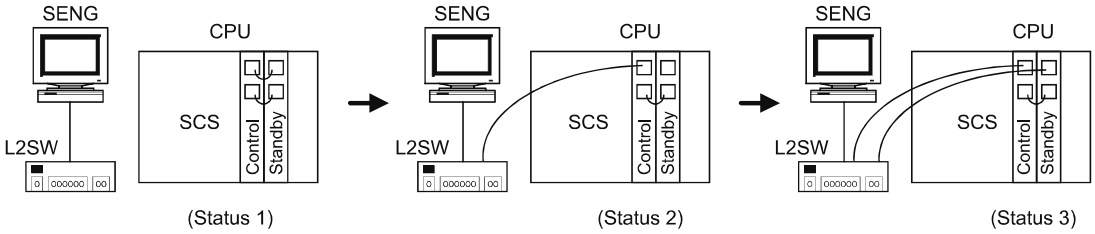


Figure F3-2 Procedure for connecting stand-alone SCS to SENG

(Status 1) above shows SCS operating in stand-alone configuration. At this timing, SENG is not powered and L2SW should be powered.

1. Disconnect the cable from the bus 1 connector of the standby-side CPU module and connect it to L2SW. (Status 2)

IMPORTANT

When you make this connection, if the cable between the bus 1 connectors of the two CPU modules of SCS is not long enough to be connected to the L2SW, you may remove the cable and use a longer cable. However, you must be very careful not to misconnect the cable.

2. Connect the bus 1 connector of the standby-side CPU module to the L2SW with a cable. Then, power on the SENG. (Status 3)

Disconnection of SENG

The SENG can be disconnected after completion of maintenance and other intended operations in the following procedure.

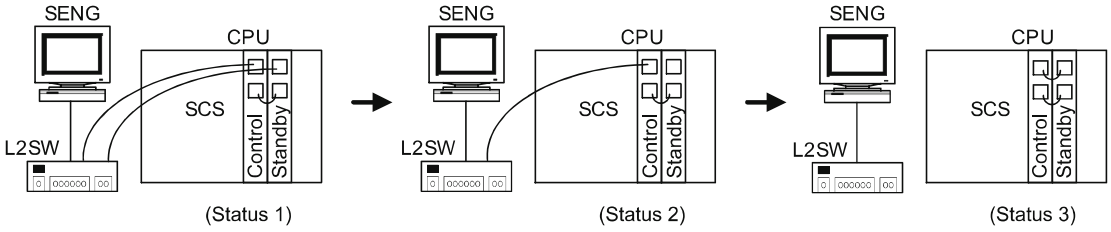


Figure F3-3 Procedure of disconnecting SENG

(Status 1) above shows a status where SCS and SENG are connected.

1. Remove the cable between the bus 1 connector of the standby-side CPU module and L2SW (Status 2) (Status 2)
2. Disconnect the bus 1 cable of the control-side CPU module from L2SW and connect it to the bus 1 connector of the standby-side CPU module (Status 3) (Status 3)

Replacement of one of the redundant CPU modules

Use the following procedure to replace one of the redundant CPU modules.

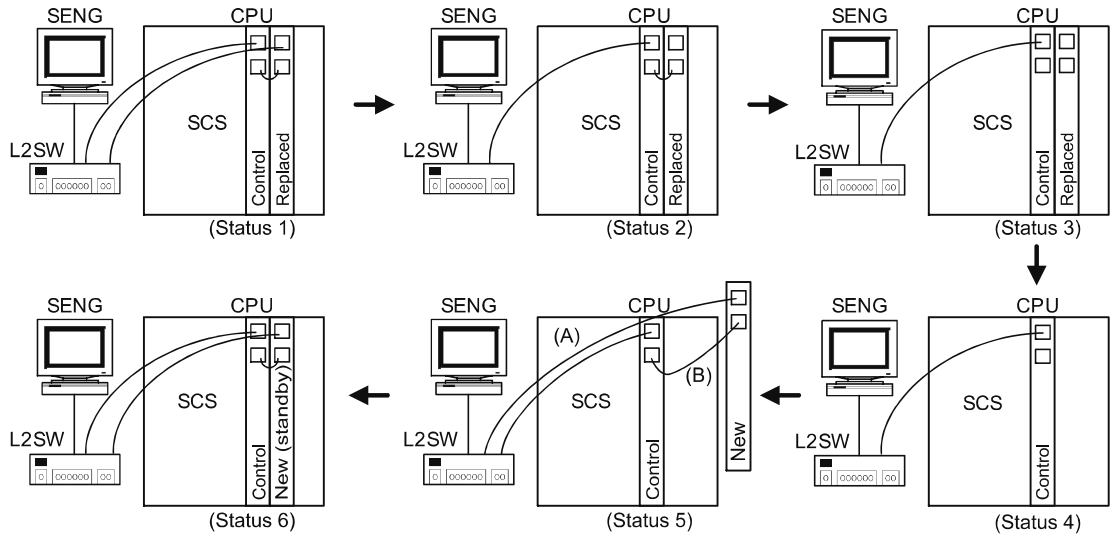


Figure F3-4 Procedure of replacing one of the redundant CPU modules

(Status 1) above shows a status where an SENG is connected for the purpose of checking diagnostic information.

1. Remove the cable between the bus 1 connector of the CPU module to be replaced (standby-side) and L2SW. (Status 2)
2. Remove the cable between the bus 2 connectors on both CPU modules. (Status 3)
3. Remove the CPU module to be replaced from the node. (Status 4)
4. Prepare a new CPU module as a replacement and perform the following connections. (Status 5)
   a. Connection between bus 1 connector of the new CPU module and L2SW
   b. Connection between bus 2 connectors on both CPU modules
5. Install a new CPU module in the node. (Status 6)

G. Emergency procedures

It is required to plan the operation procedure beforehand for emergencies including the occurrence of a shutdown demand or an equipment failure.

An emergency operation is required in case of the following. Referring to these operation flows, plan the emergency operation specifically.

G1. Operation flow during the error occurrence

This section describes the operation flow when an error occurs in the system.

Operation when SCS issues a pre-alarm because of a signal from the field

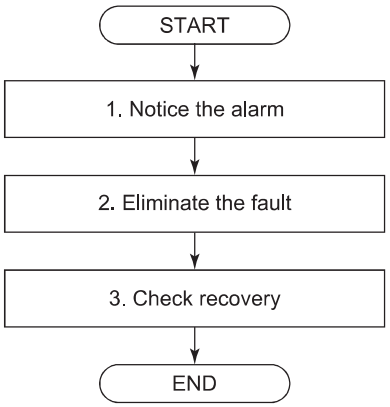


Figure G1-1 Operation when SCS issues a pre-alarm because of a signal from the field

1. Confirm the alarm with an alarm panel or HIS (for CENTUM Integration Structure).
2. Operate the DCS or field devices to eliminate the fault by following the operation manual.
3. Confirm the recovery of normal operation at the plant or DCS.

Operation when plant is shutdown because of a demand from the field

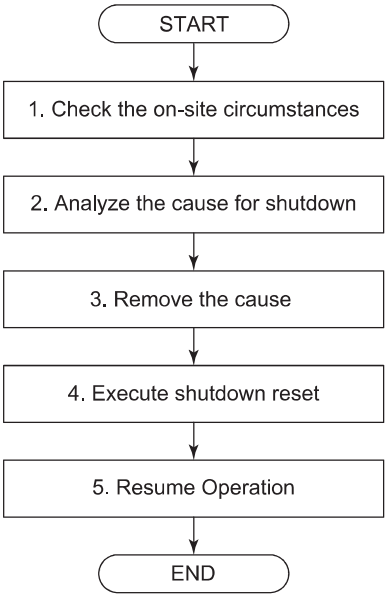


Figure G1-2 Operation when plant is shutdown because of a demand from the field

1. Maintenance personnel check the present state in the plant.

2. An engineer analyzes a cause of the shutdown with the SOE Viewer in SENG. The engineer identifies the cause of the fault with the diagnostic information message at the time when a diagnostic fault occurs and event information is displayed in the SOE Viewer. For CENTUM Integration structure, the engineer can display the process alarm message issued by SCS as a historical message on the SOE Viewer to facilitate the identification of the cause. The engineer then makes a procedure for removing the cause of the fault for recovery. The messages can also be stored as a record by outputting them to a file.
3. The maintenance personnel remove the cause of the fault according to the work procedure.
4. The maintenance personnel execute a shutdown reset operation from the ESD console.
5. Confirm the state of the plant again to restart the plant according to the operation manual.

Operation when a user manually executes a shutdown

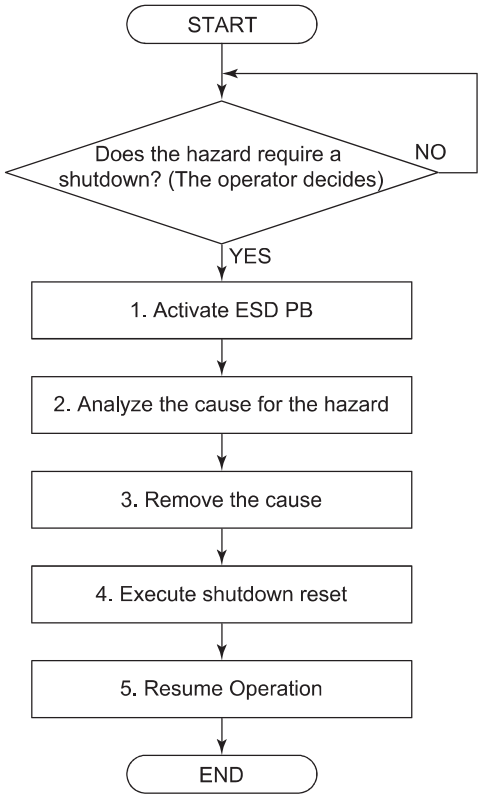


Figure G1-3 Operation when a user manually executes a shutdown

1. Maintenance personnel confirm the state in the plant and operate ESD PB (Emergency shutdown button) installed in the ESD console in order to avoid dangerous accidents.
2. The engineer analyzes the cause of the hazard with historical messages or trend data of the DCS and the SOE Viewer in SENG, and makes a work procedure for removing the cause of the fault.
3. The maintenance personnel remove the cause of the fault according to the work procedure.
4. The maintenance personnel operate a shutdown reset from the ESD console.
5. Confirm the state of the plant again to restart the plant according to the operation manual.

Operation when ProSafe-RS equipment fails

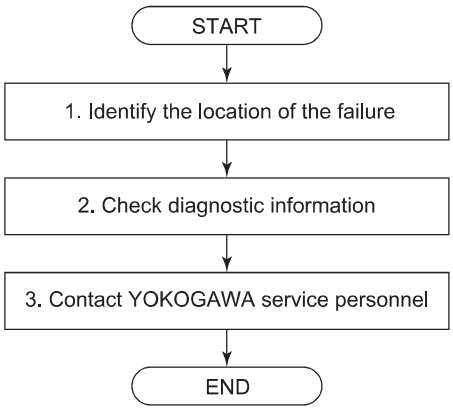


Figure G1-4 Operation when ProSafe-RS equipment fails

1. The engineer starts the SCS State Management window from SENG of the SCS where a fault occurs and confirms the present status on the display. A diagnostic information mark is displayed for I/O modules having a diagnostic fault. The engineer selects the I/O module, and display Diagnostic Information window of the I/O modules to confirm a Diagnostic Information Message related to the I/O modules.
2. The engineer confirms the messages generated by the diagnostic function of SCS. Double-click the message for the corresponding measures. This opens the Help dialog box in which the measures are indicated. Clicking a relevant message in the Diagnostic Information Window and then a [confirmation] button on the Toolbar opens the Confirmation dialog box. Diagnostic Information Messages can be confirmed by pressing the [confirmation] button on this dialog box (Operation for confirming individual messages).
3. Inform the service section at YOKOGAWA of the above information.

G2. Operations and recovery procedures during the SCS error occurrence

This chapter explains the action taken when an error occurs in the system and the recovery procedures. If an error occurs in the system, operations corresponding to the error level are performed.

There are the following three error levels.

- Fatal error
- Major error
- Minor error

TIP

In this document, I/O shutoff switches and DO shutoff switches of the universal type I/O module are referred to as an output shutoff switch.

SEE ALSO

For more information about operations at minor error occurrence and recovery procedure, refer to:

G2.3, “Actions taken at minor error occurrence and recovery procedure” on page G2-35

Overview of system operations at occurrence of fatal errors and major errors

The following provides an overview of system operations corresponding to the different SCS error levels.

Actions taken at fatal error occurrence

A fatal error disables hardware and/or software so that operation cannot be continued. Both sides of a redundant CPU module stop and all output modules output the fail-safe value.

Actions taken at major error occurrence

When a major error occurs, some hardware cannot continue the ordinary operation. When an error occurs, the system takes action which you have configured in advance for the failure of hardware. The application logics that handle major errors must also be configured.

Shutdown operations

The shutdown operations fix the output status from an SCS. There are the following three types of operations:

- Shutdown executed by a user-defined application logic
- Shutdown where the CPU fixes the output values of areas with failures
- Shutdown executed by an output module when it detects an error in the host system (CPU)

When a fatal error occurs, the CPU stops and all output modules shut down; this is called all output shutdown.

Output value at fault

The value that is output as the fail-safe value when an output module detects an error is called the Output Value at Fault. This value can be specified as an I/O Parameter for each DO or AO channel. Specify the following I/O Parameter.

Table G2-1 I/O Parameter for specifying an output value at fault

	For I/O list engineering: Safety I/O Editor of AD Suite	For RS original engineering: I/O Parameter Builder
FIO DO	Output Processing at Fault	Output Value in Detecting Error
N-IO DO	Output Processing at Fault	Output Processing at Fault (*1)
FIO AO N-IO AO	Output Processing at Fault and Output Value at Fault	Output Processing at Fault and Output Value at Fault (*1)

*1: When you use N-IO, I/O list engineering is recommended.

For AO, specify whether holding the output or outputting a fixed value in Output Processing at Fault. To output a fixed value, specify a value in Output Value at Fault.

IMPORTANT

In FIO DO, the I/O Parameter name of the setting destination is different in AD Suite and I/O Parameter Builder. The item you specified in Output Processing at Fault in AD Suite is reflected to Output Value in Detecting Error of I/O Parameter Builder when you run Reflection.

The output module does not output the "Output Value at Fault" in following status:

- The output module being initialized
- The output module with Output Shutoff switch and the switch is energized.
- The malfunctioning output channel or the output module

TIP

The descriptions in the later chapters will have the explanations regarding the tight-shut values may become the output values of the analog output modules when the Tight-Shut/Full-Open function is enabled with an I/O parameter. However, if the Tight-Shut/Full Open function is disabled, the output value of the module becomes the "default initial value upon power-on" instead of the tight-shut value.

SEE ALSO

For more information about “Tight-shut/full-open” functions and “output value upon power-on”, refer to:

“■ Tight-shut/Full-open” on page App.1-27

G2.1 Actions taken at fatal error occurrence and recovery procedure

The CPU stops if a fatal error occurs in it. If the CPU module is in redundant configuration and the control right is switched to the CPU module on the standby side, the error is treated as a minor error. If the error affects the entire system, no output can be made, but in other cases, communication from the CPU is stopped; all output modules output the fail-safe value at CPU error. The fail-safe value is the value defined by the user in advance in an I/O parameter as the value output by output modules when the CPU fails.

G2.1.1 Operations and recovery procedures during the error occurrence in the entire SCS

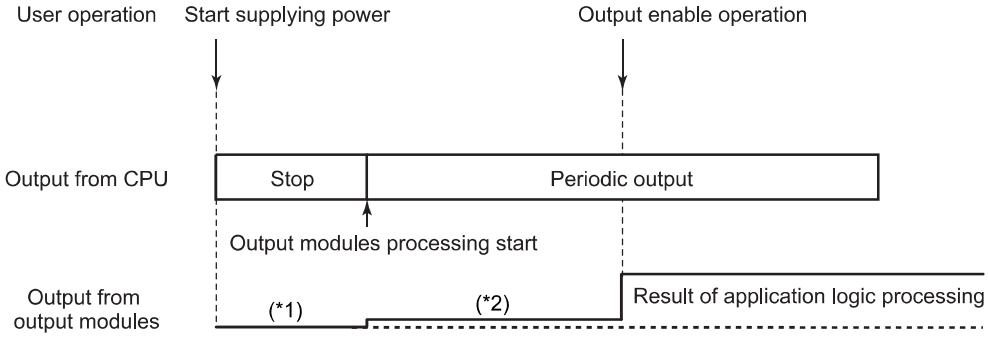
This is an operation which is performed when electric supply is started or stopped for the entire SCS including CPU modules and I/O modules.

Actions taken at error occurrence

Regardless of the duration of a power failure, the initial start processing is performed when the power supply to the CPU nodes is renewed. Once the power is supplied to the system, I/O module startup processing is performed and the operating mode shifts to the Waiting mode. After the starting the I/O module, "0" is output from the DO channel while the tight-shut value is output from the AO channel to the field.

Recovery procedure

The user should perform the output enable operation from the SENG after confirming that all output modules have been started successfully. Once the output enable operation is performed, output values of the application logic are output to the field. When all outputs are placed in the Output Enable status, the operating mode shifts to the Running mode.



*1: “0” for DO modules, and “0.0 [mA]” for AO modules.
*2: “0” for DO modules, and the tight-shut value for AO modules

Figure G2.1.1-1 Recovery from errors affecting the entire system

G2.1.2 Actions taken at CPU module error occurrence and recovery procedure

If an error occurs in the hardware of the CPU module, CPU node or software, only the CPU stops. If the CPU module is placed in redundant configuration, it is judged that a fatal error has occurred when both CPUs fail.

The CPU also stops when offline download is performed to an operating SCS.

Actions taken at error occurrence

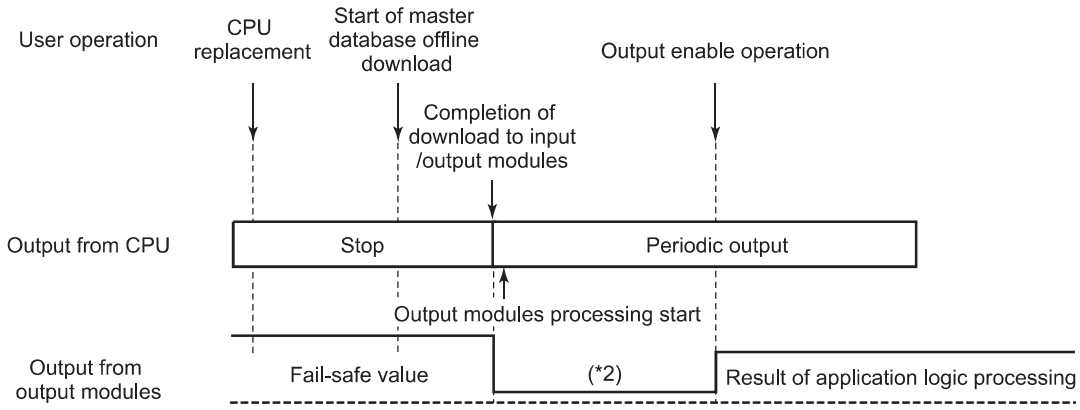
If the CPU does not create any data output for a certain length of time, the connected output modules will assume that the CPU is in a status where it cannot set an output value, and all output modules will output each fail-safe value specified by the user in advance. (This is called as "All output shutdown.") Input modules, on the other hand, are not affected by CPU errors. In the case of redundant CPU modules, the same operation as for a single CPU module configuration is performed if the module on the standby side fails.

Recovery procedure

In order to recover from an error occurred in the CPU module, the CPU module replacement may or may not be necessary.

Recovery procedure by replacing a failed CPU module

The following figure illustrates the output values from the SCS after the CPU module has been replaced, based on a single CPU module configuration.



*1: In the master database offline download, configuration information is downloaded to the I/O modules.
*2: "0" for DO modules, and the tight-shut value for AO modules.

Figure G2.1.2-1 Recovery after CPU module replacement

SEE ALSO For more information about the procedure for replacing the CPU module, refer to:

I1.2, "Maintenance for ProSafe-RS equipment" on page I1-9

Recovery procedure after the CPU module is restarted

Follow the recovery procedure below if the CPU module is restarted when the CPU and software are normal.

1. Fail-safe values are being output to the field from output modules. When the CPU starts up, the states of input/output modules are checked and the operating mode shifts to the Waiting mode.

2. Perform the output enable operation from the SCS Maintenance Support Tool of the SENG.
   When output modules are placed in the Output Enable status, the result of the application logic processing is output to the field. The operating mode shifts to the Running mode.

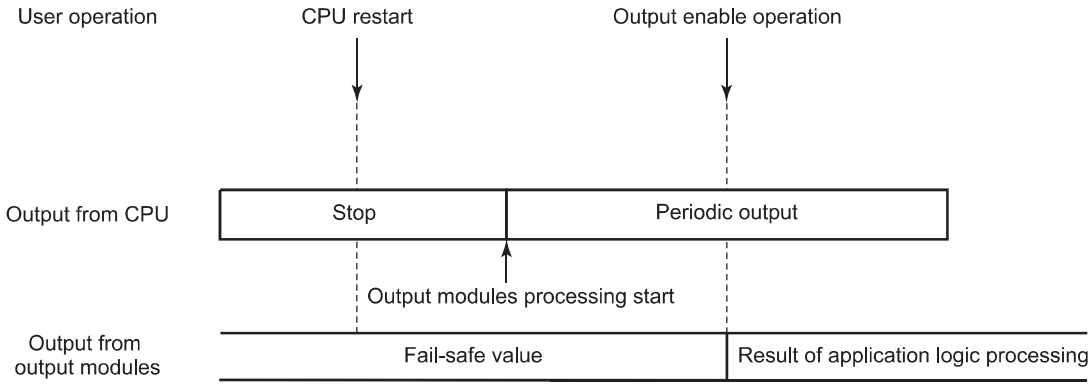


Figure G2.1.2-2 Recovery when the CPU module is restarted

Offline download

If you perform offline download to the running SCS, the CPU stops temporarily.

Also, IOM download is performed to all I/O modules.

Once an offline download is started, the output values from output modules will conform to the Figure "Recovery after CPU Module Replacement."

G2.1.3 Behavior at abnormal calculation

If there are mistakes in the application logic, intended control can no longer be performed. For the sake of safety, such mistakes must be completely removed before starting the actual operation, by thoroughly checking and testing in advance.

If there is any mistake that is left undeleted, causing overflow and other abnormal calculations during execution of the application logic, SCS stops because correct control cannot be continued. However, by making specifications with a builder, it is possible to avoid stoppage of SCS and continue the operation (*1). Diagnostic information messages are generated at occurrence of abnormal calculation and upon recovery respectively.

*1: Supported in the SCS of SCS system program R2.03 or later.

IMPORTANT

The purpose of this function is to temporarily avoid the error conditions of SCS. If an abnormal calculation occurs, review the application logic as soon as possible and modify the logic such that the abnormal calculation will not recur.

The SCS automatically recovers if the cause of abnormal calculation is removed or resolved.

Specification of behavior at abnormal calculation

Use the SCS Constants Builder to specify the behavior at abnormal calculation.
If "Continue operations" is specified, the SCS will not fail and will continue operations even if any of the following abnormal calculations occur.

- Division by zero
- Access to the outside of an array
- Overflow in floating-point calculation
- Overflow in casting

SEE ALSO For more information about how to specify the behavior upon abnormal calculation with SCS Constants Builder, refer to:

C1.2.6, “SCS Constants Builder” on page C1-21

Occurrence of division by zero

A division-by-zero calculation error occurs under the following conditions and is processed as follows.

Occurrence conditions

The denominator is zero in a division of DINT or REAL type data.

SCS processing at error occurrence

If "SCS fails" is specified in SCS Constants Builder, SCS fails.

But if "SCS continues" is specified and this error occurs, the maximum value of the applicable type (the maximum negative value if the value is negative) is assigned to the variable of the operation result. The POU (program) where the calculation error occurred does not stop but operates until the end.

Access to the outside of an array

An access to the outside of an array occurs under the following conditions and it is processed as follows.

Occurrence conditions

An index of an array variable points to the outside of the array.

SCS processing at error occurrence

If "SCS fails" is specified in SCS Constants Builder, SCS fails. But if "SCS continues" is specified and this illegal access occurs, the corresponding POU (function/function block) is stopped immediately. The POU is executed in the next and subsequent scans as well, but the execution is stopped at the same location unless the problem is resolved.

The POU (program/function/function block) that called the function/function block in which the calculation error exists is executed until the end.

SCS processing at error occurrence when SCS continues the control (details)

If you specify a value exceeding an array size for an index of an array variable in a user-defined function or user-defined function block described in the ST language, an error of accessing outside the array range occurs. The processing of the user-defined function or user-defined function block that caused the error is terminated immediately.

- The return value of the user-defined function is zero (in the case of DINT, REAL or TIME type) or FALSE (BOOL type).
- In the case of user-defined function blocks, the output parameters that were written before the occurrence of access to the outside of an array maintain the written values, and the output parameters that were not written maintain the previous values. The same rule applies to the local parameters as well.
- The values above are passed to the POU that called the user-defined function or user-defined function block where the illegal access occurred and the POU is executed until the end.

Overflow in floating-point calculation

An overflow in floating-point calculation occurs under the following conditions and is processed as follows.

Occurrence conditions

An overflow occurs in calculation between REAL type operands(*1)

*1: An overflow in integer calculation is not regarded as abnormal calculation.

SCS processing at error occurrence

If "SCS fails" is specified in SCS Constants Builder, SCS fails.

But if "SCS continues" is specified and this error occurs, the maximum value of the given type is assigned to the variable of the operation result. The maximum negative value is assigned if the first operand is negative in the case of addition/subtraction as well as if the signs of first and second operands are different in the case of multiplication/division.

The POU (program) where the calculation error occurred does not stop but operates until the end.

Overflow in casting

An overflow in casting occurs under the following conditions and is processed as follows.

Occurrence conditions

When casting REAL type data to BOOL, DINT or TIME type, the resultant value exceeds the maximum value that can be expressed by the variable.

SCS processing at error occurrence

If "SCS fails" is specified in SCS Constants Builder, SCS fails.

But if "SCS continues" is specified and this error occurs, the following values are assigned to the variables of the calculation results.

Table G2.1.3-1 Value of the variable to which the result of calculation is assigned

Variable type	Value
BOOL	TRUE
DINT	Maximum value of the DINT type (the maximum negative value if the value is negative)
TIME	Maximum value of the DINT type

The POU (program) where the calculation error occurred does not stop but operates until the end.

SCS processing at error occurrence when SCS continues the control (details)

- Casting from REAL type variable to DINT type
  When casting a value of a REAL type variable to DINT type using the ANY_TO_DINT operator, if the original value is greater than the maximum value that can be expressed by DINT type, the calculation result is replaced by the maximum DINT value (the maximum negative DINT value if the original value is negative).
- Casting from REAL type variable to TIME type variable
  When casting a value of a REAL type variable to TIME type using the ANY_TO_TIME operator, if the original value is greater than the maximum value that can be expressed as an unsigned 32-bit integer, the calculation result is replaced by the maximum value of an unsigned 32-bit integer. Although the TIME type can express up to 24 hours, truncation is not performed immediately when an overflow occurs; truncation is performed in the subsequent arithmetic calculation. (The TIME type does not take a negative value, but if a negative value is assigned in ANY_TO_TIME, the value is converted to a signed 32-bit integer once and then treated as TIME type keeping the bit sequence.)

Notification of abnormal calculation occurrence/recovery

Occurrence of abnormal calculations and recovery from them are notified via diagnostic information messages if SCS continues the control. By using the system function block (SYS_CERR), whether a calculation error has occurred or not can be handled in the application logic.

Notification of abnormal calculation occurrence

If a calculation error occurs, it is notified by the diagnostic information message (No. 4145) that indicates an occurrence of abnormal calculation. If calculation errors occur in multiple POUs (programs), a diagnostic information message is generated for each POU (program).

If different types of calculation errors occur in the same POU (program) at the same time, a diagnostic information message is generated for each type of calculation error.

● Re-notification of abnormal calculation occurrence

If the abnormal calculation status continues for a certain period of time or longer, the diagnostic information message notifying the abnormal calculation is generated repeatedly as warning. The re-warning interval is 10 minutes by default.

The re-warning interval can be changed using SYS_CERR.

● Handling of abnormal calculation status with application logic

The abnormal calculation status can be handled in the application logic by using the system function block (SYS_CERR). (*1)

*1: SYS_CERR can be used in SCS databases created by SENG of R2.03.00 or later.

● Notification of recovery from abnormal calculation

If the POU (program) that previously caused a calculation error is executed normally until the end, the calculation error of the POU (program) is regarded to have been cancelled and the diagnostic information message indicating recovery from abnormal calculation (No. 4146) is notified. The diagnostic information message indicating recovery is generated for each diagnostic information message notifying error occurrence.

■ Behavior in test functions

In logic simulation tests and SCS simulation tests, behaviors at abnormal calculation are different from those in the actual system.

SEE ALSO For more information about the behavior upon occurrence of an abnormal calculation with the test function, refer to:

"● Actions on abnormal calculation" in "■ Debug and test" in 2., "Logic simulation test operations" in Test Function Guide (IM 32P04B30-01EN)

G2.2 Actions taken at major error occurrence and recovery procedure

This section explains the operations of an SCS when a major error occurs and the recovery procedure, for the cases where errors occur in the following locations.

- Input module
- Output module
- Universal type I/O module
- Input channel
- Output channel
- Communication path between the CPU module and input/output modules
- Optical ESB bus repeater devices
- N-IO related hardware
- Safety subsystem communication paths, safety subsystem communication, and fire and gas communication modules

Notification of error status

An SCS notifies the application logic of the fact that an error occurred. It also notifies errors to the user via the SCS State Management Window of the SENG, the Status Display view of the HIS, and diagnostic information messages.

Since the following processing is performed, the user can create a shutdown application logic based on these conditions to determine desired output values for each output module.

- The status of channels belonging to the area with the failure becomes BAD.
- The status is reflected in the system function block.
- In the case of errors related to input modules and/or channels, the input value is set to the "Input value at error occurrence." The "Input value at error occurrence" is provided to the application logic instead of the actual process value if an error is detected in input module . The user must define in advance the "Input value at error occurrence" for each channel with an I/O parameter.

SEE ALSO For more information about the items to be defined as I/O parameters, refer to:

Appendix 1.3, “Settings for channel items” on page App.1-8

Recovery from error state

The following subsections explain the recovery measure to be taken for I/O modules when a major error occurs.

The following operations are needed to recover from an error.

- IOM download
- Output enable operation (for output modules only)

G2.2.1 Actions taken at input module error occurrence and recovery procedure

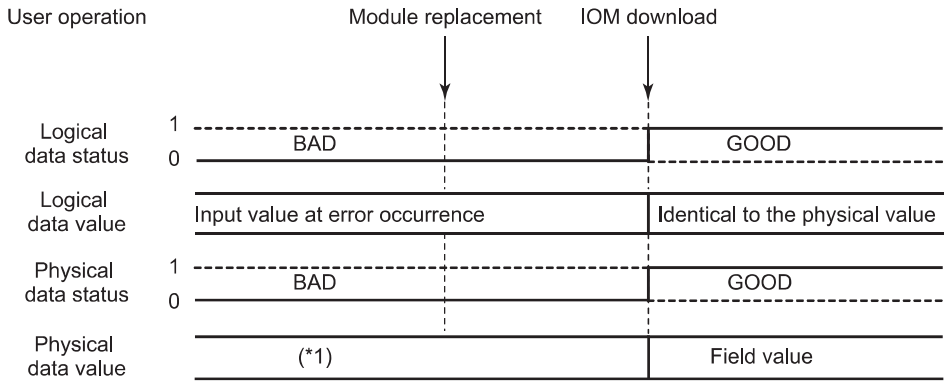
If there is a malfunction in an input module hardware, SCS treats it as an input module error. In the case of a redundant input module, the control rights switches, but the application logic continues running. This is considered as a minor error. The following explains the operations performed when an error occurs in the case of modules in single configuration or single operation status.

Actions taken at error occurrence

- CPU processing
  When an input module fails, the CPU sets the pre-defined values in the I/O parameters to all channels of the module and force the data status to BAD. The application logic should handle these changes in the inputs and statuses as errors. In order to prevent the plant from the fatal damages caused by input module failures, application logics for detecting the failures and handling the errors should be created.
- Error notification
  A module error is notified via a diagnostic information message (alarm class 1). In the SCS State Management Window on the SENG or the Status Display view on the HIS, the failed module is shown in red to indicate an error.

Recovery procedure

1. Investigate the cause of the failure based on the error code shown in the IOM Report.
2. If the input module itself is faulty, replace the module.
   If the cause of the failure is on the field side, remove the abnormality on the field side.
3. From the SCS Maintenance Support Tool of the SENG, execute IOM download.
   The CPU starts up the input module, and once the input value is acquired normally, the data status returns to GOOD.



*1: The value varies with the input module type and status.

Figure G2.2.1-1 Input module error

G2.2.2 Actions taken at input channel error occurrence and recovery procedure

An input channel error typically occurs in two cases, when there is an error on the field side or when there is a hardware failure in individual channels of an input module.

Actions taken at error occurrence

- CPU processing
  The CPU sets the input value at error occurrence, which is a value defined by the user in advance in an I/O parameter, for the faulty input channel and sets the data status to BAD.

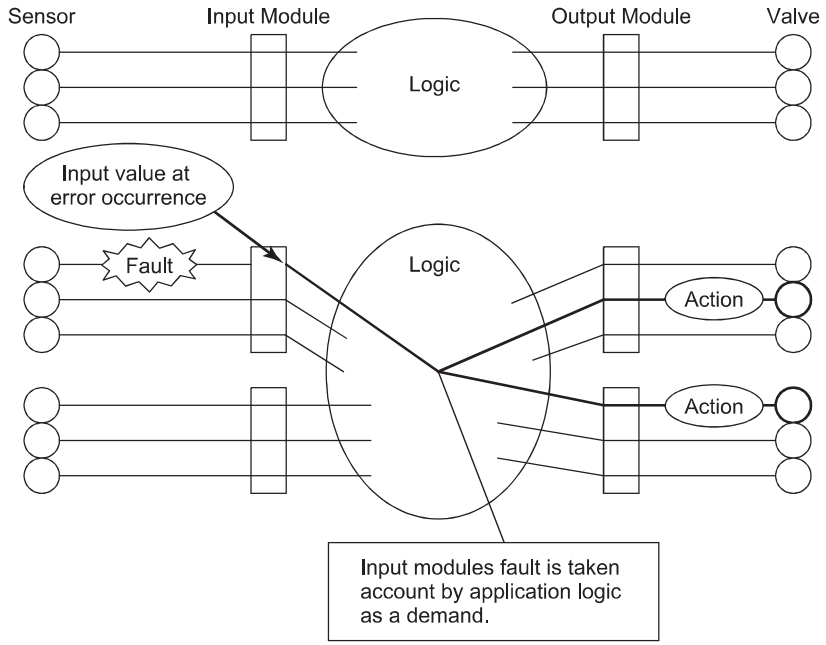


Figure G2.2.2-1 Overview of operation when an input channel error is detected

- Error notification
  A channel error is notified via a diagnostic information message (alarm class 1). However, the SCS State Management Window of the SENG and the Status Display view of the HIS display the module where channel error has occurred in the color that indicates normal.

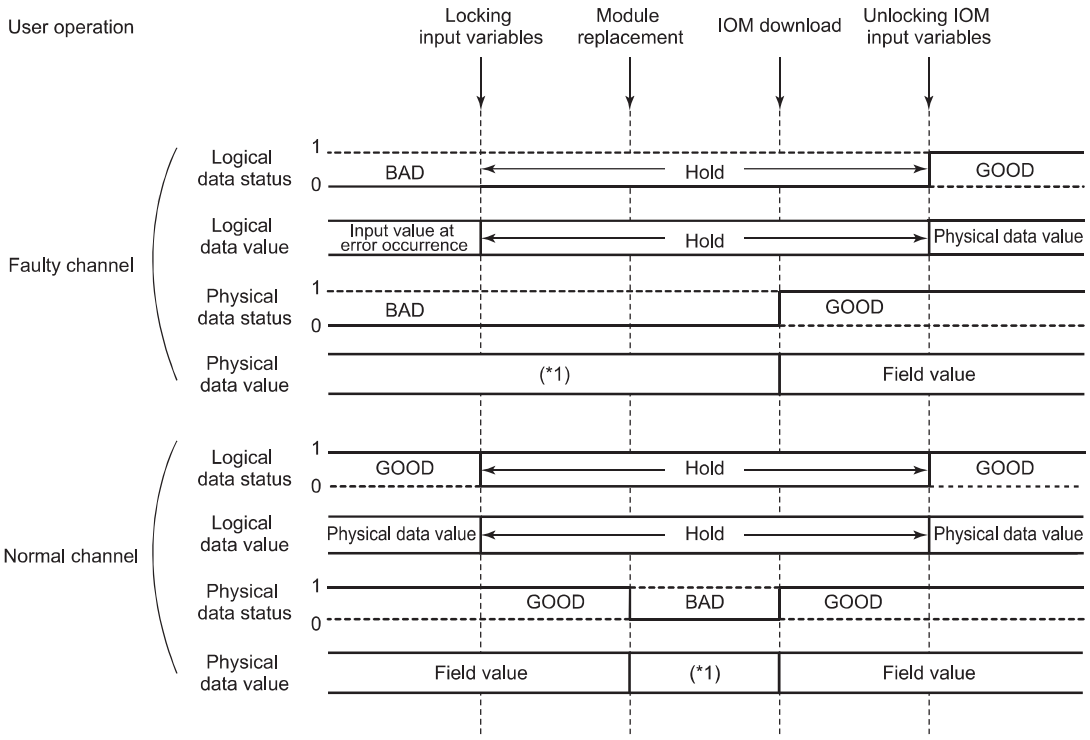
Recovery procedure

The type of recovery procedure to be used depends on whether or not the error occurred on the module side.

Recovery procedure in the case of error on the module side

If a hardware error occurred in one or more channels of an input module, the input module needs to be replaced. The module replacing procedure for single module configuration is as follows:

1. Fix the input values sent to the application logic from the related input variables. Use the locking operation of the forcing function or maintenance override in order to fix the input variables. This minimizes the impact at module replacement.
2. After replacing the module, perform IOM download.
   The input module starts up normally.



*1: The value varies with the input module type and status.

Figure G2.2.2-2 Input module replacement (with locking operation)

SEE ALSO For more information about operations for locking input variables, refer to:

F8.8, “Windows used for forcing of I/O variables” in Engineer's Reference Manual (IM 32P04B10-01EN)

Recovery procedure in a case where the module is normal

If a failure is discovered in the field or input module connection, remove the cause of the failure. Removing the cause of the failure allows the channel with the failure status to go back to using the field value, and the data status changes to GOOD.

G2.2.3 Actions taken at output module error occurrence and recovery procedure

The result of the application logic processing is set to the logical data and physical data of the relevant output variables, and this data is then written to each channel of the corresponding output module via the I/O driver. On the other hand, the CPU acquires the status of the output module as well as the status of each channel of the output module, and sends diagnostic information messages or reflects the state information in the system function block used for channel status display. By using a system function block, module/channel statuses can be monitored via the application logic. The figure below illustrates the relationship between the CPU and output module.

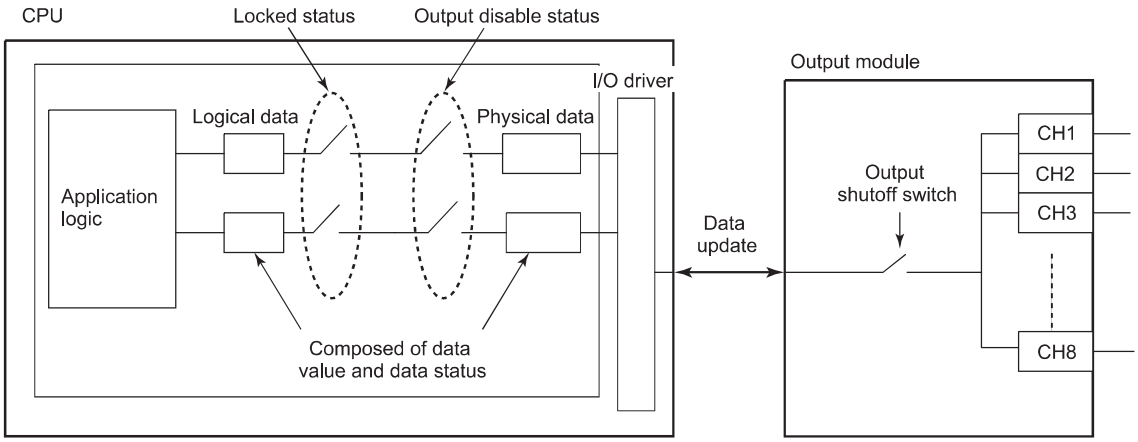


Figure G2.2.3-1 Overview of CPU and output module

Actions taken at error occurrence

If any output module has failed, the SCS performs failure diagnosis and switches the control right and/or sends diagnostic information messages. If the control right of the duplexed modules has been switched, the actions corresponding to a minor error is taken.

If the output module was operating in the single operation mode, the following actions are taken.

- CPU processing
  The CPU sets the fail-safe value, which is predefined in an I/O parameter, to the physical data of each output channel of the faulty output module and places all the output channels in the Output Disable status. At this point, the operating mode shifts to the Waiting mode. Writing to the output module is stopped thereafter. The data statuses of all channels of the output module become BAD. The user can configure the application logic so that other associated outputs are shut down automatically based on data status changes of specific output channels to BAD.
- Error notification
  A module error is notified via a diagnostic information message (alarm class 1). In the SCS State Management Window on the SENG or the Status Display view on the HIS, the failed module is shown in red to indicate an error.

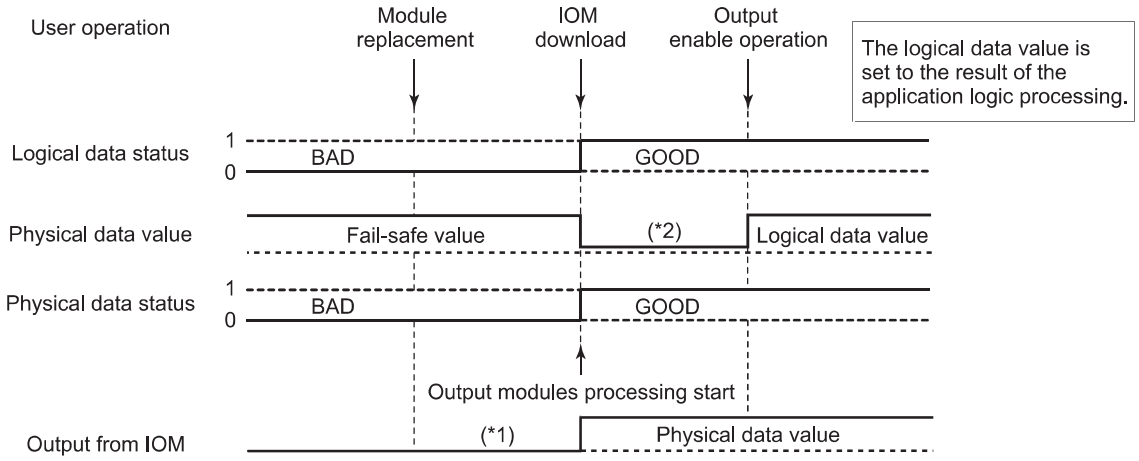
Recovery procedure

The procedure for recovery from an output module error is as follows:

1. Investigate the cause of the failure based on the error code shown in the IOM Report.
   If a system function block for output status display is used, the failure location can be checked.
2. If the output module itself is faulty, replace the module.
   If the cause of the failure is on the field side, remove the abnormality on the field side.

3. From the SCS Maintenance Support Tool of the SENG, execute IOM download.
   After the IOM download, the CPU performs startup processing of the output module. If the startup processing is completed, the output module is recognized as normal and data update starts. After the module returns to normal, "0" is output for DO modules, while the tight-shut value is output for AO modules, from all channels of the output modules.
4. Test the output module.
5. From the SCS Maintenance Support Tool of the SENG, perform the output enable operation.
   Output values of the application logic will be output. Once all output channels are placed in the Output Enable status, the operating mode shifts to the Running mode.

The figure below illustrates the flow from a failure of an output module to the recovery.



*1: “0” for DO modules, and “0.0 [mA]” for AO modules.
*2: “0” for DO modules, and the tight-shut value for AO modules.

Figure G2.2.3-2 Recovery from output module error with module replacement

G2.2.4 Actions taken at output channel error occurrence and recovery procedure

An output channel error typically occurs in two cases, when there is an error on the field side or when there is a hardware failure in individual channels of an output module. Depending on the cause of the failure, the Output Shutoff switch in the output module may be activated and an output module failure may occur, in which case the action take at error occurrence and recovery procedure may be different from those applicable to an output channel error.

To prepare for output channel failures, an application logic must be created in advance for each output channel using a function block for system status indication.

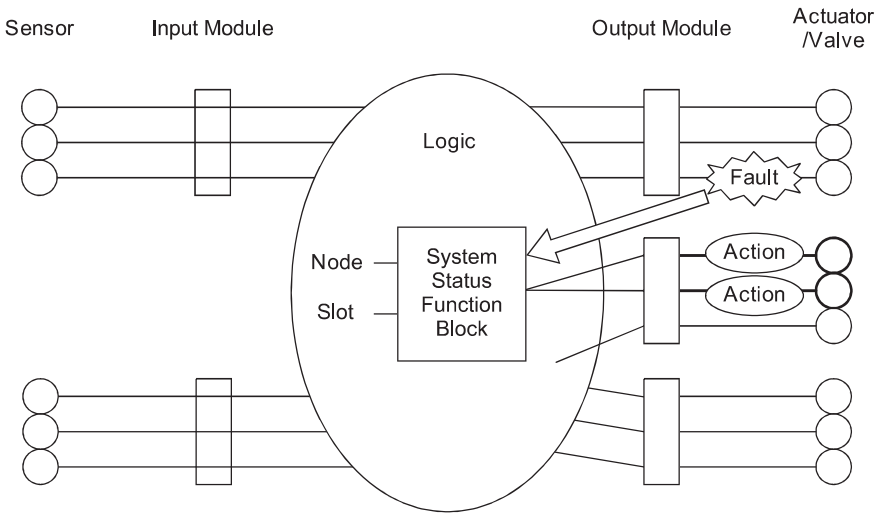


Figure G2.2.4-1 Description of logic related to output failure

SEE ALSO For more information about function blocks for system status indication, refer to:

11., “Safety system function blocks” in POU Reference Manual (IM 32P03B20-01EN)

Actions taken at error occurrence

The actions taken at error occurrence are explained for each of the following two cases: when the Output Shutoff switch is activated and when an error occurs in a single output channel without activating the Output Shutoff switch.

Channel errors accompanied by activation of the Output Shutoff switch

Even when the failure concerns only a certain output channel, the entire output module may be affected if the Output Shutoff switch in the output module is activated. In this case, "0" and "0.0 [mA]" are output from all output channels for the DO modules and AO modules, respectively.

The targets of output shutoff operation include dangerous failures (such as DO module channels are clutched to ON status) and failures where internal module protection is required (such as overcurrent of AO modules). However, the user can define in an I/O parameter whether to activate the output shutoff switch for dangerous failures where module protection is not required by the system.

The user must determine if the failure occurred in the field or in the module, based on the detailed error information provided in the Diagnostic Information window and IOM Report dialog box.

SEE ALSO For more information about IOM Report, refer to:

H3.1, “IOM Report of AIO/DIO modules” on page H3-2

Operation at occurrence of output channel errors

Errors that do not activate the Output Shutoff switch, such as disconnection on the field side, are notified as failures of individual output channels. The following operations are performed if errors occur in individual output channels.

- CPU processing
  The CPU sets the fail-safe value, which is predefined in an I/O parameter, in the physical data of the faulty output channel and places the channel in the Output Disable status. At this point, the operating mode shifts to the Waiting mode. Other normal output channels output the result of the application logic processing. The CPU continues updating the data of the output module.
- Error notification
  An output channel error is notified via a diagnostic information message (alarm class 1). The data status of the faulty output channel is set to BAD. In the SCS State Management Window on the SENG and the Status Display view on the HIS, the output module is shown in the color indicating a normal state. The status of each channel can be checked in the Diagnostic Information window of SCS Maintenance Support Tool of the SENG.

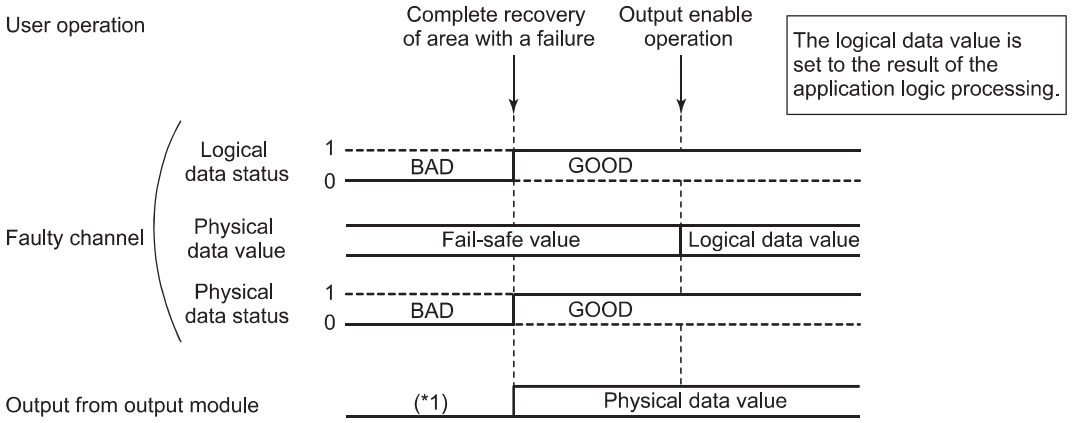
Recovery procedure

If a channel error occurred, check the following in the SCS State Management Window and IOM Report dialog box in the SCS Maintenance Support Tool to determine an appropriate recovery measure.

- Has the Output Shutoff switch been activated? Does the error concern only one channel?
- Is it a hardware failure in the module or an error on the field side?

Single channel errors (disconnection and other errors on the field side)

1. Investigate the cause of the failure and recover the field side.
   When the output module recovers, a recovery message is output and the fail-safe value, which was defined by the user in advance, is output from the relevant output channel.
2. After confirming that the output module has recovered to normal, perform the output enable operation from SCS Maintenance Support Tool of the SENG.
   Output values of the application logic will be output.

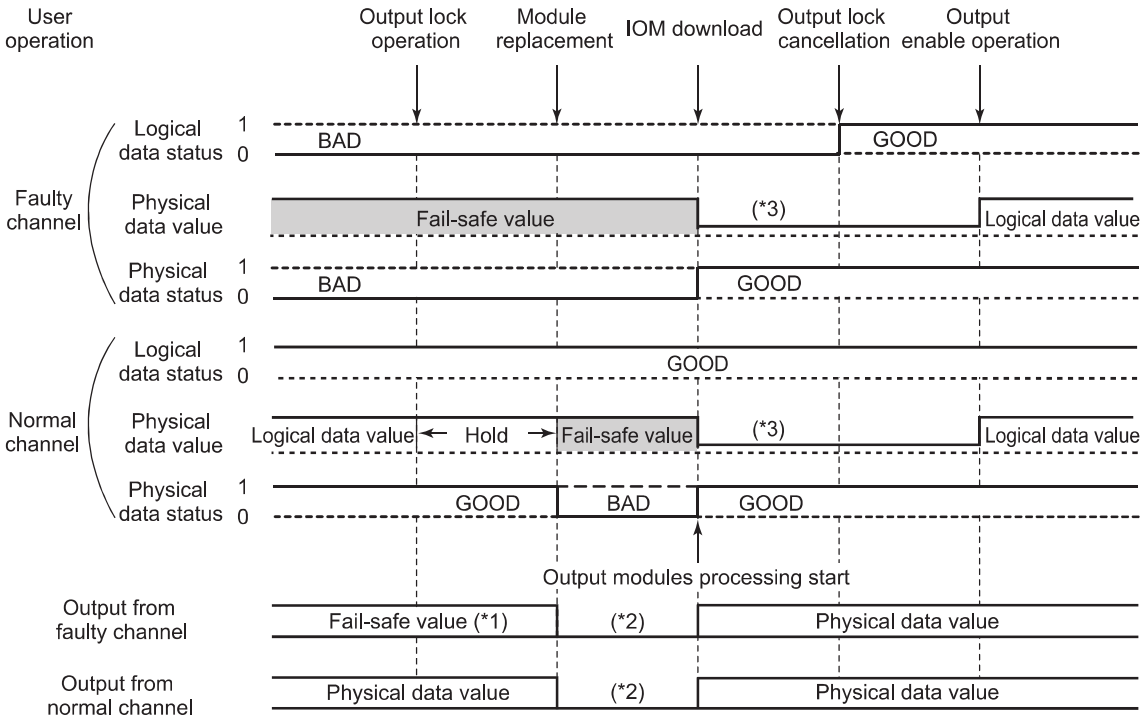


*1: “0” for DO modules, and “0.0 [mA]” for AO modules.

Figure G2.2.4-2 Recovery from channel errors

In the case of errors on a single channel (module channel hardware failure)

If any of the channels on the module side is judged to be erroneous, the output module must be replaced. The figure below illustrates the recovery procedure and the data value and data status at each timing.



*1: Fail-safe value (This value may be set to “0” for DO modules and “0.0 [mA]” for AO modules, depending on the failure condition.)
*2: “0” for DO modules, and “0.0 [mA]” for AO modules.
*3: “0” for DO modules, and the tight-shut value for AO modules.

Figure G2.2.4-3 Recovery from channel errors (with module replacement)

When the Output Shutoff switch has been activated

If the Output Shutoff switch has been activated, the following values are output from all the channels of the module.

- DO module: 0
- AO module: 0.0 [mA]

If the Output Shutoff switch has been activated, check the module status color shown in the SCS State Management Window.

- When the module status is red
  If the module status is shown in red, the possible causes of failure are as follows:
  - Hardware failure of module channels
  - Error on the field side

  See the IOM Report and identify which is the case. In both cases, the recovery measures are the same as the procedures taken after an error concerning an individual channel. Follow the recovery procedure for errors on the field side or hardware failure depending on the situation.
- When the module status is blue

If the module status is shown in blue, the output module is in the startup wait status. In this case, perform the following recovery procedure.

1. Investigate the cause of the failure and recover the field side.
2. When the recovery procedure has completed, perform the "Start output module" from the SCS Maintenance Support Tool of the SENG.

   The CPU performs the startup processing of the output module. When the output module recovers to normal status, the data status returns to normal.
3. From the SCS Maintenance Support Tool of the SENG, perform the output enable operation.
   Output values of the application logic will be output.

SEE ALSO

For more information about starting output module operation, refer to:

"■ Start output module operation" on page C8-1

For more information about procedures for recovery from an error on the field side, refer to:

"● Single channel errors (disconnection and other errors on the field side)" on page G2-18

For more information about procedures for recovery from a channel hardware failure, refer to:

"● In the case of errors on a single channel (module channel hardware failure)" on page G2-19

■ Operation and recovery procedure when overload state is detected while SDV526/L1DV526 is outputting ON signal

This section describes the operations of the module and the recovery procedure for cases where an output overload state (*1) has occurred while SDV526/L1DV526 is outputting ON signals. When SDV526/L1DV526 is in a redundant configuration, signals are output from both modules, so the operation on the detection of an overload state and the recovery procedure are described separately for the active module and standby module.

The operation in a non-redundant configuration is the same as the active module in a redundant configuration.

*1: An overload state occurs when the connected field device has a fault that causes a short circuit or overcurrent when the output from the module is set to ON.

● Behavior of SCS and recovery procedure when the active module in redundant configuration or module in non-redundant configuration has failed

- Behavior
  - If an overload state is detected only in the active module of redundant configuration, the control right is transferred to the standby module and the operation continues. (*1)If an overload state is detected on both modules, the standby module goes to IOM Fail and the control right is not transferred.
  - The module sets the output signal of the error channel to OFF, and the channel goes to an Output Disable status.
  - The channel is released from the error but it remains in the Output Disable status.

  *1: In this case, recover the error module that has become a standby module by carrying out the recovery procedure for a standby module.
- Recovery procedure
  1. Clear the cause of overload state to recover the field device.
  2. Use the SCS maintenance support tool on SENG and perform the output enable operation.
     This allows the output value of the application logic to be output.

Behavior of SCS and recovery procedure when the standby module in redundant configuration has failed

- Behavior
  - The output shutoff switch is activated and the standby module goes to IOM Fail.
  - In the SCS State Management Window of the SCS maintenance support tool, the module's status is shown in blue (startup wait status).
- Recovery procedure
  1. Clear the cause of overload state to recover the field device.
  2. Use the SCS maintenance support tool on SENG and perform the output module startup operation.
     The module starts up and operates as a standby module.

Behavior of SDV521/L1DV521 or SDV53A/L1DV53A and recovery procedure when a short circuit is detected

This section describes the behavior of the SDV521/L1DV521 or SDV53A/L1DV53A module and the recovery procedure for cases where a short circuit has occurred in the field wiring of the module.

- Behavior
  - The module sets the output signal of the error channel to OFF, and the channel goes to an Output Disable status.
  - The channel may be released from the error but it remains in the Output Disable status.
- Recovery procedure
  1. Clear the cause of short circuit to recover the wiring on the field side.
  2. Use the SCS maintenance support tool on SENG and perform the output enable operation.

     This allows the output value of the application logic to be output.

G2.2.5 Operations and recovery procedures during the error occurrence in the universal type I/O module

If there is a malfunction in the hardware of I/O module, an error occurs in universal type I/O module. If the I/O module is redundant, the control rights are switched, and the application logic continues running. This is considered as a minor error. The following explains the operations performed when an error occurs during the single configuration or single operation.

Operations during error occurrence in the I/O module

Operations during the error occurrence in the I/O module differ depending on the set channel type.

If the channel of the I/O module is set to input, operations are similar to when an error occurs in the input module.

If the channel of the I/O module is set to output, operations are similar to when an error occurs in the output module.

I/O module recovery procedures

Recovery procedures for the I/O module differ depending on the set channel type.

If the channel of the I/O module is set to input, recovery operations are similar to when an error occurs in the input module.

If the channel of the I/O module is set to output, recovery operations are similar to when an error occurs in the output module.

SEE ALSO For more information about operations at input module error occurrence and recovery procedure, refer to:

G2.2.1, “Actions taken at input module error occurrence and recovery procedure” on page G2-12

For more information about operations at output module error occurrence and recovery procedure, refer to:

G2.2.3, “Actions taken at output module error occurrence and recovery procedure” on page G2-15

Operations at input channel error occurrence and recovery procedure

Operations and recovery procedures during input channel error occurrence in the universal type I/O module are the same as those for input channel error occurrence in an input module.

SEE ALSO For more information about operations at input channel error occurrence and recovery procedure, refer to:

G2.2.2, “Actions taken at input channel error occurrence and recovery procedure” on page G2-13

Operations at output channel error occurrence and recovery procedure

This section describes the operations and recovery procedures when an output channel of the universal type I/O module has failed under the following conditions:

- When the Output Shutoff switch is activated
- When an output channel fails without activating the Output Shutoff switch

Output shutoff switch of the universal type I/O module

The output shutoff switch in the universal type I/O module is different depending on the set channel signal type.

- DO channel : DO shutoff switch
- AO channel: I/O shutoff switch

The following shows the channel operations when a DO shutoff switch and I/O shutoff switch have been activated.

- When DO shutoff switch is activated due to malfunction detection by DO channel:
  An error occurs with all DO channels in the universal type I/O module and the output of the corresponding channels are shut off.
- When an I/O shutoff switch has been activated upon detection of a failure by the AO channel
  An error occurs with all AI (2-wire), AO, DI, and DO channels in the universal type I/O module and the input and output of the corresponding channels are shut off.

Channel errors during output shutoff switch operation

When DO shutoff switch in the universal type I/O module is activated during the error occurrence, the output of all DO channels in the I/O module becomes 0, even if the error occurs only in a certain output channel.

Similarly, when an internal I/O shutoff switch in the universal type I/O module is activated, the outputs of all AO channels in the I/O module become 0.0 [mA] and the output of the DO channel becomes 0. If the universal type I/O module has an input, the inputs of all AI (2-wire) channels and DI channels in the I/O module become the input value at error occurrence.

At this time, the system alarm of channel error is sent for the channels that are shut off.

The output shutoff is activated for dangerous failures, such as DO module channels are stuck in the ON status, and failures where internal module protection is required, such as overcurrent of AO modules. However, the user can define in an I/O parameter whether to activate the output shutoff switch for dangerous failures where module protection is not required by the system.

The user must determine if the failure occurred in the field or in the module, based on the detailed error information that is provided in the Diagnostic Information window and IOM Report error.

Operation at occurrence of output channel errors

Operations and recovery procedures during output channel error occurrence in the universal type I/O module are the same as those for output channel error occurrence in an output module.

SEE ALSO For more information about operations at error occurrence on an individual output channel and recovery procedure, refer to:

G2.2.4, “Actions taken at output channel error occurrence and recovery procedure” on page G2-17

G2.2.6 Actions taken at errors between CPU and Input/ Output module and recovery procedure

Errors between the CPU and input/output module refer to errors on both sides of the SB bus and errors on both sides of the communication module of a node.

The value output from output channels when a system error is detected must be specified in advance as a fail-safe value in an I/O parameter.

SEE ALSO For more information about behavior upon occurrence of an error when using an optical ESB bus repeater, refer to:

G2.2.7, “Actions taken at error occurrence for optical ESB bus repeater devices” on page G2-26

Actions taken at error occurrence

If a node error or bus error occurs, both the CPU and input/output module perform actions taken at error occurrence, respectively.

CPU processing

- The input value at error occurrence is set for input variables corresponding to all the input channels that do not respond.
- The fail-safe value is set for the physical data of output variables corresponding to all the output channels that do not respond, and they are placed in the Output Disable status.
- The input value at error occurrence set for the input variables and the fail-safe value set for the output variables are specified in I/O parameters.
- The CPU stops updating data of the relevant output module.

SEE ALSO For more information about the items to be defined as I/O parameters, refer to:

Appendix 1.3, “Settings for channel items” on page App.1-8

Error notification

- A channel error is notified via a diagnostic information message (alarm class 1). The data status of all the channels is set to BAD.
- When a node encounters an error, a diagnostic information message regarding the node error will be generated. When the node returns to normal, a diagnostic information message (alarm class 1) is notified to indicate recovery from the I/O module error.

Recovery procedure

In order to make an output of an output module recover after handling a hardware failure, it is necessary to perform the output enable operation from SCS Maintenance Support Tool of the SENG.

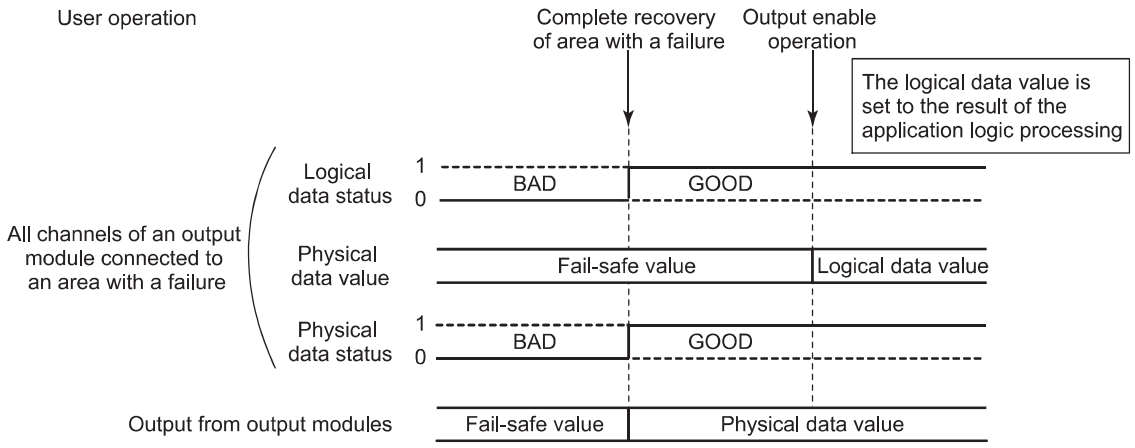


Figure G2.2.6-1 Output module recovery from communication path errors

TIP

Input modules resume using input values from the field and their data status becomes GOOD once the cause of failure is removed.

G2.2.7 Actions taken at error occurrence for optical ESB bus repeater devices

This section explains the actions taken at error occurrence to the following optical ESB bus repeater devices.

Devices for SCS that supports SIL 3

- SNT401/SNT411 and SNT501/SNT511 (Optical ESB bus repeater modules)
- SNT10D (Unit for optical bus repeater module)

Devices for SCS that supports SIL 2

- L1NT401/L1NT411 and L1NT501/L1NT511 (Optical ESB bus repeater modules)
- L1NT10D (Unit for optical bus repeater module)

The model names of devices for SCS that supports SIL 3 are used in the explanation. Model names in brackets indicate devices for SCS that supports SIL 2.

Actions taken at errors of optical ESB bus repeater/fiber-optic cable

The actions to be taken for a failure of optical ESB bus repeater module or abnormality of fiber-optic cable is the same as the actions taken at an ESB bus error.

- In the event of a failure in one of the optical ESB bus repeater modules in a redundant configuration, or disconnection or other abnormality in any fiber-optic cable connecting these modules, a "diagnostic information message indicating the SSB401 (L1SB401) error (Message No. 0065)" is notified as the event of the I/O node connected via the applicable failure location.
  Example:

  0065 SCS0101 SBS Fail FIO NODE 02 SBS RIGHT

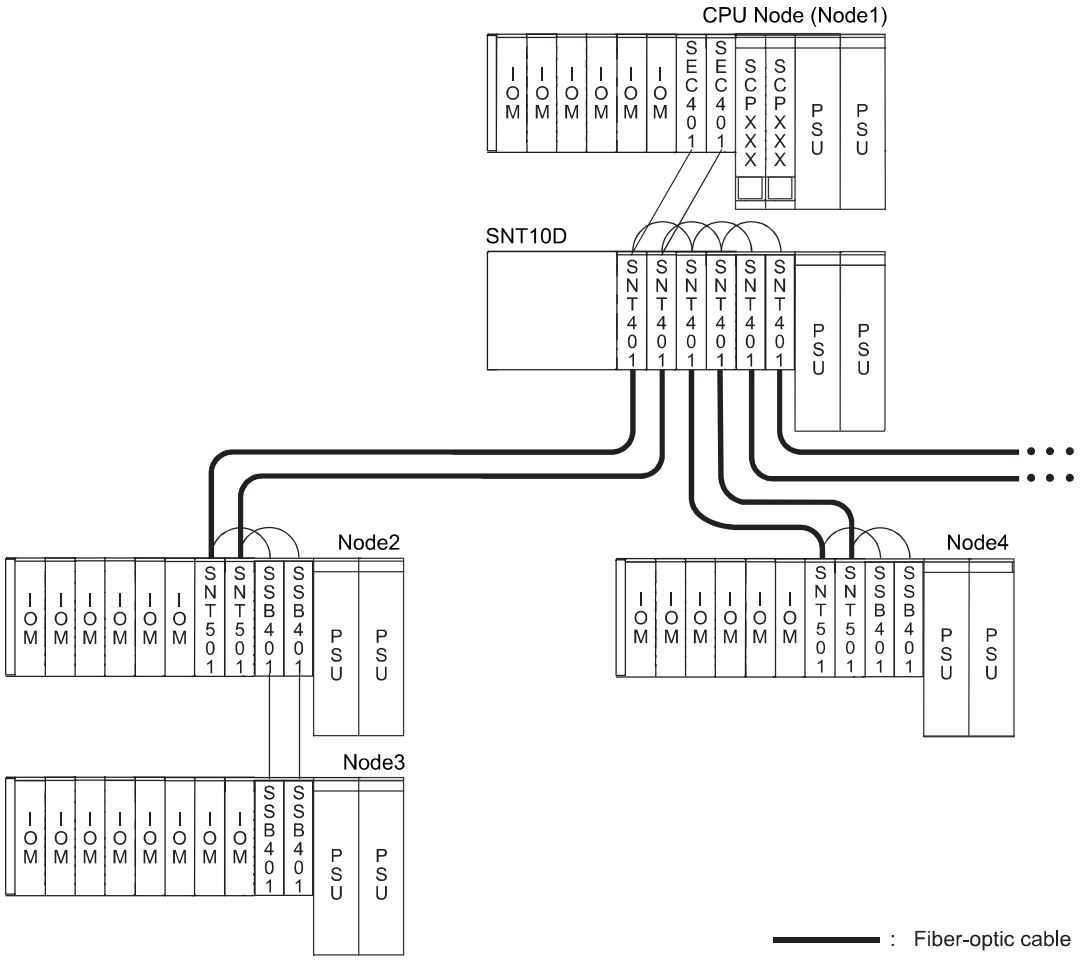


Figure G2.2.7-1 Connection example of devices for SCS that supports SIL 3

The actions taken at errors of optical ESB bus repeater modules is explained using the above figure showing a connection example.

Nodes 2 and 3 are accessed via SNT401 and SNT501 (L1NT401 and L1NT501) modules. Therefore, a failure in the SNT401 or SNT501 (L1NT401 or L1NT501) module that is relaying Node 2 or 3 disables communication with Nodes 2 and 3.

- A diagnostic information message indicating an SSB401 (L1SB401) error (Message No. 0065) is notified for Nodes 2 and 3 in either of the following cases:
  - In the SNT10D (L1NT10D) shown in the figure, one of the SNT401 (L1NT401) modules connecting Nodes 2 and 3 fails.
  - One of the SNT501 (L1NT501) modules installed in Node 2 fails.
- If both of the SNT401 (L1NT401) modules or both of the SNT501 (L1NT501) modules fail, a node error occurs in each I/O node connected via the failed optical ESB bus repeater modules. If both of the SNT501 (L1NT501) modules installed in Node 2 fail, Nodes 2 and 3 connected via the SNT501 (L1NT501) modules generate an error. Similarly if both of the SNT401 (L1NT401) modules installed in the SNT10D (L1NT10D) fail, Nodes 2 and 3 also generate an error.

TIP

A diagnostic information message indicating an ESB bus error (Message No. 0063) is issued only when an error occurs in all I/O nodes excluding the CPU node. In a configuration where optical ESB bus repeater modules are used to provide multiple ESB bus lines, this diagnostic information message (Message No. 0063) is not issued in the event of an error in only one line.
For example, assume a system configuration that partially uses optical ESB bus repeater modules. Even if errors are occurred in bus 1 of all I/O nodes those are connected to the ESB bus but are not connected to fiber-optics, the aforementioned diagnostic information message indicating an ESB bus error (Message No. 0063) is not issued.

The same rule applies when the SEC402 (L1EC402) is used to connect nodes to both the upper and lower sides. For example, the diagnostic information message No. 0063 is not notified if errors occurred in only one side of the duplicated buses of all I/O nodes connected via the upper connector.

Actions taken at errors of node power supply

Installing optical ESB bus repeater modules in a unit for optical bus repeater module

If optical ESB bus repeater modules are installed in SNT10D (L1NT10D), which is a unit for optical bus repeater module, set the hardware setting switch [1] (installation unit setting DIP switch 1) on the optical ESB bus repeater modules to "0: Installation in unit for optical bus repeater module." When the switch is set this way, an error in one of the SNT10D (L1NT10D) power-supply modules will be notified as a failure of the I/O nodes connected via the optical ESB bus repeater modules.

- If an error occurs in one of the power-supply modules of the SNT10D (L1NT10D) in which the optical ESB bus repeater modules are installed, the optical ESB bus repeater modules of the corresponding side stop communicating. If the error occurred in the left power-supply module, the optical ESB bus repeater modules installed in odd-number slots stop communication. If the error occurred in the right power-supply module, the optical ESB bus repeater modules installed in even-number slots stop communication. Communication has stopped from the optical ESB bus repeater module on one side, so "diagnostic information messages indicating the SSB401 (L1SB401) error (Message No. 0065)" for all I/O nodes connected via the applicable optical ESB bus repeater modules are notified.
- In the event of errors in both of the power-supply modules of the SNT10D (L1NT10D) in which the optical ESB bus repeater modules are installed, the errors are notified to all I/O nodes connected via the optical ESB bus repeater modules installed in the applicable SNT10D (L1NT10D).

Installing optical ESB bus repeater modules in a CPU node or I/O node

If optical ESB bus repeater modules are installed in a CPU or I/O node, set hardware setting switch [1] (installation unit setting DIP switch 1) to "1: Installation in node (safety control unit or safety node unit)."

- If SW [1] is set to "1," the optical ESB bus repeater modules will continue to operate without being affected, even if an error occurs in one of the power-supply modules of the node in which the optical ESB bus repeater modules are installed.
- In the event of an error in both of the power supply modules of the node in which the optical ESB bus repeater modules are installed, an error occurs in this node and all I/O nodes connected via the applicable optical ESB bus repeater modules.

IMPORTANT

- When installing optical ESB bus repeater modules in a SNT10D (L1NT10D), set the installation unit setting DIP switch 1 to "0." If this switch is set to "1," a failure of the I/O nodes connected via the optical ESB bus repeater modules is not notified when one of the power-supply modules of the SNT10D (L1NT10D) is in error status.
- When installing optical ESB bus repeater modules in a CPU or I/O node, set the installation unit setting DIP switch 1 to "1." If this switch is set to "0," an error occurring in one of the power-supply modules of the CPU or I/O node will be recognized as an error in the optical ESB bus repeater modules on one side.

G2.2.8 Operations during hardware error occurrence related to N-IO

This section describes the operations when hardware errors related to N-IO occur. It also explains the recovery monitoring operation for the point where the malfunction occurred.

N-ESB bus

- Error detection
  The SCS performs N-ESB bus diagnosis when accessing the I/O module of the N-IO node. If one side of N-ESB bus is faulty, it is considered as minor error. If both the sides of N-ESB buses are faulty, it is considered as major error, and all N-IO nodes that are connected to the corresponding N-ESB bus are considered as errors.
- Recovery monitoring
  The SCS monitors the recovery status of N-ESB bus periodically. When the bus has recovered, the N-ESB bus status in the SCS returns to normal. Then, the SCS switches over both buses alternately while communicating with NIU.

N-IO node

- Error detection
  The SCS monitors the status of N-ESB bus module periodically. If one side of N-ESB bus module is faulty, it is considered as minor error If both the sides of N-ESB bus module are faulty, the corresponding N-IO node and all N-IO nodes under it are considered as major errors. The bus types that connect the subordinate N-IO nodes, irrespective of whether they are N-ESB bus or optical ESB bus, are considered as major errors.

  The following figure shows the effective range of the N-IO node when it is abnormal.

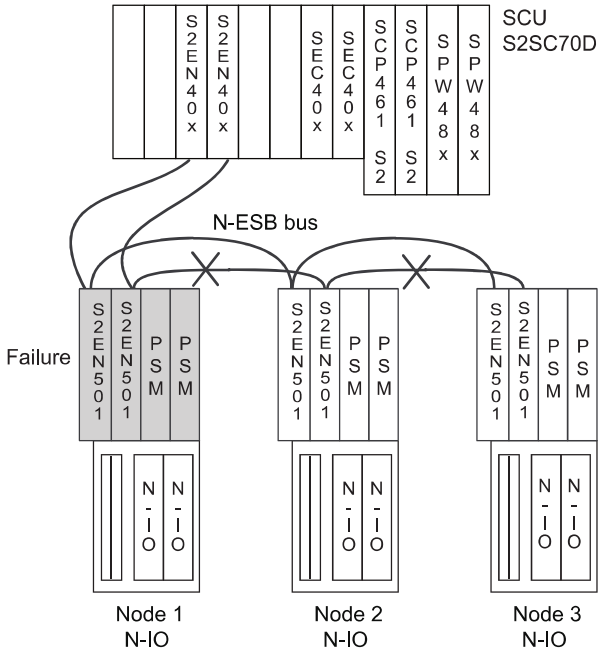


Figure G2.2.8-1 Effective range of the abnormal N-IO node

Node2 and Node3 communicate with the SCS through S2EN501 of Node1. If S2EN501 of Node1 that communicate with the SCS is faulty at both sides or has power failure, the communication to all I/O module of Node 2 and Node 3 is disabled.

- Recovery monitoring
  The SCS periodically monitors the recovery of abnormal N-IO node. When the N-IO node has recovered, the N-IO node status in the SCS returns to normal.

Power supply module of the N-IO node

- Error detection
  The SCS monitors the status of the power supply module of the N-IO node periodically. If the power supply module is faulty at one side, the N-IO node is considered to have a minor error. If the power supply module is faulty at both sides, the N-IO node is considered to have a major error.
- Recovery monitoring
  The SCS monitors the recovery of the power supply module of the abnormal N-IO node periodically. When the module has recovered, the power supply module status in the SCS returns to normal.

F-SB bus

- Error detection
  The SCS performs diagnosis of the F-SB bus between NIU and I/O unit when accessing the I/O module of the N-IO node. If one side of F-SB bus is faulty, it is considered as minor error. If both sides of F-SB bus are faulty, the I/O modules of the corresponding NIU becomes error, and it is considered as a major error.
- Recovery monitoring
  The SCS monitors the recovery status of F-SB bus periodically. When the bus has recovered, the F-SB bus status in the SCS returns to normal. Then, NIU communicates with the I/O module by using both buses simultaneously.

G2.2.9 Operations at fire and gas communication error occurrence and recovery procedure

This section explains the operations upon occurrence of an S2LP131, fire and gas device, or fire and gas communication error and recovery procedure therefor.

The CPU sets the communication data to the value upon error specified by the user and changes the data status to BAD with the timing described below. The timing of status change will vary between data used with safety communication and data used with interference-free functions.

- Data used with safety communication
  The timing at which the Safety Layer of the SCS uses the Safety Measure of PROFIsafe and detects an error
- Data used with interference-free functions
  The timing at which the S2LP131 uses the communication status of PROFINET and detects an error of the communication path

Operations at error occurrence along path between the CPU and S2LP131 and recovery procedure

Errors along the path between the CPU and S2LP131 are errors of the FIO node and errors on both sides of the SB bus and ESB bus from the CPU to the S2LP131. This sections explains the operations at error occurrence and recovery procedures therefor.

Operation at error occurrence

- CPU processing
  The CPU sets values specified in advance as I/O Parameters by the user to all communication data in the range of the error. The user can specify in advance whether to use the value immediately before the error is detected or to use the preset “input value at error occurrence.”
- Error notification
  The CPU notifies a message containing diagnosis information for the FIO node error. In addition, an IOM error and recovery diagnosis message is notified upon recovery. The CPU sets the data status of all communication data in the range of the failure to BAD while the error is occurring.

  In the SCS State Management window of SENG or the Status Display view of HIS, the location of the error is shown in red. This will switch to green upon recovery from the error.

Recovery procedures

Remove the cause of the error. After removing the cause of the error, you do not need to perform output enable operation from SENG.

Operations at S2LP131 error occurrence and recovery procedure

S2LP131 errors are hardware failures, communication board errors, disconnection from the node, and configuration errors.

Operation at error occurrence

- CPU processing
  The CPU sets values specified in advance as I/O Parameters by the user to all communication data obtained via the S2LP131. The user can specify in advance whether to use the value immediately before the error is detected or to use the preset “input value at error occurrence.”

- Error notification
  The CPU notifies a message containing diagnosis information for the IOM error. The CPU sets the data status of all communication data obtained via the S2LP131 to BAD while the error is occurring.

  In the SCS State Management window of SENG or the Status Display view of HIS, the S2LP131 is shown in red. This will switch to green upon recovery from the error.

Recovery procedures

Remove the cause of the error. After removing the cause of the error, you do not need to perform output enable operation from SENG.

Operations at error occurrence along path between the S2LP131 and fire and gas devices and recovery procedure

Errors along path between the S2LP131 and fire and gas devices are S2LP131 port errors, YFGW410 failures, path errors between S2LP131 and YFGW410, and path errors between YFGW410 and GS01.

SEE ALSO For more information about operations at safety communication error occurrence and recovery procedure, refer to:

"■ Operations at error occurrence regarding safety communication between the CPU and fire and gas devices and recovery procedure" on page G2-33

Operation at error occurrence

- CPU processing
  The CPU sets values specified in advance as I/O Parameters by the user to data used with interference-free functions in the range of the error. The user can specify in advance whether to use the value immediately before the error is detected or to use the preset "input value at error occurrence."
- Error notification
  The CPU notifies a message containing diagnosis information indicating a communication error of the S2LP131. The CPU sets the data status of the data used with interference-free functions in the range of the error to BAD while the error is occurring.

  In the SCS node status display dialog box of HIS, "1C" is shown in red. The display will disappear upon recovery from the error.

Recovery procedures

Remove the cause of the error. After removing the cause of the error, you do not need to perform output enable operation from SENG.

Operations at error occurrence regarding safety communication between the CPU and fire and gas devices and recovery procedure

Errors regarding safety communication are CRC errors between the CPU and fire and gas devices and errors such as timeouts.

Operation at error occurrence

- CPU processing
  The CPU sets values specified in advance as I/O Parameters by the user to data used with safety communication in the range of the error. The user can specify in advance whether to use the value immediately before the error is detected or to use the preset "input value at error occurrence."
- Error notification

The CPU notifies a message containing diagnosis information for the fire and gas communication error. The CPU sets the data status of the data used with safety communication of fire and gas devices to BAD while the error is occurring.

In the SCS node status display dialog box of HIS, "1C" is shown in red. The display will disappear upon recovery from the error.

Recovery procedures

Remove the cause of the error. After removing the cause of the error, you do not need to perform output enable operation from SENG.

G2.3 Actions taken at minor error occurrence and recovery procedure

A minor error does not affect the application logic execution function itself. For example, "one-side" failure of a redundant hardware applies to this.

When an error occurs in a device that has been configured for dual redundancy, the control rights get transferred to the device on standby so processing can continue. Such errors are regarded as minor. After switching the control right, the same operation as for single configuration system is performed. The fact that the control right is switched due to a failure is notified via a diagnostic information message. Since the SCS can continue controlling in this case, the data status is not changed nor is any error status notification to system function blocks performed. Confirm that the failed hardware is switched to standby side and then replace the failed hardware.

IMPORTANT

Observe the following precautions when one of the redundant pair of I/O modules has failed and you must fix it:

- If you pull out the failed I/O module, do not insert it again.
- When you replace the I/O module, do not insert an I/O module that is not assured as normal.

If you do not observe these precautions, the field side may be adversely affected if the inserted module is faulty.

SEE ALSO For more information about the procedures for replacing ProSafe-RS devices, refer to:

I1.2, “Maintenance for ProSafe-RS equipment” on page I1-9

H. Monitoring the SCS status

You can monitor the SCS status from the following windows:

- The SCS Status Overview window can be used to view the status of SCSs that are registered in the RS project.
- The State Management window can be used to check the detailed status of the specified SCS.
- The IOM Report can be used to check the detailed status of I/O modules.
- The Diagnostic Information window can be used to check the diagnostic information messages that are generated in SCS.

TIP

- In this manual, the safety control unit and the safety node unit are called as CPU node and FIO node, respectively.
- In this document, I/O shutoff switches and DO shutoff switches of the universal type I/O module and are referred to as an output shutoff switch.

H1. SCS status display

The status of SCS is displayed in the following windows:

- SCS Status Overview window
- SCS State Management window

This section describes how to display and operate these windows.

H1.1 SCS status overview

The SCS Status Overview window displays a list of SCSs assigned to the given RS project. In addition to the current operating conditions of SCSs, it also displays if there is any diagnostic information messages from any of the SCS diagnostic functions; it is easy to know which SCS has errors.

How to display the SCS Status Overview window

The SCS Status Overview window can be launched using the following two methods:

- From the Launcher menu of SCS Manager
- From the [Start] menu of Windows

From the Launcher Menu of SCS Manager

1. Select [Maintenance] from the [Tools] menu of SCS Manager.
   The Maintenance Launcher menu appears.
2. Select [SCS Status Overview] from the Maintenance Launcher menu.
3. Enter your password.
   Password entry is not required when the Access Control and Operation History Management Package is used.

   The SCS Status Overview window is displayed.

From the Start menu of windows

1. Start SCS Status Overview.
2. Enter your password.
   When Windows authentication mode is set, enter a password. When the Access Control and Operation History Management Package is applied, enter the name and password of the engineer.

   The SCS Status Overview window is displayed.

SCS Status Overview window structure

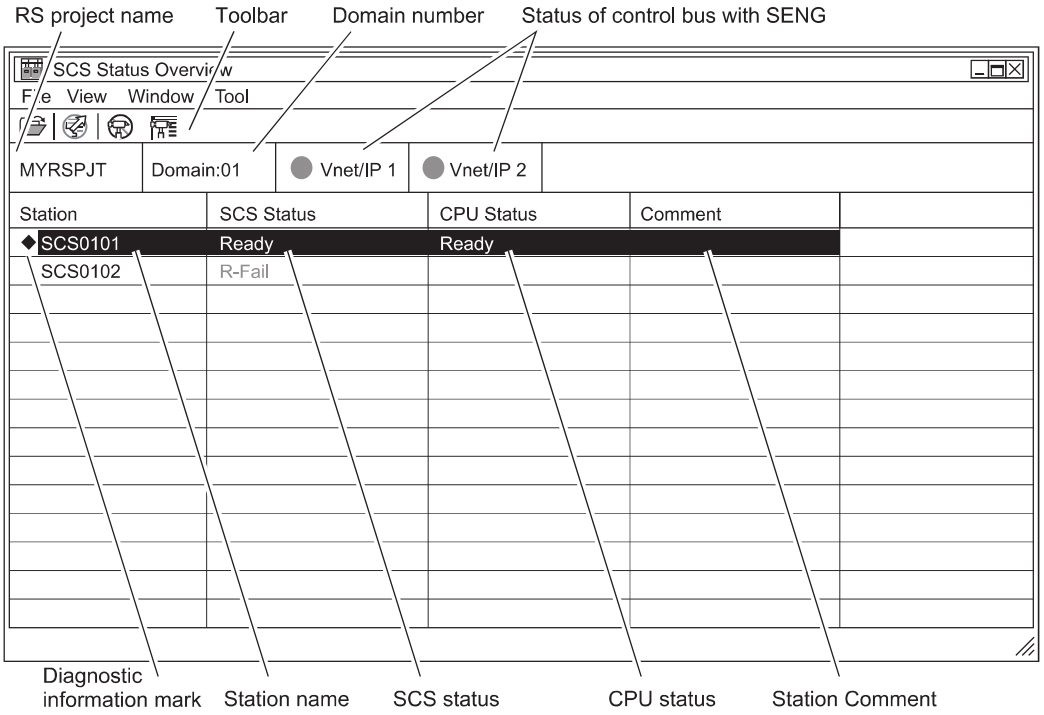


Figure H1.1-1 SCS Status Overview window structure

The components of the window are explained as follows.

Toolbar

The following buttons are provided on the toolbar.

Table H1.1-1 Toolbar buttons

Button	Name	Description
	Open	Call up Project Selection dialog box.
	Diagnostic Information	Call up Diagnostic Information window.
 (*1)	Time Setup	Call up Adjust Time dialog box.
	Setup Tool	Call up Setup Tool.

*1: Not available when using SCS Simulator.

Call up Project Selection dialog box

Click this button to open the Project Selection dialog box, where you can switch between RS projects.

Call up Diagnostic Information window

Click this button to open the Diagnostic Information window related to the SCS selected in the SCS Status Overview window. The Diagnostic Information window allows you to perform confirmation, deletion, printing and saving to file operations on the diagnostic information managed by SCS.

Call up Adjust Time dialog box

The Adjust Time dialog box allows you to set the system date and time. In the case of a CENTUM integration structure, the system time on the CENTUM side is also changed.

But in the following cases, the system time cannot be changed:

- When an SNTP server is connected on the Vnet/IP network and the system time is synchronized with the standard time, the system time cannot be changed from the SENG.
- When a V net router style below S3 is used, the system time of the Vnet/IP network cannot be changed from the SENG in the V net domain.

SEE ALSO For more information about time setting, refer to:

I3., “Setting system time” on page I3-1

Call up Setup Tool

Setup Tool allows you to customize the operating environment of SCS Maintenance Support Tool.

SEE ALSO For more information about setup tool, refer to:

A6.3, “Customization of the SCS Maintenance Support Tool window” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

System status list view

This view shows a list of operation information of SCSs (whole status and CPU status) in a RS project. The operating status of the control bus connected from the SENG is displayed in the upper part of the list view.

Diagnostic information marks are displayed to the left of SCS names for which diagnostic information messages have been generated. If any of the diagnostic information messages is not acknowledged, the diagnostic information marks flash.

If you double-click a line of an SCS in the Station name column, the SCS State Management window for the corresponding SCS opens.

Table H1.1-2 Items displayed in System status list view

Item	Description
RS Project name	RS project name
Domain number	Domain number to which the local SENG belongs
V net or Vnet/IP status	Status of the control bus to which the local SENG is connected
Diagnostic information mark	Presence of diagnostic information messages and their acknowledgement status
Station name	Station name of an SCS
SCS status	Status of an SCS
CPU status	Status of the SCS’ CPU
Station comment	SCS station comments

Control bus status

Indicates the name and status of the control bus on which the SENG is connected.

Table H1.1-3 Display of V net or Vnet/IP status

Status	Display	Display color
Normal	●	Green
Error	×	Red

Diagnostic information mark

These are used to indicate whether there are any diagnostic information messages, and their acknowledgement status.

Table H1.1-4 Display of diagnostic information marks

Status	Display	Display color
Indicates that the diagnostic information messages exist. Flashes if unacknowledged messages exist.	◆	Red
Indicates that all messages are acknowledged and errors exist in nodes or input/output modules.	◇	Red
Indicates that all messages are acknowledged and deleted, and no error exists in nodes or input/output modules.	(No display)	

SCS status

Indicates the status of entire SCS.

Table H1.1-5 Display of SCS status

Status	Display	Display color
Normal	Ready	
Copying	Copy	Blue
Communication Error	Communication Error (*1)	Red
SCS Simulator is running	Test	

*1: "Communication Error" is displayed when SCS stops. It indicates that the connection for communication is not established.

CPU status

Indicates status of SCS CPU.

Table H1.1-6 Display of CPU status

Status	Display	Display color
Normal. CPUs on both sides are normal in the case of duplex configuration.	Ready	
Abnormal. CPUs on both sides are abnormal in the case of duplex configuration.	Fail	Red
CPU on the right side is abnormal in the case of duplex configuration	R-Fail	Red
CPU on the left side is abnormal in the case of duplex configuration	L-Fail	Red

H1.2 SCS State Management window

The SCS State Management window displays detailed information about the operating status of CPU modules and input/output modules for a single SCS. If there is an error, the erroneous area is shown using a different color. It also displays whether or not there are any messages that have not been acknowledged.

The SCS State Management window allows you to perform the following operations:

- IOM Download operation, Output Enable Operation and Start Output Module operation
- Display of detailed information of each input/output module

How to display the SCS State Management window

The SCS State Management window can be launched using the following two methods:

- From the Launcher menu of SCS Manager
- From the SCS Status Overview window

From the Launcher menu of SCS Manager

1. From the menu bar of SCS Manager, select [Tools] > [Maintenance].
   The Maintenance Launcher menu appears.
2. Select [SCS State Management] from the Maintenance Launcher menu.
3. Enter your password.
   Password entry is not required when the Access Control and Operation History Management Package is used.

   The SCS State Management Window is displayed.

SEE ALSO For more information about security-related operations of the SCS Maintenance Support Tool, refer to:

B5., “Security of SCS Maintenance Support tool” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

From the SCS Status Overview window

Double-click the station name of an SCS in the SCS Status Overview window. The SCS State Management window for that SCS appears.

SCS State Management window structure

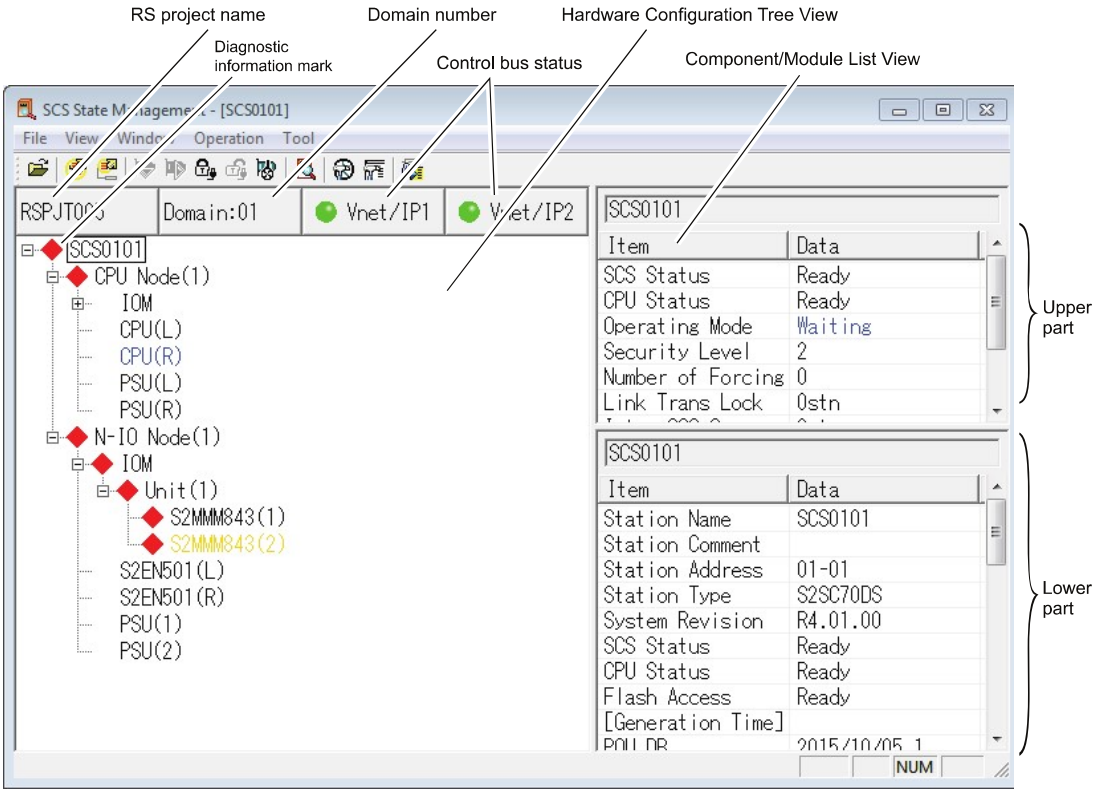


Figure H1.2-1 SCS State Management window structure

TIP

- For SCS that supports SIL 3, SEC402, SEC401, SNT401, SNT501, SNT411, SNT511, and SNT10D are not displayed.
- For SCS that supports SIL 2, L1EC402, L1EC401, L1NT401, L1NT501, L1NT411, L1NT511, and L1NT10D are not displayed.

The components in the window are explained as follows.

Toolbar

The following buttons are provided on the toolbar.

Table H1.2-1 Toolbar buttons

Button	Name	Description
	Open	Call up Project Selection dialog box.
	Diagnostic Information	Call up Diagnostic Information window.
	Common Diagnostic Information	Call up Diagnostic Information window (common).
 (*1)	IOM Load	Call up IOM Download tool
 (*1)	Start output module	Output Module Start

Continues on the next page

Table H1.2-1 Toolbar buttons (Table continued)

Button	Name	Description
 (*1)	Disable Maintenance port	Call up the NIU maintenance port setting tool. To disable the port.
 (*1)	Enable Maintenance port	Call up the NIU maintenance port setting tool. To enable the port.
	I/O Channel Status	Call up I/O Channel Status dialog box.
 (*1)	System Report	Call up System Report dialog box.
 (*1)	Time Setup	Call up Adjust Time dialog box.
	Setup Tool	Call up Setup Tool.
	SCS Status Overview	Call up SCS Status Overview window.

*1: Not available when using SCS Simulator.

Call up Project Selection dialog box

Click this button to open the Project Selection dialog box, where you can switch between RS projects.

Call up Diagnostic Information window

Click the following buttons to open the Diagnostic Information window. The icon on the button changes if there are diagnostic information messages.

- [Diagnostic Information] Button
  This button calls up all diagnostic information messages from the hierarchy tree selected in Hardware Configuration Tree View, to be displayed in the Diagnostic Information window. For example, if you click this button when selecting a node, all diagnostic information messages common to this node and those for all input/output modules for the node and nodes below it are displayed together.
- [Common Diagnostic Information] Button
  This button calls up only diagnostic information messages for the tree selected in Hardware Configuration Tree View to be displayed. For example, if you click this button when selecting a node, only diagnostic information messages common to this node will be displayed in the Diagnostic Information window.

  The [Common Diagnostic Information] button can be used when a station or a node is selected on Hardware Configuration Tree View.

The Diagnostic Information window allows you to perform acknowledgement, deletion, printing and saving to file operations on diagnostic information managed by the SCS.

SEE ALSO For more information about Diagnostic information window, refer to:

H5.2, “Diagnostic Information window” on page H5-3

Call up IOM Download tool

The IOM Download tool is used to recover when input/output modules are replaced or input/output modules fail.

If the user does not have the authority to write, the [IOM Load] button is grayed out and disabled.

SEE ALSO For more information about IOM download tool, refer to:

I4.6, “IOM Download tool” on page I4-80

Output module start

If an error serious enough to activate the Output Shutoff switch occurs, there is a case where the output module stops its output and waits for the Output Module Start depending on an error cause. Perform the Start Output Module operation to start the output modules whose output is stopped. Note that even if you restart the output module, the output of all channels of the output module remain disabled. In order to output the result of application logic from the output module on the control side, perform the Output Enable Operation as well.

If the user does not have the authority to write, the [Start output module] button is grayed out and disabled.

SEE ALSO For more information about starting output module and the Output enable operation, refer to:

C8., “Output enable operation” on page C8-1

Call up I/O Channel Status dialog box

The I/O Channel Status dialog box displays the statuses of the channels of all input/output modules of the SCS in list format. This dialog box also allows you to enable the output of channels whose output are disabled (Output Enable Operation).

SEE ALSO For more information about Output enable operation, refer to:

C8., “Output enable operation” on page C8-1

For more information about I/O channel status, refer to:

H4., “Displaying I/O channel status” on page H4-1

Call up NIU maintenance port setting tool

The NIU maintenance port setting tool is called to enable or disable the NIU maintenance port. It can be called after selecting the following components in Hardware Configuration Tree View. You can also called it from menu bar.

Table H1.2-2 Setting method to enable or disable the NIU maintenance port

Objective	How to start the tool
Disable the maintenance port of all the nodes of each station collectively.	Select the station from Hardware Configuration Tree View, and then select [Operation] > [Disable Maintenance port]. Or, click the [Disable Maintenance port] button on the tool bar.
Disable the maintenance ports on a per node basis	Select the N-IO node from Hardware Configuration Tree View, and then select [Operation] > [Disable Maintenance port]. Or, click the [Disable Maintenance port] button on the tool bar.
Enable the maintenance ports on a per node basis	Select the N-IO node from Hardware Configuration Tree View, and then select [Operation] > [Enable Maintenance port]. Or, click the [Enable Maintenance port] button on the tool bar.

Call up System Report dialog box

The SCS Report dialog box displays the status of the displayed SCS as character strings. IOM Report dialog box also displays the status of the displayed input/output modules. This function allows printing reports and save them in files in text format.

SEE ALSO For more information about system reports, refer to:

H2., “System reports” on page H2-1

Call up Adjust Time dialog box

Click this button to open the Adjust Time dialog box.

SEE ALSO For more information about time setting, refer to:

I3., “Setting system time” on page I3-1

Call up Setup Tool

Setup Tool allows you to customize the operating environment of SCS Maintenance Support Tool.

SEE ALSO For more information about setup tool, refer to:

A6.3, “Customization of the SCS Maintenance Support Tool window” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

Call up SCS Status Overview window

Click this button to return to the SCS Status Overview window.

Hardware Configuration tree view

This view displays the hardware configuration of a single SCS in tree format. The upper part of the tree view shows the status of the control buses connected to the SCS.

The CPU node displays the CPU module, power supply module and I/O module. The I/O module of the CPU node also includes the N-ESB bus coupler module. The FIO node displays the power supply module and the I/O module. The N-IO node displays the power supply module, I/O module and N-ESB bus module. If there is any diagnostic information message for any hardware components displayed in tree format, a diagnostic information mark is displayed at the left of each component. Since diagnostic information marks are displayed on the alarm layer, if an error is detected in an I/O module, a diagnostic information mark will also appear in the I/O node and SCS of the upper components. In this way, the user can simply display the upper components to check whether any lower diagnostic information messages exist in the alarm layer. If an error is detected in the upper component, the lower components show the status that is obtained before the error has occurred in the upper component.

In the case of dual redundant input/output modules, diagnostic information messages for both sides are displayed regardless of which input/output module you select.

If there are any diagnostic information messages that have not been acknowledged, the diagnostic information mark flashes.

Double-click the name of component or input/output module to display detailed information of the selected item in Component/Module List View.

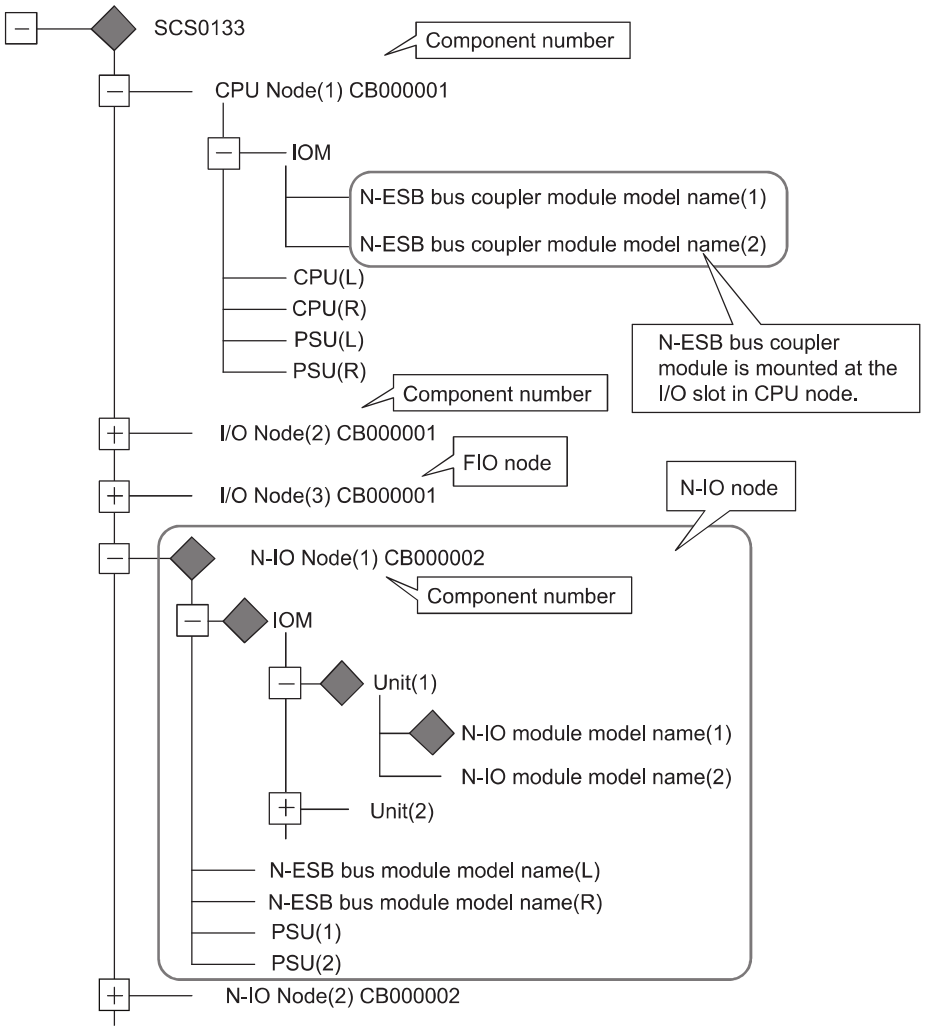


Figure H1.2-2 Hardware Configuration tree view

Table H1.2-3 Items displayed in Hardware Component tree view

Display items	Description
RS Project name	RS project name
Domain number	Domain number to which the SCS belongs
V net or Vnet/IP Status	Status of the control bus to which the SCS is connected
Diagnostic information mark	Presence of diagnostic information messages and their acknowledgement status
Component name or module name	Node or I/O module names (*1)

*1: If ALR111M is set when the I/O module is defined, ALR111 is displayed in the SCS State Management window. Similarly ALR121 is displayed for ALR121M and ALE111 is displayed for ALE111M.

Control bus status

It displays the status of the control bus where the SCS is connected. The following table shows the relationship between the status, display, and display colors of the control bus.

Table H1.2-4 Display of V net or Vnet/IP status

Status	Display	Display color
Normal	●	Green
Error	×	Red

Diagnostic information mark

The relationship between the status, display, and the display colors of the diagnostic information mark is shown in the following table.

Table H1.2-5 Display of Diagnostic information mark

Status	Display	Display color
Indicates that diagnostic information messages exist. Flashes if unacknowledged messages exist.	◆	Red
Indicates that all messages are acknowledged and errors exist in nodes or input/output modules.	◇	Red
Indicates that all messages are acknowledged and deleted, and no error exists in nodes or input/output modules.	(No display)	

Component name or module name

The relationship between component name or module name and the display colors is shown in the following table.

Table H1.2-6 Display of component name or module name status

Status	Display color	Remark
Normal		When using SCS Simulator, the components and modules are displayed as Normal even though they are not physically installed.
Error	Red	
Standby	Yellow	
Hardware ready	Blue	This status indicates that an APC is being executed in the case of CPU module, and information is being copied from the control side to the standby side.
Copying	Blue	This status indicates that information is being copied from the control side to the standby side in the case of SCS.
Waiting for startup	Blue	In the case of output module, this status indicates that the output module is waiting for startup.

Component names or module names are displayed with one of the following characters attached to the right of the name.

Table H1.2-7 Characters attached to the component name and module name

Component name, module name.	Displayed characters	Attached character
CPU node	CPU Node	Node number (1)
FIO node	I/O Node	Node number (2) to (14)
N-IO node	N-IO Node	Node number (1) to (32)
Component Number		Set component number
CPU module	CPU	(L) or (R) for the CPU node. Automatically attached after the redundancy is determined from the SCS station model.
Power supply module	PSU	(L) or (R) for the CPU node and FIO nodes (1) or (2) for N-IO nodes
Unit	Unit	Unit number (1) to (6) for N-IO nodes

Continues on the next page

Table H1.2-7 Characters attached to the component name and module name (Table continued)

Component name, module name.	Displayed characters	Attached character
Input/output module		For the CPU node and FIO nodes, the module model and slot number (1) to (8) are attached under IOM. For N-IO nodes, the module model and (1) to (2) are attached under Unit.
ESB bus module		For the CPU node and FIO nodes, the module model and control bus number (1) or (2) are attached.
N-ESB bus coupler module		For the CPU node, the module model and control bus number (1) or (2) are attached.
N-ESB bus module		For N-IO nodes, the module model and (L) or (R) are attached.

Upper part of Component/Module list view

The following items are always displayed in the upper part of the list view.

- SCS Status
- CPU Status
- Operating mode
- SCS security level
- Number of variables locked by the forcing function
- Number of stations locked in the SCS Link Transmission
- Subsystem Communication Data Locking/Unlocking
- Number of locked stations in the inter-SCS safety communication
- Number of safety subsystem communication I/O locks (only for S2SC70)
- Status of the NIU maintenance port (only for S2SCS70)

Lower part of Component/Module list view

The lower part of the list view displays detailed information about the operating status of the component or module selected by double-clicking in Hardware Configuration Tree View.

Content enclosed in [ ] indicates an index.

The display for each item varies depending on the component or input/output module selected in Hardware Configuration Tree View.

Lower part of list view when a station is selected

The following table shows the contents that are displayed in the lower part of the list view when a station is selected.

Table H1.2-8 Status display (When a station is selected)

Item	Description
Station name	Station name of the SCS
Station comment	Station comments for the SCS
Station Address	Shown in the form of "Domain number-Station number".
Station Type	SCS station type
System Revision	Release number of the system program loaded on the SCS

Continues on the next page

Table H1.2-8 Status display (When a station is selected) (Table continued)

Item	Description
SCS Status	Status of SCS
CPU Status	Status of CPU of the SCS
Flash Access	[Ready] is displayed while in the normal state, and [Writing] (blue) is displayed if the flash memory is being written.
Generation Date/Time	Date and Time when the POU DB, Variable DB, System DB and Integration DB were created.
Application time (*1) (*2)	Actual scan period (msec), set scan period (msec), and program execution time (%)
CPU Idle Time (*1)	Idle time (sec)
Communication Load (*1)	Average value (%) and current value (%)
Control Status	Displayed as [Run] when running and as [Stop] (red) when stopped.
Operating Mode	The operating mode of SCS is displayed in the corresponding color.
Security Level	Displays the security level of SCS. The security level is displayed in blue for Levels 1 and 0.
Number of Forcing	Displays the number of variables that have been locked using the forcing function. The number is displayed in blue if one or more locked variables exists.
Number of stations locked in the SCS Link Transmission	Displays the number of stations being locked in the SCS Link Transmission. The number and [Stn] are displayed in blue if there is one or more locked stations.
Number of locked stations in the inter-SCS safety communication	Displays the number of stations that are locked in the inter-SCS safety communication. The number and "Stn" are displayed in blue if locked stations exist.
Lock of subsystem communication data	[YES](blue) is displayed if the subsystem communication data are locked and [No] is displayed if the subsystem communication data are not locked. If the SCS does not have any communication module, [No] is displayed.
Number of safety subsystem communication I/O locks (*3)	Displays the number of communication definitions locked with safety subsystem communication. The number is displayed in blue if one or more locked communication definitions exist.
Status of the NIU maintenance port (*3)	When NIU maintenance port is enabled, "Enable" is displayed in red; when it is disabled, "Disable" is displayed.

*1: When SCS Simulator is running, the program execution time is displayed as 100, and CPU idle time and communication load are displayed as 0.
*2: In the case of SCS with R2.02 or earlier system program, actual scan period is not displayed. The set scan period is displayed in the position of actual scan period.
*3: Displayed only for S2SCS70.

- SCS Status

Table H1.2-9 Display of station status

Status	Display	Display color
Normal	Ready	
Copying	Copy	Blue
Communication Error (*1)	Communication Error	Red
SCS Simulator is running	Test	

*1: "Communication error" is also displayed when SCS is stopped.

- CPU Status

Table H1.2-10 Display of CPU status

Status	Display	Display color
Normal. CPUs on both sides are normal in the case of duplex configuration.	Ready	
Abnormal. CPUs on both sides are abnormal in the case of duplex configuration.	Fail	Red
CPU on the right side is abnormal in the case of duplex configuration	R-Fail	Red
CPU on the left side is abnormal in the case of duplex configuration	L-Fail	Red

- Operating Mode

Table H1.2-11 Display of Operating mode

Status	Display	Display color
Stop status (*1)	Stop	Red
Offline Downloading (*1)	Loading	Red
Initialized status	Initial	Red
Waiting for output enable request	Waiting	Blue
Operating	Running	

*1: Normally, these states are not displayed.

Lower part of list view when a CPU node is selected

The following table describes the contents that are displayed in the lower part of the list view when the CPU node is selected.

Table H1.2-12 Status display (when a CPU node is selected)

Item	Description
Node Number	Displays the node number 1.
Component Number (*1)	Displays the component number.
Node Comment	Displays comments for the node.
Node Status	[Ready] is displayed when the status is normal, [Fail] (red) is displayed if the status is abnormal, and [Communication Error] (red) is displayed if the communication status is abnormal.
IRIG-B Status	Displayed only when IRIG-B time synchronization is applied. [Ready] is displayed when the status is normal and [Fail] (red) is displayed if the status is abnormal.
Time Sync	Indicates the time synchronization status. [Vnet/IP] is shown if not synchronized with the time on the SNTP server; [SNTP] is shown if synchronized.
Intake Air Temperature	[Ready] is displayed when the status is normal and [Fail] (red) is displayed if the status is abnormal.
Exhaust Air Temperature	
Battery Temperature	
SCU Fan (*2)	
Battery Status	
Operation data reset switch(*3) (*4)	Displays the status of operation data reset switch. [Hold] is displayed when it is set to maintain NVARM at power recovery and [Reset] (red) is displayed when it is set to clear it.
ESB Bus Status (*5)	[Ready] is displayed when the status is normal and [Fail] (red) is displayed if the status is abnormal.

*1: Displayed for S2SC70 or L1SC70.
*2: Not available if the model of SCS does not have a fan.
*3: Operation data reset switch item is displayed for SSC60 or S2SC70. If S2CP471 is installed in SSC60 or S2SC70, setting status of Operation data reset switch appears. If other than S2CP471 is installed, "Hold" is always displayed.
*4: Displayed for L1SC70.
*5: Not displayed for SCS with CPU node only or for S2SC70/L1SC70.

TIP

The status of Operation data reset switch can be checked by SCS State Management Window, LED on the CPU module, SYS_DIAG function block, or the SCS Station Status Display view on the HIS.

Lower part of the list view when the CPU module of the CPU node is selected

The following table shows the contents that are displayed in the lower part of the list view when the CPU module of the CPU node is selected.

Table H1.2-13 Status display (When a CPU module is selected)

Item	Status	Display	Display color
CPU Status	Normal	Ready	
	Error	Fail	Red
	Standby	Stand-By	Yellow
	Hardware ready	Hard Ready	Blue
	Communication Error	Communication Error	Red
Bus Status	Normal	Ready	
	Error	Fail	Red

Lower part of list view when a CPU node power supply module is selected

The following table shows the contents that are displayed in the lower part of the list view when the power supply module of the CPU node is selected.

Table H1.2-14 Contents of the status display (when PSU is selected)

Item	Status	Display	Display color
PSU Status	Normal	Ready	
	Error	Fail	Red
	Communication Error	Communication Error	Red
24 V DC Power Supply Status	Normal	Ready	
	Error	Fail	Red

Lower part of the list view when the N-ESB bus coupler module of the CPU node is selected

The following table shows the contents that are displayed in the lower part of the list view when the N-ESB bus coupler module of the CPU node is selected.

Table H1.2-15 Contents of the status display (when the N-ESB bus coupler module of the CPU node is selected)

Item	Status	Display	Display color
I/O module model		Input module model	

Continues on the next page

Table H1.2-15 Contents of the status display (when the N-ESB bus coupler module of the CPU node is selected) (Table continued)

Item	Status	Display	Display color
I/O module status	Normal	Ready	
	Error	Fail	Red
	Transmission error	Communication Error	Red
Bus status	Normal	Ready	
	Error	Fail	Red

Lower part of the list view when the representative I/O module of the CPU node is selected

In the CPU node, the status of the I/O module or N-ESB bus coupler module can be displayed in the representative I/O module. The following table shows the contents that are displayed in the lower part of the list view when the representative I/O module with N-ESB bus coupler module installed is selected in the CPU node.

Table H1.2-16 Contents of the status display (when the representative IOM of the CPU node is selected: N-ESB bus coupler module)

Item	Status	Display	Display color
Representative I/O module status	Normal	Ready	
	Error	I/O Fail	Red
	Transmission error	Communication Error	Red
Representative channel status	Normal	Ready	

Lower part of the list view when an FIO node is selected

The following table shows the contents that are displayed in the lower part of the list view when an FIO node is selected.

Table H1.2-17 Status display (when an I/O node is selected)

Item	Description
Node Number	Displays the node number.
Component Number	Displays the component number. (*1)
Node Comment	Displays comments for the node.
Node Status	Displays either normal or abnormal.

*1: When an FIO node is selected in S2SC70 or when it is L1SC70

- Node status

Table H1.2-18 Display of Node status

Status	Display	Display color
Normal	Ready	
Error	Fail	Red
Communication Error	Communication Error	Red

Lower part of the list view when the ESB bus interface module of an FIO node is selected

The following table shows the contents that are displayed in the lower part of the list view when the ESB bus interface module of an FIO node is selected.

Table H1.2-19 Status display (when an I/O node ESB bus interface module is selected)

Item	Status	Display	Display color
ESB-S Status	Normal	Ready	
	Error	Fail	Red
	Communication Error	Communication Error	Red

Lower part of the list view when the power supply module of an FIO node is selected

The following table shows the contents that are displayed in the lower part of the list view when the power supply module of an FIO node is selected.

Table H1.2-20 Status display (when an I/O node power supply module is selected)

Item	Status	Display	Display color
PSU Status	Normal	Ready	
	Error	Fail	Red
	Communication Error	Communication Error	Red
24 V DC Power Supply Status	Normal	Ready	
	Error	Fail	Red

Lower part of the list view when an N-IO node is selected

The following table shows the contents that are displayed in the lower part of the list view when an N-IO node is selected.

Table H1.2-21 Content of the status display (when an N-IO node is selected)

Item	Status	Display	Display color
Node number		Node number	
Component number		Component number	
Node comment		Node comment	
Node status	Normal	Ready	
	Error	Fail	Red
	During maintenance	Maintenance	Blue
	Transmission error	Communication Error	Red
NIU maintenance port status	Enable	Enable	Red
	Disable	Disable	
External alarm input	Normal	Ready	
	Error	Fail	Red
	Diagnosis by external alarm input is disabled	Blank	
Temperature status	Normal	Ready	
	Error	HI, LO	Red

Lower part of the list view when the N-ESB bus module of an N-IO node is selected

The following table shows the contents that are displayed in the lower part of the list view when the N-ESB bus module of the N-IO node is selected.

Table H1.2-22 Contents of the status display (when the N-ESB bus module of an N-IO node is selected)

Item	Status	Display	Display color
N-ESB-S status	Normal	Ready	
	Error	Fail	Red
	During maintenance	Maintenance	Blue
	Error due to maintenance of one module	Fail (Due to maintenance of one module)	Red
	Transmission error	Communication Error	Red
NIU maintenance port status	Enable	Enable	Red
	Disable	Disable	

Lower part of the list view when the power supply module of an N-IO node is selected

The following table shows the contents that are displayed in the lower part of the list view when the power supply module of an N-IO node is selected.

Table H1.2-23 Contents of the status display (when PSU of an N-IO node is selected)

Item	Status	Display	Display color
PSU status	Normal	Ready	
	Error	Fail	Red
	Transmission error	Communication Error	Red
Detail	Normal (*1)		
	PSU stopped supplying power	Power Off	Red
	PSU output over voltage	Overvoltage	Red

*1: The PSU is normal, or not in the power off or over voltage status.

Lower part of the list view when a unit of an N-IO node is selected

The following table shows the contents that are displayed in the lower part of the list view when a unit of an N-IO node is selected.

Table H1.2-24 Contents of the status display (when a unit of an N-IO node is selected)

Item	Status	Display	Display color
Unit number		Unit number	
Bus status	Normal	Ready	
	Error	Fail	Red
	Communication error	Communication Error	Red

Lower part of list view when the representative Input/Output module is selected

I/O module of each node can be grouped, and the group status can be displayed in the list view as a representative I/O module. Individual I/O modules are displayed under the representative I/O module in tree format.

Table H1.2-25 Contents of the status display (when the representative IOM of a node is selected)

Item	Status	Display	Display color
Representative Input/Output Module Status	Normal	Ready	
	Error	I/O Fail	Red
	Communication Error	Communication Error	Red
Status of Representative Channel	Normal	Ready	
	Error	Channel Fail	Red

Lower part of the list view when an individual I/O module of the CPU node or an FIO node is selected

The following table shows the contents that are displayed in the lower part of the list view when an individual I/O module of the CPU node or an FIO node is selected.

Table H1.2-26 Contents of the status display (when an individual I/O module of the CPU node or an FIO node is selected)

Item	Status	Display	Display color
Input/Output Module Type		I/O module model (*1)	
Input/Output Module Status	Normal	Ready	
	Waiting	Stand-by	Yellow
	Error	Fail	Red
	Waiting for startup	Waiting	Blue
	Communication Error	Communication Error	Red
Bus Status	For each bus, [Ready] is displayed when the status is normal and [Fail] (red) is displayed if the status is abnormal.		
Port status (*2)	Normal	Ready	
	Error (*3)	Error	Red
Channel Status	Normal	Ready	
	IOP+ (*4)	IOP+	Red
	IOP- (*4)	IOP-	Red
	Transmitter failure+ (*5)	TRNS+	Red
	Transmitter failure- (*5)	TRNS-	Red
	Analog input error	OvrRange	Red
	Error	Ch Fail	Red

*1: If ALR111M is set when the I/O module is defined, ALR111 is displayed in the SCS State Management window. Similarly ALR121 is displayed for ALR121M and ALE111 is displayed for ALE111M.
*2: Displayed only when a communication module used for communicating with a subsystem is selected.
*3: With S2LP131, an error is a state where either one or both of a safety subsystem communication path error (SS-SCPATH) and a safety subsystem communication error (SS-SCOM) are occurring.
*4: This is only if an analog input module is used.
*5: Displayed only when an analog input module other than the one for TC/RTD is selected.

Lower part of the list view when an individual I/O module of an N-IO node is selected

The following table shows the contents that are displayed in the lower part of the list view when an individual I/O module of an N-IO node is selected.

Table H1.2-27 Contents of the status display (when an individual I/O module of an N-IO node is selected)

Item	Status	Display	Display color
I/O module model		I/O module model	
I/O module status	Normal	Ready	
	Standby	Standby	Yellow
	Error	Fail	Red
	Transmission error	Communication Error	Red
Bus status	Normal	Ready	
	Error	Fail	Red
Channel status (*1)	Normal	Ready	Red
	IOP+ (*2)	IOP+	Red
	IOP- (*2)	IOP-	Red
	Transmitter failure+ (*2)	TRNS+	Red
	Transmitter failure- (*2)	TRNS-	Red
	Analog input error (*2)	OvrRange	Red
	Barrier missing (*3)	IS Barrier Disconnected	Red
	Barrier connection error (*3)	IS Barrier Configuration Error	Red
	I/O open circuit error (*4)	Open Circuit	Red
	I/O short circuit error (*5)	Short Circuit	Red
	Field failure	Field Side Error	Red
	Error	Ch Fail	Red
Channel signal type	Not used	Blank	
	Current input	(IN) Current	
		(IN) Current - IS (*3)	
	Current input (HART)	(IN) Current - HART	
		(IN) Current - HART - IS (*3)	
	Status input	(IN) Status	
		(IN) Status - IS (*3)	
	Current output	(OUT) Current	
		(OUT) Current - IS (*3)	
	Current output (HART)	(OUT) Current - HART	
		(OUT) Current - HART - IS (*3)	
	Status output	(OUT) Status	
		(OUT) Status - IS (*3)	
	1.3 A status output	(OUT) Status 1.3A*	
		(OUT) Status 1.3A* - IS (*3)	
	2.0 A status output	(OUT) Status 2.0A*	
		(OUT) Status 2.0A* - IS (*3)	

*1: Does not display the status of those channels where an I/O variable are not allocated.
*2: Displayed only if an analog input module is selected.

*3: Displayed only when the intrinsic safety barrier is used.
*4: Displayed only when open circuit detection is set.
*5: Displayed only when "Detect Short Circuit" is set.

H2. System reports

System report includes SCS Report window and IOM Report window in the SCS State Management Window. The above two windows can be used for displaying SCS status and input/output module status respectively. When abnormality occurs, the details displayed on these windows can help analyzing the causes of problems. The reports can be printed out or saved into text files.

SCS Report

SCS Report displays the SCS status.
Select a device item other than the input/output modules in Hardware Configuration Tree View of the SCS State Management window, and then click [System Report] button on the toolbar. The SCS Report dialog box will be displayed.

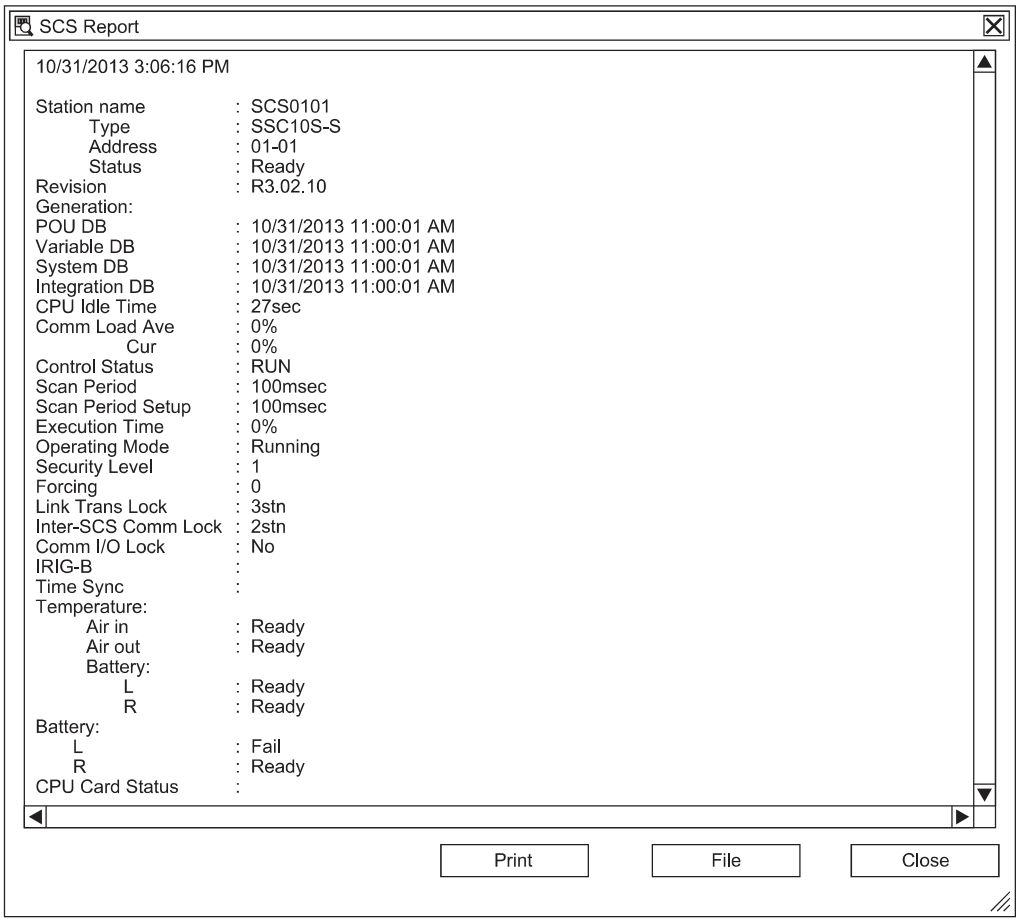


Figure H2-1 SCS Report dialog box

Display example of the SCS report of the system that has a combination of FIO and N-IO

In the SCS report of the system that has a combination of FIO and N-IO, the node status is displayed in the following order: CPU node, FIO node, and N-IO node.

```
**********
FIO Node Status:                          * Discrimination from N-IO node
  Line No.          :
  Node No.          :
  Comment           :
  Component No. :0001                     * Component number
  Com Status (L)  :Ready / Fail
               (R)  :Ready / Fail
  PSU Status (L)  :Ready / Fail
               (R)  :Ready / Fail
  I/O Unit          :Ready / Fail
  Slot No. Type    Status Bus1 Bus2 Port1 Port2 Port3 Port4 Channel
   1      XXXXXX Ready / Fail                          ("XXXXXX" is an IOM model name.)
   2      XXXXXX Ready / Fail
**********

**********
N-IO Node Status:                                      * Discrimination from the existing FIO node
  Node No.          :
  Comment           :
  Component No. :0001                   * Component number
  NIU Status (L)   :Ready / Fail / Fail (Only one module is under maintenance) / Maintenance
               (R)  :Ready / Fail / Fail (Only one module is under maintenance) / Maintenance
  Maintenance Port (L)  :Enabled / Disabled              * NIU maintenance port L/R enable/disable
                       (R)  :Enabled / Disabled
  PSU Status 1    :Ready / Fail         * PSU Status 1/2
               2    :Ready / Fail
  I/O Unit          :Ready / Fail
  Diagnosis         :       * The detected error information is separated with comma for each error and displayed.
  Unit No:    1                         * Unit No: 1 - 6
  BUS Status 1    :Ready                * F-SB bus between NIU and IOM Unit
               2    :Ready
      Slot No. Type     Status In-Bus1 In-Bus2 Channel  * In-Bus1/2
      1       XXXXXX Ready / Fail                      ("XXXXXX" is an IOM model name. )
      2       XXXXXX Ready / Fail
  Unit No:    2
      :
   omitted
      :
**********
```

● Operations in the SCS Report dialog box

Use the following buttons to perform operations.

Table H2-1 Explanation of button names and operations

Button	Description
Print	Print the display of the SCS Report dialog box.
File	Save the display of the SCS Report dialog box (text format).
Close	Close the SCS Report dialog box.

■ IOM Report

The input/output module status or the communication module status detected by the SCS CPU module is displayed in the IOM Report window.
Select the input/output module or the communication module in Hardware Configuration Tree View of the SCS State Management window, and then click [System Report] button on the toolbar. The IOM Report dialog box will be displayed.

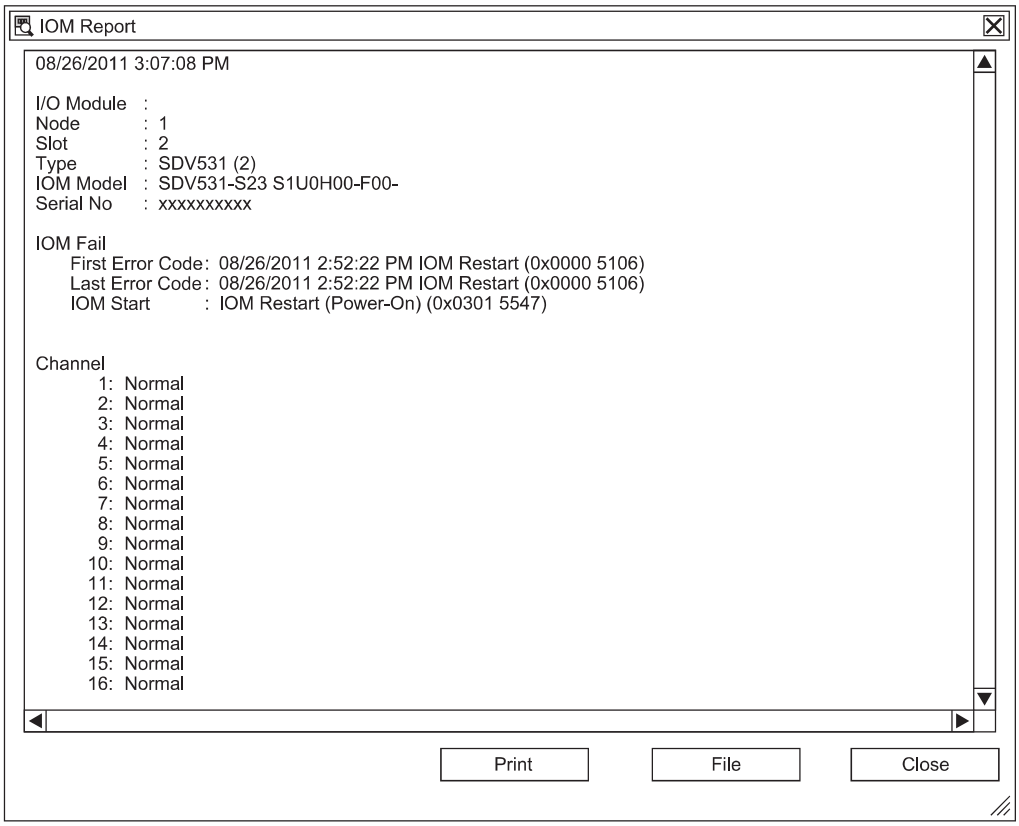


Figure H2-2 IOM Report dialog box

Operations in the IOM Report dialog box

Use the following buttons to perform operations.

Table H2-2 Explanation of button names and operations

Button	Description
Print	Print the display of the IOM Report dialog box.
File	Save the display of the IOM Report dialog box (text format).
Close	Close the IOM Report dialog box.

H3. Checking diagnostic information by using IOM Report

This chapter explains the following items regarding the diagnostic information relating to AIO/DIO modules and communication modules that are displayed in the IOM Report dialog box called from the SCS Maintenance Support Tool.

- Format of diagnostic information displayed in the IOM Report dialog box
- Details of diagnostic information displayed in the IOM Report dialog box

SEE ALSO For more information about IOM Report for the serial communication module, refer to:

H3.2, “IOM Report of communication modules” on page H3-19

Calling the IOM Report

In the Hardware configuration tree view within the SCS State management window of the SCS Maintenance support tool, select an input/output module and click the "System report" button on the tool bar; the IOM Report dialog box appears.

SEE ALSO For more information about the structure and operations of the IOM Report dialog box, refer to:

H2., “System reports” on page H2-1

H3.1 IOM Report of AIO/DIO modules

This section describes the IOM Report for the analog input/output modules (AIO modules) and the digital input/output modules (DIO modules). In the description of these items, AIO/DIO modules are referred to as input/output modules.

Display content in the IOM Report

The IOM Report displays the diagnostic information regarding input/output module errors. The input/output module errors are categorized and displayed as follows:

- Cause of the input/output module error (CPU detection)
  This is a display of the input/output module error status detected by the CPU module of the SCS. The input/output module status as viewed from the CPU (such as No response and HRDY OFF) and other information are displayed. The detailed cause of the input/output module failure is displayed under "Error information inside the input/output module."
- Error information inside the input/output module
  Causes of an error and a recovery are collected from the input/output module, and then displayed.
- Cause of the channel error
  Channel error status is displayed. IOP errors detected by the CPU module and channel errors detected by the input/output module are displayed. If an IOM module becomes error due to an error in an I/O channel, multiple error messages regarding the channel of the I/O module maybe displayed.

TIP

If a bus error occurs between an input/output module and a CPU module, the following codes indicating the source of the error are reported in the IOM Report generated after operations are restored.

- Cause of the input/output module error (CPU Detection)
  No response from the input/output module. CPU is unable to retrieve error information from the input/output module.
- Error information inside the input/output module
  Communication cannot be established with the host CPU or bus for the input/output module, resulting in a host failure error and a fallback operation.

Note also that if there is an input/output module hardware failure, HRDY OFF is displayed in Cause of the input/output module error (CPU Detection) and you can identify the cause of the failure from the error information in the input/output module.

H3.1.1 Display format for the IOM Report of FIO

If the I/O module of FIO is used, the IOM report is displayed in the following format.

```
I/O Module:
Node            : 2
Slot            : 1
Type            : SAI143S
IOM Model       : SAI143-S03 S1U0H00- F00-
Serial No       : XXXXXXXX

(Current status)          : (Current error information (CPU detection))
        First Error Code  : (Information for first error)
        Last Error Code   : (Information at recovery)
         (Error information inside the input/output module)

Channel
1:          (Channel status) (The latest channel error)
              (Cause of the channel error detected by the input/output module)
2:          (Channel status) (The latest channel error)
              (Cause of the channel error detected by the input/output module)
              .
              .

16:         (Channel status) (The latest channel error)
              (Cause of the channel error detected by the input/output module)

(4 kbyte dump display)
```

An example of I/O module error

This is the explanation of the example of the IOM Report that appears when you select a module and call it under the following circumstance.

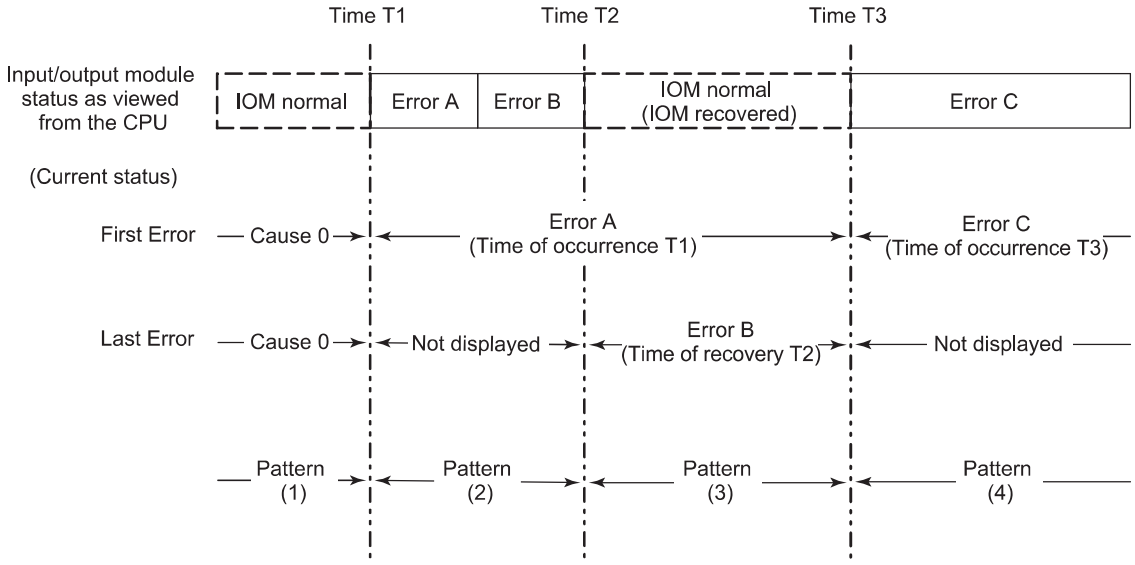


Figure H3.1.1-1 Input/Output module error

The following information will be displayed in each of the situations shown in the figure.

- Pattern (1)

This is a state where there is no input/output module error after the initial cold start of the CPU. In this case, the current status (normal) will be displayed. The first and last error code lines will display the time when the input/output module was started and the cause (Cause 0), respectively.

- Pattern (2)
  This is a state where there is an input/output module error. The current status and the current error content, as well as the time of the first error occurrence (T1) and the first error (Error A), will be displayed. The last error will not be displayed. (The last error code line will not be displayed.)
- Pattern (3)
  This is a state where the input/output module has recovered from the error. The current status (normal), the time of the first error occurrence (T1), the first error (Error A), the time of recovery (T2), and the last error (Error B) will be displayed.
- Pattern (4)
  This is a state where there is an input/output module error. The time of the first error occurrence (T3) and the first error (Error C) will be displayed.

Display format details (I/O module details)

Cause of the input/output module error and error information inside the input/output module are displayed in the following format.

Table H3.1.1-1 Cause of the Input/Output module error and error information inside the Input/Output module

Display item	Description
Current status	The current IOM status will be displayed in the following format. IOM Normal/IOM Fail/IOM Fail (Output Shutoff)
Current error information (CPU detection)	The cause of the current input/output module error detected by the CPU will be displayed with error code. Example: No response (0x0000 5101) Display condition: The information is displayed when there is an input/output module error.
Information for first error	The time of the first error occurrence detected by the CPU (when the input/output module status changed from normal to error) and the error information will be displayed with error code. Example: 20/4/2005 12:34:56 IOM Fail (HRDY OFF) (0x0000 5105) Display condition: The information is displayed when an error occurs with the input/output module even once.
Error information at recovery	The recovery time of the I/O module and the latest error information will be displayed with error code. Example: 20/4/2005 12:50:56 IOM Restart (0x0000 5106) Display condition: The I/O module is currently normal and the displayed information is the latest error in the past.
Information of errors within the I/O module (*1)(*2)	How the input/output module was started and the error code inside the input/output module will be displayed. Example 1: When the input/output module is normal IOM Start: IOM Restart (Power On) (0x0301 5547) Example 2: When there is an input/output module error IOM Fail: IOM Readback Error (0x0101 5502) Display condition: The information is displayed when the cause of the error is stored inside the input/output module, and the input/output module information can be obtained.

*1: The "Information of errors within the I/O module" lists the details of factors of the "Current status" that are due to the I/O module. The status information for individual channels is not included here.
*2: The "starting factors" displayed in the "Information of errors within the I/O module" are detailed factors upon the previous start of the I/O module or recovery from an error.

Display format details (channel details)

The details of a channel error will be displayed as follows:

Table H3.1.1-2 Cause of the channel error

Display item	Description
Channel status (*1)	The current channel status will be displayed. If the I/O module is dual-redundantly configured, the channel status on the control side module will be displayed. - (When the channel is not in use) / Normal / IOP+ / IOP- / TRNS+ / TRNS-/OvrRange/Ch Fail
Latest channel error (*1)	This part displays the time that the channel recovered from the error and the latest error information. If the I/O module is dual-redundantly configured, the latest error on the control side module will be displayed. This item is displayed only when the channel status is normal. Example: Normal (21/6/2005 12:50:56 Last Error: IOP+)
Cause of the channel error detected by the input/output module(*2)	The last-saved channel error in the I/O module will be displayed. If multiple errors are kept in the I/O module, the multiple errors may be displayed. Even if the I/O module is in dual-redundant configuration, the error of the module will be displayed anyway. Example : Open Circuit (0x0401 5561) Short Circuit (0x0401 5562)

*1: The channel status during IOM Failure is the status right before the IOM fails.
*2: If the IOM failure is caused by the abnormality of a channel, the error of the channel will be displayed in IOM Report.

Example 1: Channel Failed
1: IOP+
2: Ch Fail
Open Circuit (0x0401 5561)

Example 2: Channel Recovered
3: Normal (22/8/2011 12:50:56 Last Error :IOP+)
4: Normal (22/8/2011 12:50:56 Last Error :Ch Fail)
Open Circuit (0x0401 5561)

TIP

The channel status and the last error of a pair of dual-redundantly configured input/output modules will be collected from the active input/output module. If the input/output module is placed in a redundant configuration, read the descriptions regarding the IOM Report of the active input/output module for details.

H3.1.2 Display format for the IOM report of N-IO

The section explains the IOM Reports in the N-IO hardware for N-ESB bus coupler module, N-ESB bus module, and I/O module.

N-ESB bus coupler module (S2EN40x)

The IOM report of S2EN402 and S2EN404 is displayed in the following format.

```
YYYY/MM/DD  HH:MM:SS
(Status)
Bus Coupler Module:
Node            : 2
Slot            : 1
Type            : S2EN404
IOM Model       : S2EN404
FPGA Revision   : 01

(Current Status)
Port1 Status    : Link Up
Port2 Status    : Link Up
Port3 Status    : Link Up
Port4 Status    : Link Up

Port 1 Live List  :  1,  2,  3,  4,  5,  6,  7,  8,  9, 10, 11, 12, 13, 14, 15, 16
Port 2 Live List  : 17, 18, 19, 20, 21, 22, 23, 24
Port 3 Live List  : 25, 26, 27, 28, 29, 30
Port 4 Live List  : 31, 32

(256 byte dump display)
```

Table H3.1.2-1 Display items of S2EN40x

Item	Description
YYYY/MM/DD HH:MM:SS	Date and time when the IOM Report is displayed
Status	Acquisition status of the IOM Report (*1)
Type	Module type: Bus Coupler Module
Node	Node number
Slot	Slot number: 1 to 8
Type	Model of the module: Model of the module defined in SENG
IOM Model	Manufacturing information of the module Model of the module that is installed
FPGA Revision	Revision of FPGA (Field Programmable Gate Array)
Current status	The IOM status is displayed. IOM Normal: Normal IOM Fail: Failure
Port n Status	Link status of N-ESB port n (n=1 to 4) Link Up: Transmission possible Link Down: Communication not possible (*2)
Port n Live List	Live list information of the N-IO node that is connected under the N-ESB port n (n=1 to 4) Addresses of N-IO nodes that support the communication from S2EN40x are listed Scope: 1 to 32, ascending order, maximum 16 nodes; addresses that are not in succession are displayed close to each other. (*3)

*1: Blank when it is normal.
- When implementing a module different from the defined module: This IOM differs from the model name which the engineering function defined.

- When module cannot be accessed: Cannot get the memory information in this IOM.

*2: In S2EN402, Link Down is always displayed for port 3 and port 4.
*3: In S2EN402, no node address is displayed for port 3 and port 4.

N-ESB bus module (S2EN501)

The IOM report of S2EN501 is displayed in the following format.

```
YYYY/MM/DD  HH:MM:SS
(Status)
Node Interface Unit:
Node          : 2
Slot          : Left
Type          : S2EN501
IOM Model     : S2EN501-S00030
FPGA Revision : 8033
Serial No.    : xxxxxxx

(Current Status)
Maintenance Port : Enabled
PSU 1 Status     : Normal
PSU 2 Status     : Fail  (OVERVOLTAGE:  25.1V)
Temperature      : Normal  (24C)
External Equipment:  Normal

(256 byte dump display)
```

Table H3.1.2-2 Display items of S2EN501

Item	Description
YYYY/MM/DD HH:MM:SS	Date and time when the IOM Report is displayed
Status	Acquisition status of the IOM Report (*1)
Type	Module type: Node Interface Unit
Node	Node number
Slot	Slot number: Left or Right
Type	Model of the module: Model of the module defined in SENG
IOM Model	Manufacturing information of the module Model and basic specification code of the module that is installed
FPGA Revision	Revision of FPGA (Field Programmable Gate Array)
Serial No.	Serial No. : Serial No. of the module that is actually installed.
Current status	Displays the status of NIU. NIU Normal: Normal NIU Fail: Failure NIU Fail (Due to maintenance of one module): Failure due to maintenance of one module (*2) NIU Maintenance: Under maintenance
Maintenance Port	Displays the status of the maintenance port Disabled: Inactive Enabled: Active
PSU 1 Status	The status of PSU 1 Normal: Normal Fail: Failure The results of the power diagnosis and voltage value are shown in (). POWER OFF: Stops PSU function OVERVOLTAGE: PSU output shows over-voltage CODE = XXXX: Error with code XXXX has occurred

Continues on the next page

Table H3.1.2-2 Display items of S2EN501 (Table continued)

Item	Description
PSU 2 Status	The status of PSU 2 Redundant power: same as PSU 1
Temperature	Temperature around S2EN501 Normal: Normal HI: HI alarm LO: LO alarm Temperature (Celsius) is shown in ().
External Equipment	The status of the discrete input from external devices Normal: Normal Fail: Failure

*1: Same as S2EN40x.
*2: This status indicates that one module of the NIU is normal and the other is under maintenance.

N-IO I/O module (example for S2MMM843)

The IOM report is displayed in the following format.

```
YYYY/MM/DD  HH:MM:SS
(Status)
I/O Module:
Node                : 2
Unit                : 1
Slot                : 1
IOM Type            : S2MMM843
IOM Model           : S2MMM843-SS1030S1U000000
Serial No.          : xxxxxxx
Base Plate Type     : S2BN1D
Base Plate Model    : S2BN1D

F-SB Status
  Bus          S2EN501        Status
  1            L              Normal
  1            R              Normal
  2            L              Normal
  2            R              Normal

(Current status) : (Current error (CPU detection))
      First Error Code : (First error)
      Last Error Code : (Error at recovery)
      (Error information in IOM)

Channel
       1 : (Channel type)
          (Channel Status) (Cause of Last Error)
                    (History of Error Cause in IOM)
        (Skip)
       16 : (Channel type)
            (Channel Status) (Cause of Last Error)
                    (History of Error Cause in IOM)
(6k byte dump display)
```

Table H3.1.2-3 Display Items of the N-IO I/O Module

Item	Details	Description
YYYY/MM/DD HH:MM:SS		Date and time when the IOM Report is displayed
Status		Acquisition status of the IOM Report (*1)

Continues on the next page

Table H3.1.2-3 Display Items of the N-IO I/O Module (Table continued)

Item	Details	Description
Type		Module type: I/O Module
Node		Node number
Unit		I/O Unit number: 1 to 6
Slot		Slot number: 1 to 2
Type		Model of the module: Model of the module defined in SENG
IOM Model		Manufacturing information and firmware revision of the module Model, basic specification code, hardware revision, and firmware revision of the module that is installed
Serial No.		Serial No. : Serial No. of the module that is actually installed.
Base Plate Type		Model of the base plate: Model of the base plate defined in SENG
Base Plate Model		Model of the base plate: Model of the base plate that is installed (*2)
F-SB Status	IN-Bus	Flexible-SB bus number seen from IOM (1, 2): 1 or 2
	S2EN501	Slot position of S2EN501: L (left) or R (right)
	Status	Communication status between S2EN501 and IOM Normal: Normal Fail: Failure
(Main cause of error in IOM)	Current status	Displays the current status of IOM. IOM Normal: Normal IOM Fail: Failure IOM Fail (Output Shutoff): Error in output shutoff switch operation
	Current error details	Displays the current cause of the IOM error that is detected by the CPU in character strings and error code. Displayed when there is an error in IOM. Example: No response (0x0000 5101)
	First Error (*3)	Displays the first error code detected by the CPU in character strings, error code, and time (time of error occurrence). First error indicates the change of IOM status from normal to error. It appears when an error occurs even once. Example: 2016/2/24 12:34:56 IOM Fail (HRDY OFF) (0x0000 5105)
	Last Error (*3)	Displays date and time of recovery, last error code and startup cause. Displays in the normal state of IOM after recovery from error. Example: 2016/2/24 12:50:56 IOM Restart (0x0000 5106)
	Information of errors within the IOM (*4) (*5)	Displays the IOM internal error code and startup cause. This is displayed when IOM information is obtained and the error cause is stored. Example 1: IOM in normal state IOM Normal: IOM Restart (Power On) (0x0301 5547) Example 2: IOM in error state IOM Fail: IOM Readback Error (0x0101 5502)

Continues on the next page

Table H3.1.2-3 Display Items of the N-IO I/O Module (Table continued)

Item	Details	Description
Channel		Displays the following information for each channel. The number of channels depends on the IOM type. S2MMM843, S2MDV843: 1 to 16 channels
	Channel type	Displays the signal type of the I/O channel defined in IOM Builder.
	Channel status (*6) (*7)	Displays the current channel status. If IOM is redundant, channel status of the control side is displayed. - (Unused) / Normal / IOP+ / IOP- / TRNS+ / TRNS- / Rang Over / Ch Fail, etc.
	Cause of Last Error (*6)	Displays date and time of recovery from channel error, and cause of the last error. . If IOM is redundant, cause of the last error that has occurred in the module of the control side is displayed. It is displayed only when the channel is normal. Example: Normal (2015/6/21 12:50:56 Last Error: IOP+)
	Display of history of IOM error causes (*7)	Cause of the last error saved in IOM is displayed (if there are multiple errors, they are individually displayed). Even when IOM is redundant, error cause (cause of error detected in the corresponding module) of the corresponding module is displayed. Example 1: Open Circuit (0x0401 5561) Example 2: Short Circuit (0x0401 5562)

*1: Same as S2EN40x.
*2: In the base plate for intrinsic safety barrier, the basic specification code (-xxxC/ -xxxD) is displayed at the end of base plate model. Only a character (4th character = position of terminal) is displayed according to the base plate while others are displayed as xxx.
*3: The current status of IOM and display pattern of First Error/Last Error are similar to SSC60 FIO.
*4: The "Information of errors within the IOM" lists the details of factors of the "Current status" that are due to the I/O module. The status information for individual channels is not included here.
*5: The "starting factors" displayed in the "Information of errors within the IOM" are detailed factors upon the previous start of the I/O module or recovery from an error.
*6: The status before the error occurrence is retained during the IOM error occurrence.
*7: When the "Channel status" is Normal, this indicates that the "Display of history of IOM error causes" is a history of errors from the past. The channel status can be confirmed from the SCS State Management Window and HIS due to being notified to the operating status and system alarm.

SEE ALSO For more information about signal types of the channels, refer to:

"● Lower part of the list view when an individual I/O module of an N-IO node is selected" on page H1-20

For more information about IOM error causes, channel status, and details displayed in history of errors, refer to:

H3.1.3, "Code system for causes of errors in the IOM Report" on page H3-12

● High current output

The IOM report is displayed in the following format when the signal type of the channel is set to high current output with S2MMM843 or S2MDV843.

```
Channel
    1 : (OUT) Status 2.0A*
        Ch Fail
    2 : (OUT) Status 2.0A
        -
    3 : (OUT) Status 2.0A
        -
                Open Circuit (0x0401 5561)
```

This section describes the IOM Report when there is an error in the non-primary channel.

Channel error information is displayed in the part that shows the channel status of the IOM report. For example, if failure occurs in non-primary channel 3 of combined 1 to 3 channels,

information is displayed in both the primary channel of the IOM report and the non-primary channel where error occurred.

When the high current output is set, “Cause of last error” of the primary channel indicates the compound causes of the primary channel and non-primary channel. When the high current output is set, check the “Cause of last error” of the primary channel.

“Channel status” is displayed in the primary channel. “Cause of last error” is also displayed if error occurred in the past. Actual error cause is displayed in “Error cause history of IOM” in the non-primary channel. However, "-" is displayed in “channel status” to indicated that the channel is not used.

If an error occurs only in the primary channel, information is displayed only in the number of the primary channel.

Table H3.1.2-4 Display items of high current output

Signal type	Character string	Description
Status output (1.3A output)	(OUT) Status 1.3A*	Primary channel
	(OUT) Status 1.3A	Non-primary channel
Status output (2A output)	(OUT) Status 2.0A*	Primary channel
	(OUT) Status 2.0A	Non-primary channel

The "Display of history of IOM error causes" displays the latest information on the causes of errors that have occurred anytime in the past leading to the present. With the large current output (DO), even in a case when an error has occurred with a certain channel, information of occurrence in the past may be remaining in the error cause history of a different channel that is currently normal.

H3.1.3 Code system for causes of errors in the IOM Report

The display format and the code system in the IOM Report to indicate the causes of errors are as follows:

Display format

Category of input/output module errors Δ Category of causes of errors

Code system for category of Input/Output module errors

- 0x00XX
  Error detected by the CPU
- 0x01XX
  Input/Output Module Hardware Failure
- 0x02XX
  Input/output module setting error (such as a disconnected connector on the field side)
- 0x03XX
  Recovery from an input/output module error (such as when the input/output module was recovered from 0x02 above, or recovered after the fallback operation was executed upon detecting a host side error)
- 0x04XX
  Channel error (In this case, there is an error with the applicable channel. It indicates a wiring error or a channel hardware failure when the input/output module is in a single configuration. If the input/output module is in a redundant configuration, the channel hardware failure will be displayed as the category 0x01XX "Input/output module hardware failure.")

Code system for category of causes of errors

- 0x51XX
  Content of error detected by the CPU
- 0x55XX
  Content of error detected by the input/output module (including cause of recovery)

Cause of the Input/Output module error (CPU detection)

The following explains the details of the codes used to indicate the cause of the input/output module error detected by the CPU. The IOM Report will display these codes as "Current error information (CPU detection)," "Information for first error," or "Error information at recovery."

Table H3.1.3-1 Details of codes for cause of Input/Output module error (CPU detection)

Code (hexadecimal)	Display	Description
0000 5101	No response	A no-response error has occurred during the communication between the CPU and the input/output module. The error occurred is either with the input/output module or in the communication path to the input/output module.
0000 5102	IOM model Code Error	The model name of the input/output module defined in the SENG does not match that of the input/output module installed. Verify the model name of the input/output module.

Continues on the next page

Table H3.1.3-1 Details of codes for cause of Input/Output module error (CPU detection) (Table continued)

Code (hexadecimal)	Display	Description
0000 5103	IOM Configuration Error	The setting information defined in the I/O parameter builder does not match the input/output module setting information. Perform IOM download.
0000 5104	IOM Fail (HRDY OFF)	An input/output module hardware failure has been detected. An error occurred and the HRDY on the I/O module turned OFF. Check the error information inside the input/output module for the detailed cause of the error.
0000 5105	I/O Error (AP READY-OFF)	The error may have been generated because the connector is disconnected and field power not supplied, or IOM download was performed. Check the error information inside the input/output module for the detailed cause of the error.
0000 5106	IOM Restart	The input/output module has recovered from the error state. Check the error information inside the input/output module for the detailed cause of the error.
0000 5107 (*1)	Output Shutoff	An error occurred and the Output Shutoff switch was activated due to a reason other than output module failure (the HRDY does not turn OFF). Check the IOM Report for the detailed cause of the error. If this type of error occurs, perform the output module start operation after the cause of the error has been eliminated.
0000 5111	Communication Error	An error has been detected in the data check of the communication between the CPU and the input/output module. This error may have been caused due to a failure with the input/output module or the communication path between the CPU and the input/output module.
0000 5112		
0000 5113		
0000 5108 (*2)		
0000 5109 (*2)		
0000 511d (*2)		
0000 511e (*2)		
0000 5114	IOM Redundant Control Fail	An error has been detected in the redundancy control part of the I/O module. Replace the I/O module. However, when two I/O modules of single definition are changed to redundant in the FIO node and online change download is performed, this error may occur if the connector is connected only to the I/O module of either side. In this case, you need to connect the connector to the I/O modules of both sides. Recovery can be checked by system alarm message No.0082 "Normal recovery of I/O modules". In this case, it is not necessary to replace the input/output module.
0000 5115		
0000 5116	IOM Error	An error has been detected in the input/output module. Replace the input/output module. However, if the IOM Error (0000 5117) occurred after the IOM downloading or during the SCS restarts after offline downloading, there is no need to replace the input/output module.
0000 5117		

*1: Only SDV531-S13 and L1DV531
*2: N-IO only

Differences in output results as a result of differences in AIO/DIO module firmware

If the following errors occur and an IOM report is displayed, either "0000 5103" or "0000 5105" will be displayed, depending on the version of the AIO/DIO module.

- Download in progress for input/output module initialization
- Front connector disconnected
- Failure in the power supply from the front connector

When an error addressed as “0000 5103” remains unsolved although you perform IOM download as the corrective action against “0000 5103” error, the actual error is possibly one of these three errors because they are originally “0000 5105” errors. Confirm that the front connector is properly connected.

Error information inside the Input/Output module

The following explains the details of the codes for the cause of error detected by the input/output module in the channel common area of the input/output module, or in the channel area if the input/output module is in a redundant configuration. The IOM Report will display these codes as "Error information inside the input/output module."

Input/Output module hardware failure

The following explains the details of the codes for hardware failure in the channel common area of the input/output module, or in the channel area if the input/output module is in a redundant configuration.

Table H3.1.3-2 Details of codes for Input/Output hardware failure

Code (hexadecimal)	Display	Description
01xx 5501 (xx: Internal code)	IOM Channel Common Fail	There has been a failure in the channel common area of the input/output module. Replace the input/output module.
0101 5502 0401 5502 (*1)	Output Readback Error	An error has been detected in the readback process for the output value. Check the field wiring of the analog output module for any abnormality (for example, short-circuits between channels), and also confirm that the total resistance of all connected cables and devices does not exceed the value of the allowable output load resistance for output modules that is written in the GS (General Specification). If the wiring and resistance are appropriate, replace the output module.
0101 5503 0401 5503 (*1) (*2)	Internal Power Supply Fail	An error has been detected in the channel power supply. Replace the input/output module.
0101 5504 0401 5504 (*1)	Output Channel Stuck at ON	A failure that the output channel is unable to change from ON to OFF has been detected. Check the field wiring for any abnormality (for example, short-circuits between channels). If there is no field wiring error, replace the output module.
0101 5505 0401 5505 (*1)	I/O Channel Stuck at OFF	With the input channel, a failure where the input signal does not turn ON has been detected. With the output channel, a failure where the output signal cannot be turned ON has been detected. If there are not errors with the field wiring, replace the I/O module.

Continues on the next page

Table H3.1.3-2 Details of codes for Input/Output hardware failure (Table continued)

Code (hexadecimal)	Display	Description
0101 5506 0401 5506 (*1)	Over Current	An overcurrent failure has been detected inside the input/output module. Replace the input/output module.
01xx 5507 04xx 5507 (xx: Internal code) (*1)	IOM Channel Fail	There have been some errors with the channel area of the input/output module. Check if there is an input of a signal value at a level between ON and OFF or chattering has occurred. If the input signal level is normal or chattering has not occurred, replace the input/output module.

*1: For a channel failure, the error code and the error status will vary depending on whether the I/O module is of a duplex configuration or a single configuration.
- The upper error code is for a redundantly configured I/O module, while the lower error code is for a non-redundantly configured I/O module.
- If the input/output module is in a redundant configuration, this error will be an IOM Fail error. In a non-redundant configuration, the error will occur only to the failed channel.

*2: FIO only

SEE ALSO

For more information about allowable load resistance of the analog output modules for SIL 3, refer to:

ProSafe-RS Analog I/O Modules (for FIO) (GS 32P06K60-01EN)

For more information about allowable load resistance of the analog output modules for SIL 2, refer to:

ProSafe-RS Lite Analog I/O Modules (GS 32P56K30-01EN)

Input/Output module setting error

The following explains the details of the codes for input/output module setting error.

Table H3.1.3-3 Details of codes for Input/Output module setting error

Code (hexadecimal)	Display	Description
0201 5521 (*1)	Connector on Field Side Disconnected	The connector on the field side is disconnected. Check the connector.
0201 5522 (*1)	Field Power Supply Error	There has been a voltage error with the field power supply. Check if there are any errors with the field power supply or the wiring. If there is no error, replace the input/output module.
0201 5523	Execution of Download	IOM download is being executed.
0201 5524 0401 5524 (*1) (*2)	Transmitter Power Error	There has been an error with the transmitter power supply inside the input/output module. Check if there are any errors with the transmitter, the field wiring and the input/output module setting. The error may have been caused because the two-wire/four-wire setting of the current input module and the pin setting of the input/output module do not match.
0201 5525 (*3)	IOM Disabled	The I/O module has been stopped due to a request from a higher level.
0201 5526 (*4)	Base Plate Model Code Error	The model of the base plate for IOM that is defined in the builder and the model of the actually mounted base plate do not match. Check the model of the base plate.
02xx 5542 (xx: Internal code) (*4)	Fallback	The I/O module has detected an error in the communication with the host, and the fallback operation was executed. Check the communication path between the CPU and I/O module.

*1: FIO only
*2: For a channel failure, the error code and the error status will vary depending on whether the I/O module is of a duplex configuration or a single configuration.

- The upper error code is for a redundantly configured I/O module, while the lower error code is for a non-redundantly configured I/O module.
- If the input/output module is in a redundant configuration, this error will be an IOM Fail error. In a non-redundant configuration, the error will occur only to the failed channel.

*3: Only style S4 or later of SAI143 and L1AI143
*4: N-IO only

Recovery from Input/Output module error

The following explains the details of the codes for recovery from input/output module error.

Table H3.1.3-4 Details of codes for recovery from Input/Output module error

Code (hexadecimal)	Display	Description
0301 5541 (*1)	Connector on Field Side Recover	The input/output module has recovered from the disconnection error of the field side connector.
03xx 5542 (xx: Internal code)	Fallback	The I/O module has recovered from fallback.
0301 5543	Field Power Supply Recover	The field power supply has recovered to a normal state.
0301 5544	Download Completed	IOM download has been completed.
0301 5545 (*2)	IOM Enabled	The I/O module has recovered from being stopped due to a request from a higher level.
0301 5546 (*1)	Output Shutoff	The output shutoff switch has recovered from operation. Follow the recovery procedures.
0301 5547	IOM Restart (Power-On)	The input/output module started after turning the power on.
0301 5548 (*1)	Transmitter Power Recover	The transmitter power supply has recovered to a normal state.

*1: FIO only
*2: Only style S4 or later of SAI143 and L1AI143

Cause of the channel error

The following explains the details of the codes related to channel error. The IOM Report will display these codes as "Channel status", "The latest channel error" and "Cause of the channel error detected by the input/output module" in the area where causes of channel errors are to be displayed.

Channel status, the latest channel error

"Channel status" in the IOM Report will display the channel status (cause of a channel error) detected by the CPU. The "latest channel error" is the last error that CPU detected. The details of the codes are explained in the following table.

Table H3.1.3-5 Details of codes for channel status

Code (hexadecimal)	Display	Description
0000 5121	TRNS+	A transmitter high limit error has occurred.
0000 5122	TRNS-	A transmitter low limit error has occurred.
0000 5123	IOP+	An input high limit error has occurred.
0000 5124	IOP-	An input low limit error has occurred.

Continues on the next page

Table H3.1.3-5 Details of codes for channel status (Table continued)

Code (hexadecimal)	Display	Description
0000 5125 0000 5126	OvrRange	Replace the input module. • For SAI143/L1AI143 and SAV144/L1AV144 There has been an internal error that the analog input value is out of the range between -25 % and 125 %. • For SAT145/L1AT145 and SAR145/L1AR145 There has been an internal error that the input value is either not a number, an infinity or out of the range that the module can handle.
0000 5127	Ch Fail	A channel error has occurred. Check the display of cause of the channel error detected by the input/output module for the cause of the error.
0000 5128 (*1)	IS Barrier Disconnected	Disconnection of intrinsic safety barrier has been detected. Check the connection of intrinsic safety barrier.
0000 5129 (*1)	IS Barrier Configuration Error	Setting error of intrinsic safety barrier has occurred. Settings information defined in the builder and the connected intrinsic safety barrier may be different.
0000 512a (*1)	Open Circuit	An error has occurred due to open circuit. Check the field wiring. A short circuit error is suspected if a barrier is used.
0000 512b (*1)	Short Circuit	An error has occurred due to short circuit. Check the field wiring.
0000 512c (*1)	Field Side Error	Other errors (open circuit/short circuit detection by intrinsic safety barrier, etc.) have been detected on the field side. Check the error cause in detailed cause.

*1: N-IO only

Cause of channel error detected by the Input/Output module (Input/Output module detection and the details of channel error)

"Cause of channel error detected by the input/output module" will display channel errors detected by the input/output module. Details of the codes are explained.

Table H3.1.3-6 Details of codes for cause of channel error detected by the Input/Output module

Code (hexadecimal)	Display	Description
0401 5561	Open Circuit	An error has occurred due to open circuit. Check the field wiring. In SDV526/L1DV526, open circuit occurs due to a channel fuse burnout caused by a short circuit. Check the field wiring and channel fuses.
0401 5562	Short Circuit	An error has occurred due to short circuit. Check the field wiring.
0401 5563 (*1)	Short circuit between channels	There is short circuiting between channels. Check if there are any field wiring errors.
0401 5564 (*1)	Output Overload	An output overload has been detected. Check if there are any errors with the field wiring or the loading device.
0401 5567 (*1)	RJC Error	This is an input error of reference junction compensation (RJC) in SAT145/L1AT145. The cause is likely a failure in the thermistor for the reference junction compensation for the terminal board. Check if there are any errors in the terminal board.
0401 5568 (*1)		
0401 5522 (*2)	Field Power Supply Error	There has been a voltage error with the field power supply. Check the field power supply and wiring.

Continues on the next page

Table H3.1.3-6 Details of codes for cause of channel error detected by the Input/Output module (Table continued)

Code (hexadecimal)	Display	Description
0401 5570 (*2)	DO Shutoff	Detected an error that activated the DO shutoff switch in the DO channel of S2MMM843 or S2MDV843. Check the error cause of the DO channel in IOM.
0401 5571 (*2)	I/O Shutoff	Detected an error that activated the I/O shutoff switch in the AO channel of S2MMM843. Check the error cause of the AO channel in IOM.
0401 5572 (*2)	Line Fault Detection	Open circuit or short circuit is detected in the intrinsic safety barrier. Check the field wiring.
0401 5573 (*2)	IS Barrier Configuration Error	Setting error of intrinsic safety barrier has occurred. Settings information defined in the builder and the connected intrinsic safety barrier may be different.
0401 5576 (*2)	IS Barrier Disconnected	Disconnection of intrinsic safety barrier has been detected. Check the connection of intrinsic safety barrier.

*1: FIO only
*2: N-IO only

If the status of the input/output module is single, the code 04xx xxxx error explained on the Input/output module hardware failure page is displayed as the cause of the channel error detected in the input/output module.

SEE ALSO For more information about causes of channel errors, refer to:

"● Input/Output module hardware failure" on page H3-14

H3.2 IOM Report of communication modules

This section explains the IOM Report on the following communication modules.

- Serial communication module (Modbus slave communication)
- Serial communication module (Subsystem communication)
- Ethernet communication module (Modbus slave communication or DNP3 communication)
- Ethernet communication module (Subsystem communication)
- Fire and gas communication modules (Fire and gas communication)

Display format of IOM Reports on serial communication modules (Modbus slave communication)

The display format of IOM Reports when an ALR111 or ALR121 is used for Modbus slave communication is as follows:

I/O Module:

Node:	2
Slot:	6
Type:	ALR111
IOM Model:	ALR111-S03 S0U0H0-- F0--

(4-kbyte dump display)

Display format of IOM Reports on serial communication modules (subsystem communication)

The display format of IOM Reports when an ALR111 or ALR121 is used for subsystem communication is as follows.

TIP Information of the specified communication module is displayed even when the module is configured as a redundant module.

```
I/O Module:
Node:        2
Slot:        4
Type:        ALR111
IOM Model:   ALR111-S03 S0U0H0-- F0--
Serial No:   XXXXXXXX

Subsystem Name:    (Subsystem name)
Revision:          (Subsystem package revision)

IOM Status:        (Communication module status) (Detail cause)
Port1 Status:      (Port communication status)
Port2 Status:      (Port communication status)

Communication Status
1     0000  0000  0000  0000  0000  0000  0000  0000  0000  0000
11    0000  A3B0  A3B0  A3B0  0000  0001  0001  0001  0001  0001
                .
                .
(4-kbyte dump display)
```

In the above example, communication definitions 1 to 11 indicate a normal status, while communication definitions 12 to 14 indicate an A3B0 error. After the communication definition 16, there is no communication definition or corresponding communication is not performed.

Table H3.2-1 Display items for ALR111/ALR121 in subsystem communication

Display item	Description	Remark
Subsystem name	The name of the subsystem package currently loaded to the ALR111/ALR121 is displayed. (Example) Subsystem Name: S_MODBUS	-
Subsystem package release number	The release number of the subsystem package in the ALR111/ALR121 is displayed.	-
Detailed causes of communication module statuses	The status of the communication module is displayed. • Control: Normal (at single configuration), control side in the case of a redundant module • Stand-by: Stand-by side in the case of a redundant module • Fail: Error If the module status is "Fail," the detail cause of the error (error cause code) is displayed.	Refer to the Diagnostic information message No. 0081 for the content of the error cause code.
Port 1/2 communication statuses	Displays the port status of port 1 and port 2. "Ready" is displayed in the case of communication module error. • Ready: The serial communication status is normal, or there is no communication definition. • Error: A serial communication error has occurred.	-
Communication Status (Communication error code for communication definition n: 1 <= n <= 128)	The communication status is displayed for each communication definition. This item is invalid if the communication module has generated an error. The status information for 128 definitions is displayed. 0x0000: The communication status is normal. 0x0001: There is no communication definition, or communication is not performed. 0xA3XX: Communication error code	-

Continues on the next page

Table H3.2-1 Display items for ALR111/ALR121 in subsystem communication (Table continued)

Display item	Description	Remark
Communication Status (for SLSEVENT type communication definition when subsystem communication program S_SLSMOD is used in ALR121)	The area for two definitions is required for SLSEVENT type communication definition for ProSafe-SLS event collection. 0x0000 0x0000: The communication status is normal. 0x0001 0x0000: Communication is not performed. 0xA3XX 0x0000: Communication error code	-

SEE ALSO

For more information about Diagnostic information messages, refer to:

Message Number 0081 in 3.1, "Safety Control Station Error Occurrence and Recovery Messages (Message Numbers 0001 through 0094)" in Messages Reference Manual (IM 32P02B10-01EN)

For more information about communication error codes displayed under Communication Status, refer to:

- manual for the connected Modbus system
- "■ Communication error code" in D2.1, "Communication specifications" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Reading communication status when using ProSafe-SLS communication function

When ALR121 is used for ProSafe-SLS communication function, communication status may be read in a particular way. Communication status for SLSEVENT type communication definition for ProSafe-SLS event collection is displayed in 4-kbyte that is equal to two definitions of other type. The detailed example is as follows:

Communication definition of SLSEVENT type

Communication Status										
1	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
11	0000	A3B0	A3B0	A3B0	0000	0001	0001	0001	0001	0000
21	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000

.
.

(4-kbyte dump display)

The circled 14th communication definition is SLSEVENT type and other communication definitions are types other than SLSEVENT type. Each communication definition corresponds to the following communication status:

Table H3.2-2 Correspondence between communication definition and communication status

Communication definition	Communication status
1st to 11th	Normal communication
12th to 13th	Communication error (No response from subsystem)
14th	Communication error in SLSEVENT type (No response from subsystem)
15th to 18th	No communication
19th to 29th	Normal communication

Confirm the correspondence relation between each communication definition and communication status on the Comm. I/O Definition tab of Communication I/O Builder or the Communication Group Definition list of Safety Communication I/O Editor.

Display format of IOM Reports on Ethernet communication modules (Modbus slave communication or DNP3 communication)

The display format of IOM Reports when an ALE111 is used for Modbus slave communication or DNP3 communication is as follows:

I/O Module:

Node: 2
Slot: 1
Type: ALE111
IOM Model: ALE111-S03 S0U0H0-- F0--
Serial No: XXXXXXXX

(4-kbyte dump display)

Display format of Ethernet communication module (Subsystem communication) IOM report

The following shows the display format of the IOM report if ALE111 is used for subsystem communication.

TIP Information of the specified communication module is displayed even in the case of redundancy.

```
I/O Module :
Node       : 2
Slot       : 1
Type       : ALE111
IOM Model  : ALE111-S03 S0U0H0-- F0--
Serial No  : XXXXXXXX

Subsystem Name : (Subsystem name)
Revision   :     (Subsystem package revision)

IOM Status :     (Communication module status) (Detail cause)
Port Status :    (Port communication status)

Communication Status
     1  0000 0000 0000 0000 0000   0000 0000 0000 0000 0000
    11  0000 A3B0 A3B0 A3B0 0000   0001 0001 0001 0001 0001
        :

(4-kbyte dump display)
```

In this example, communication definition from 1 to 11 shows “normal”, 12 to 14 shows "A3B0 error" and 16 onwards shows "Communication is not performed”.

Table H3.2-3 ALE111 display items for subsystem communication

Display items	Display contents	Remarks
Subsystem name	Displays the name of the subsystem package that is loaded in ALE111. (Example) Subsystem Name: S_MODTCP	
Subsystem package revision	Displays the package revision of the subsystem in ALE111. (Example) Revision: R4.01.00	

Continues on the next page

Table H3.2-3 ALE111 display items for subsystem communication (Table continued)

Display items	Display contents	Remarks
IOM status Detailed cause	The IOM status is displayed. Control: Normal status of non-redundant module, or control side of redundant modules Stand-by: Standby side of redundant modules Fail: Failure Detailed causes (error code) of the error are displayed in the case of "Fail".	Refer to System Alarm Message No.0081 for contents of error cause code.
Port status	The communication status of the port is displayed. Note that “Ready” is displayed in the case of IOM error. Ready: Communication is normal or undefined Error: Communication error has occurred	
Communication error code for each communication definition	The communication status for each communication definition is displayed. Not valid in the case of IOM error. Displays for 128 definitions. 0x0000: Normal communication 0x0001: Undefined communication or no communication 0xA3XX: Communication error code	

Display format for the IOM Report of fire and gas communication modules

The display format for the IOM Report of S2LP131 is as follows:

```
I/O Module  :
Node              : 2
Slot              : 1
Type              : S2LP131
IOM Model         : S2LP131-S01 S0U0H0--F0--
Serial No         : xxxxxxxx

Subsystem Name    : (Subsystem package name)
Revision          : (Subsystem package revision)

IOM Status        : (Communication module status) (Detail cause)
Port Status       : (Port communication status)

Communication Status
Number      Communication Group     SS-SCPATH    SS-SCOM
1           GS01-001 PV             0000         0000
2           GS01-001 DIAGSTATUS     0000
:
101         GS01-50 PV              0000         0000
102         GS01-50 DIAGSTATUS      0000
:
200

(14-kbyte dump display)
```

Table H3.2-4 Display items of S2LP131

Display item	Description	Remarks
Subsystem package name	Displays the name of the subsystem package that is loaded in S2LP131. (Example) Subsystem Name: S_FGCOM	
Subsystem package revision	Displays the revision of the subsystem package in S2LP131. (Example) Revision: R1.01.00	

Continues on the next page

Table H3.2-4 Display items of S2LP131 (Table continued)

Display item	Description	Remarks
IOM status Detailed cause	The IOM status is displayed. Control: Normal Fail: Error Detailed causes (error cause code) of the error are displayed in the case of "Fail".	Refer to System Alarm Message No.4209 and No.4211 for contents of the error cause codes.
Port status	The communication status of the port is displayed. Note that “Ready” is displayed in the case of IOM Fail. However, “Error” is displayed when an SS-SCOM error has occurred. Ready: Communication is normal or undefined Error: Communication error has occurred	
Communication error code for each communication definition	The communication status for each communication definition is displayed. Invalid in the case of an IOM error. Displays codes for 200 definitions. 0x0000: Normal communication 0x0001: No communication (*1) 0xA3XX: Communication error code (SS-SCPATH) 0x5AXX: Communication error code (SS-SCOM) Blank: There is no corresponding data. (*2)	

*1: This error code will not be displayed for SS-SCOM. PROFIsafe communication between SCS and GS01 does not have a status indicating that communication is not completed. Therefore, in the case of SS-SCOM, either 0x0000, which indicates normal communication, or 0x5AXX, which indicates a communication error, is displayed.
*2: The SS-SCOM column is blank for non-safety data.

SEE ALSO

For more information about Diagnostic information messages, refer to:

- Message Number 4209 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)
- Message Number 4211 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)

H4. Displaying I/O channel status

The I/O Channel Status dialog box displays the states of channels of all input/output modules of the relevant SCS in the list format.

Channels whose output is disabled can be changed to the output enabled condition as long as the status is normal, by clicking the [Output enabled] button in this dialog box. Once output channels are placed in the output enabled condition, the output values of the application logic are output to the field.

I/O Channel Status dialog box

On the tool bar of the SCS State Management window, click [I/O Channel Status]. The I/O Channel Status dialog box appears. If both N-IO I/O modules and FIO I/O modules are installed in SCSP3, their respective status is displayed in the [N-IO] tab and the [FIO] tab.

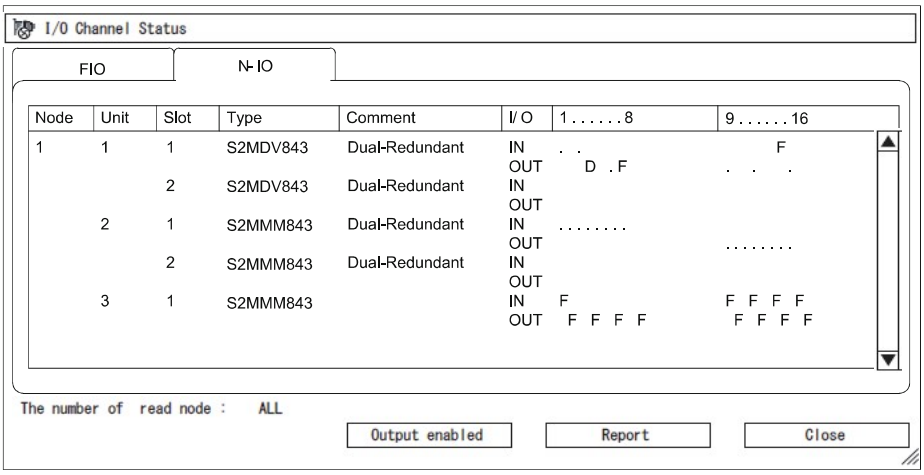


Figure H4-1 I/O Channel Status dialog box

Display of I/O Channel status

Table H4-1 Display of I/O Channel status

Status	Character	Display color
Normal	.	
Error	F	Red
Output Disabled	D	Blue

The error status indicates that the single channel is faulty and/or the error that activates the Output Shutoff switch inside the output module has occurred.

The output disable status indicates that the channel is normal but the output value from the application logic is not sent to the field.

If the I/O module has redundant configuration, the channel status of the control side is displayed in the odd number slot, irrespective of the control status during operation. The channels on the even-number slot are displayed as blank. If the I/O module has redundant configuration, Dual-Redundant is displayed in the Comment column.

The status of the primary channel is displayed, if multiple channels are combined in N-IO I/O module for high current output.

The number of read node configuration information is displayed in the status bar. ALL shows that configuration information of all the nodes is read.

Precautions for forcing functions

Use the following buttons to perform operations in the dialog box.

Table H4-2 Explanation of button names and operations

Button	Description
Output enabled	Place all channels whose outputs have been disabled in the output enabled state within the station.
Report	Displays the same contents of the I/O Channel Status dialog box in the report dialog box.
Close	Close the I/O Channel Status dialog box.

SEE ALSO For more information about enabling output, refer to:

C8., “Output enable operation” on page C8-1

H5. Displaying SCS diagnostic information

SCS diagnostic information messages can be checked in the Diagnostic Information window. The Diagnostic Information window displays diagnostic information messages maintained by the SCS. Diagnostic information messages are the notifications to the users regarding the diagnosis as well as the required necessary actions and maintenance records. From these diagnostic information messages, the location where the error occurred, the cause of the error, the degree of risk, etc., can be identified.

The engineers check the diagnostic information messages for hardware errors, communication errors, etc., in the safety system, and can examine the error causes by referencing the diagnostic information message help function.

Usage of SCS diagnostic information is described below.

Analysis of causes

The Diagnostic Information window allows the user to check diagnostic information messages generated by the SCS' diagnostic function to obtain information on how to handle errors from the Help function. In this way, they are helpful in analysis of causes and maintenance operations.

Classifying potential risks

Each Diagnostic information message has an alarm class that is determined by an error condition, the importance of devices, etc. An engineer can classify the degree of potential risk of the current situation.

Acknowledgement of diagnostic information

Diagnostic information messages maintained by the SCS can be acknowledged and deleted in the Diagnostic Information window.

H5.1 Diagnostic Information window

The Diagnostic Information window displays diagnostic information messages in a list format collected from the SCS.

How to display the Diagnostic Information window

Select a station, I/O node or input/output module, and click [Diagnostic Information] button on the toolbar of the SCS Status Overview window or the SCS State Management window. Only diagnostic information messages related to the selected device are displayed in the Diagnostic Information window.
Up to five Diagnostic Information windows can be displayed at the same time, each window showing the information of an individual station, an input/output module, etc.

Security of the Diagnostic Information window

If you entered the password for the SCS Maintenance Support Tool when launching the original window from which the Diagnostic Information Window was opened, you can perform confirmation and deletion operations. If the original window was displayed in read-only status, the Diagnostic Information window is also opened in read-only status, and operations such as checking and deleting cannot be performed.

H5.2 Diagnostic Information window

The Diagnostic Information window is shown as follows.

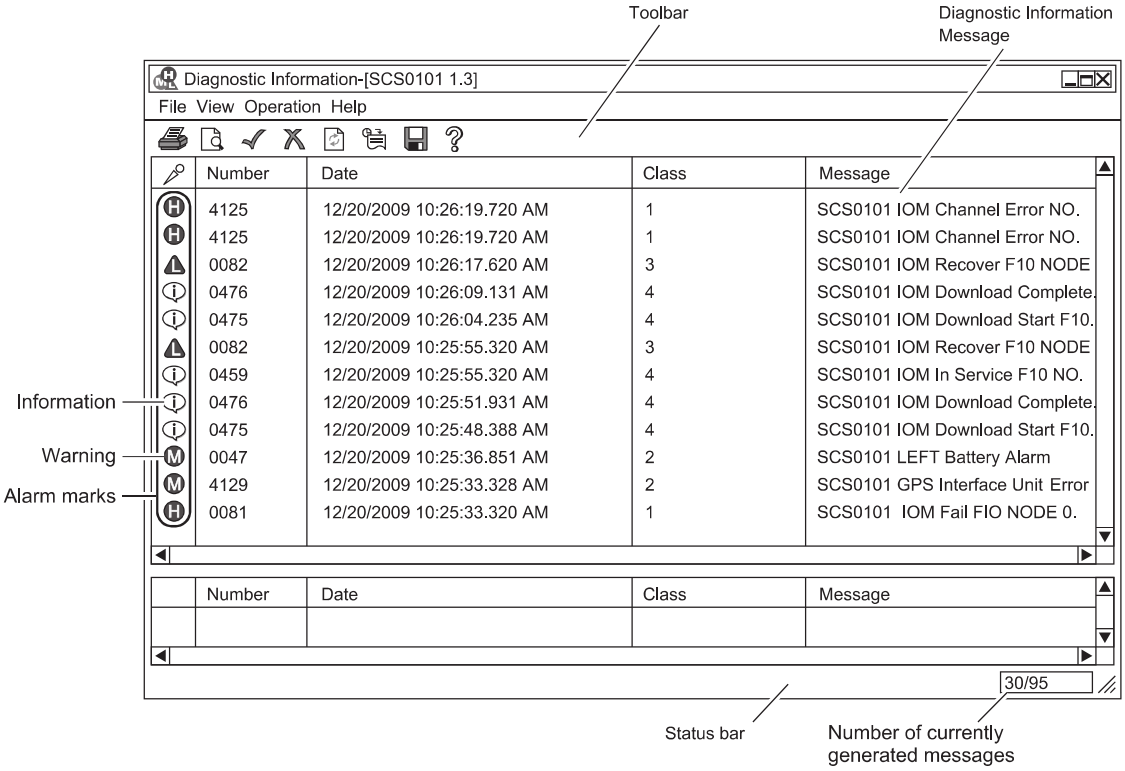


Figure H5.2-1 Diagnostic Information window

The components of the window are explained next.

Toolbar

The following buttons are provided on the toolbar.

Table H5.2-1 Toolbar buttons

Button	Name	Description
	Print	Print diagnostic information messages.
	Print preview	Display print preview.
	Acknowledgement	Acknowledge diagnostic information messages.
	Deletion	Delete diagnostic information messages.
	Update	Update diagnostic information message display.
	Historical	Divide the window and display deleted messages in the lower part (historical display).
	Save	Save diagnostic information messages in CSV format.
	Help	Display help related to the selected diagnostic information message.

Status bar

The status bar shows the number of currently displayed diagnostic information message and the total number of generated messages in the following format:

- Last number of the currently displayed diagnostic information messages/total number of generated diagnostic information messages

Configuration of diagnostic information message

A diagnostic information message consists of the following items.

Table H5.2-2 Items displayed in the Diagnostic Information window

Displayed item	Description
Alarm mark	Mark corresponding to the alarm class
Number	Message number
Time of occurrence	The time when a message occurred
Class	Alarm class determined within an SCS based on the diagnostic status
Message	Diagnostic Information message

IMPORTANT

- With the Diagnostic Information window open and if the number of Diagnostic Information messages of SCS to be displayed exceeds 5000, there are cases where old Diagnostic Information messages remain undeleted. If this occurs, click the [Refresh] button on the tool bar or re-display the Diagnostic Information window.
- Diagnostic Information window shows the messages acquired from the SCS memory by SENG and the messages sent to SENG by the SCS. After the window is displayed, SENG starts acquiring messages from the SCS memory (About 15 messages per second). The messages acquired and sent by the SCS after the window display are listed on top of the list, i.e., the list is not in chronological order. To sort the list based on the time, use the Sort function in the Diagnostic Information window. If you re-display the window after all the Diagnostic Information is collected, the list is displayed in chronological order.

Categories of diagnostic information messages

There are two message categories: warning (including recovery) and information. Diagnostic information messages included in the information category are only notified to the user, for example, they include messages that do not notify recovery messages and messages notifying the number of variables being locked by the forcing function.

Alarm mark display and diagnostic information message display color

The alarm marks attached to diagnostic information messages vary depending on the alarm class: the alarm marks flash as long as the messages have not been acknowledged and remain illuminated once the messages have been acknowledged. The character strings for diagnostic information messages (number, time of occurrence, class and message) are displayed in different colors according to the alarm class. The background color and text color can be specified using Setup Tool.

Table H5.2-3 Message character colors

Alarm mark	Category	Alarm class	Character display color in diagnostic information messages
Ⓗ	Warning	1	Red
Ⓜ	Warning	2	Red
⚠	Warning	3	Green
ⓘ	Information	4	(*1)

*1: The color set as the text color of Setup Tool (the default color is black).

SEE ALSO For more information about setup tool, refer to:

A6.3, “Customization of the SCS Maintenance Support Tool window” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

Acquisition of diagnostic information messages

Open the Diagnostic Information window to acquire and display one by one from the oldest messages in the SCS.
Messages generated after opening the window are displayed when they are generated.

Updating diagnostic information messages

Click [Update] button on the toolbar of the Diagnostic Information window to refresh information related to diagnostic information messages and diagnostic information status; the information is acquired from the SCS again and the display is refreshed.

Sorting diagnostic information messages

Click one of the columns in the list view of the Diagnostic Information window to sort diagnostic information messages.
If you click a column once, the messages are sorted in the ascending order. If you click once again, the messages are sorted in the descending order.

For example, if you want a list of Diagnostic Information messages in reverse chronological order, click the [Date] column.

Historical display of diagnostic information messages

Clicking [Historical] button on the toolbar of the Diagnostic Information window split the Diagnostic Information window into two parts and the 10 most recently deleted diagnostic information messages will be displayed in the lower part. If you click [Historical] button again, the window split will be released and the display returns to the original.

Outputting diagnostic information messages to external files

Diagnostic information messages can be saved in files in CSV format.

H6. Monitoring by diagnostic information message

SCS sends diagnostic information messages for detected faults and for the operation on the safety functions to notify user of events.

You can confirm the time when a fault occurred and the outline of the cause of the fault by reading the information provided in the diagnostic information message.

Diagnostic information messages can be checked as system alarm on SENG and HIS.

H6.1 Notification of error level through diagnostic information messages

SCS generates a diagnostic information message to notify you that an error has occurred. You can view the diagnostic information messages on the HIS and SENG. However, if a fatal error occurs on an SCS, the CPU of SCS stops; in this case, some diagnostic information messages may not be sent. Diagnostic information messages contain information regarding the level of the error detected on the SCS.

Notification of error level and error status

The status of SCS errors is reported to users through diagnostic information messages. It is also reported to Application logic. The SCS notification process and details for each error level is shown as follows:

Table H6.1-1 Error level types and the error status notification process

Error level	Diagnostic Information Messages	Notification to application logic
Fatal error	Diagnostic information message may not be notified because the CPU stops.	Notification is not possible because the CPU is stopped.
Major error	The failure location, cause of error and other information are notified.	The error and output status is notified.
Minor error	The failure location, cause of error and other information are notified.	A representative error state is notified, instead of an individual error state. An application logic that utilizes this notification can be created.

SEE ALSO For more information about behavior upon the occurrence of an error, refer to:

G2., “Operations and recovery procedures during the SCS error occurrence” on page G2-1

Alarm classes and diagnostic information messages

Failures of devices and SCS operation information are notified to the user as diagnostic information messages. The user can obtain information about the time and location of the error occurrence as well as the error type from the messages.

- The SCS adds information of the alarm class based on the error level when sending a diagnostic information message. The SENG displays messages with color according to the alarm class.

Table H6.1-2 Alarm class

Alarm class	Correspondence with error level	Meaning of alarm class	Example
Class 1 (serious alarm)	Fatal error (*1) Major error	An error that may cause system shutdown occurs and immediate action by the user is required.	Error notification of IOM in single configuration.
Class 2 (minor alarm)	Minor error	Notification that requires prompt action by the user, such as hardware replacement and remedy of user operation mistakes although the functions for safety continue to work	• Notification of a error of an IOM on one side of the redundant configuration • Notification of variable lock status by the forcing function continuing for longer than the specified time • Alarm sent by the HKU

Continues on the next page

Table H6.1-2 Alarm class (Table continued)

Alarm class	Correspondence with error level	Meaning of alarm class	Example
Class 3 (light alarm)	-	Notification of recovery from an error	-
Class 4 (notification alarm)	-	Notification of status other than SCS errors to the user	Notification of change of the security level

*1: Because the CPU stops when a fatal error occurs, the system may fail to generate a diagnostic information message that indicates the error.

- The time displayed in a diagnostic information message is the time when the SCS detected an error. The minimum unit of time is millisecond.
- The time information set for an diagnostic information message has the same high accuracy as the time information set for SOE information.

SEE ALSO For more information about the alarm class added to diagnostic information messages, refer to:

Appendix 1., “Alarm Class” in Messages Reference Manual (IM 32P02B10-01EN)

H6.2 Acknowledging and deleting diagnostic information messages

Diagnostic information messages can be acknowledged and deleted on the toolbar of the Diagnostic Information window. If you acknowledge or delete a message, the information about the operation is written to the SCS.

Messages can be acknowledged/deleted individually or in a batch. The method of acknowledging/deleting messages can be specified using Setup Tool. During the plant operation, acknowledge or delete messages individually.

IMPORTANT

- In the Diagnostic information tab of the Setup tool, if you select [Group] to specify batch acknowledgement or batch deletion, all diagnostic information messages displayed in the screen become the target of the acknowledging/deleting operation. Do not use this setting in normal plant operation. Use it only temporarily when testing, and so on.
- If the data in the NVRAM (nonvolatile RAM) on the CPU module is initialized, or if the CPU module is replaced, be sure to restart the SENG. If not, there are cases where some messages remain unacknowledged or undeleted in the Diagnostic Information window.

SEE ALSO For more information about setup tool, refer to:

A6.3, “Customization of the SCS Maintenance Support Tool window” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

Operation to acknowledge or delete individual diagnostic information messages

Acknowledging and deleting the individual messages can be performed using the toolbar on the Diagnostic Information window.

Acknowledging individual message

In the Diagnostic Information window, select one diagnostic information message and click the [Acknowledgement] button; the Acknowledgement dialog box appears.
Click the [OK] button in the Acknowledgement dialog box to acknowledge.

The flashing of the alarm mark stops in the Diagnostic Information window.

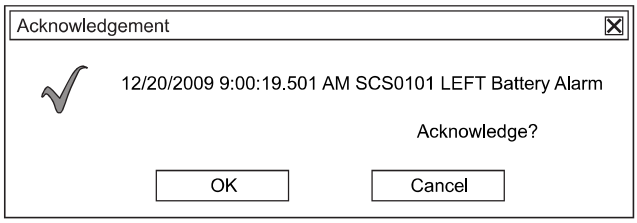


Figure H6.2-1 Acknowledgement dialog box

Deleting individual message

In the Diagnostic Information window, select one acknowledged diagnostic information message and click the [Deletion] button; the Deletion dialog box appears.
Click the [OK] button to delete the diagnostic information message.

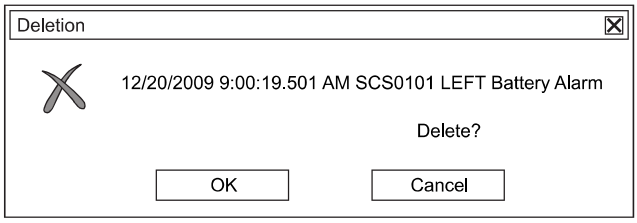


Figure H6.2-2 Deletion dialog box

Operation to acknowledge or delete all diagnostic information messages

To acknowledge or delete all the messages displayed in the screen in a batch, use the Diagnostic Information window.

IMPORTANT

Acknowledge or delete messages individually during normal plant operation; do not acknowledge or delete all messages in a batch.

Acknowledging all messages

Click the [Acknowledgement] button in the Diagnostic Information window; a warning dialog box appears. The warning dialog box appears only one time, when all messages are going to be acknowledged at once for the first time after opening the Diagnostic Information window.
If you click the [OK] button in the warning dialog box, all the diagnostic information messages displayed are acknowledged.

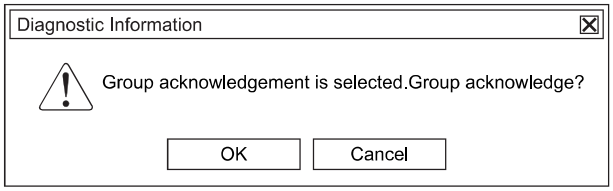


Figure H6.2-3 Warning dialog box displayed when acknowledging all messages

After you click the [Acknowledgement] button, the [Acknowledgement] button and [Deletion] button are disabled for two seconds.

Deleting all messages

Click the [Deletion] button in the Diagnostic Information window; a warning dialog box appears. The warning dialog box appears only one time, when all messages are going to be deleted at once for the first time after opening the Diagnostic Information window.
If you click the [OK] button in the warning dialog box, all the diagnostic information messages displayed and acknowledged are deleted. Diagnostic information messages that have not been acknowledged are not deleted.

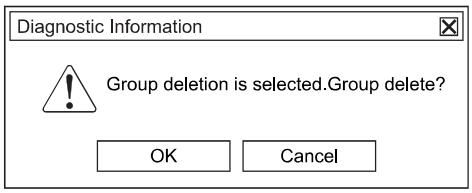


Figure H6.2-4 Warning dialog box displayed when deleting all messages

After you click the [Deletion] button, the [Acknowledgement] button and [Deletion] button are disabled for two seconds.

H6.3 Diagnostic information message help function

The diagnostic information message help function includes of the Help dialog box provided by the system and a user-defined action guide.

Help dialog box

The Help dialog box displays information stored in the Help files related to diagnostic information messages (message number, print example, meaning, cause, and so on) provided by the system.
The Help dialog box can be called in the following manners:

- Select the diagnostic information message in the Diagnostic Information window, and then click [Help] button on the toolbar.
- Double-click the diagnostic information message in the Diagnostic Information window. Help information related to the diagnostic information message you double-clicked is displayed in the Help dialog box.

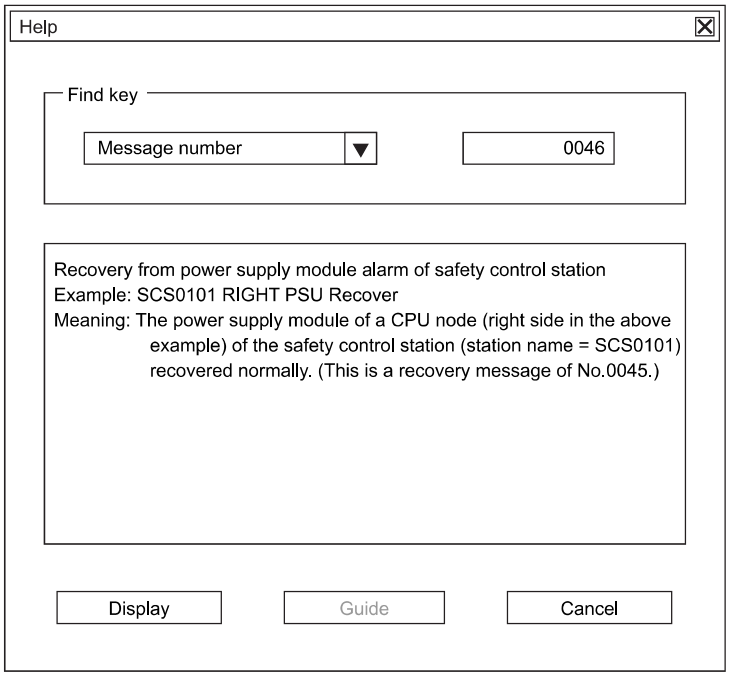


Figure H6.3-1 Help dialog box

- Guide
  The [Guide] button is enabled if a user-defined action guide has been defined. Click the [Guide] button to display the user-defined action guide corresponding to the relevant message number.

User-defined action guide

Engineers can share knowledge, information about actions to be taken, know-how's, etc. about the given situation by describing them in the user-defined action guide. It is also possible to attach images to the user-defined action guide.

Displaying a User-defined action guide

Click the [Guide] button in the Help dialog box to display the User-defined Action Guide.

Creating a User-defined action guide

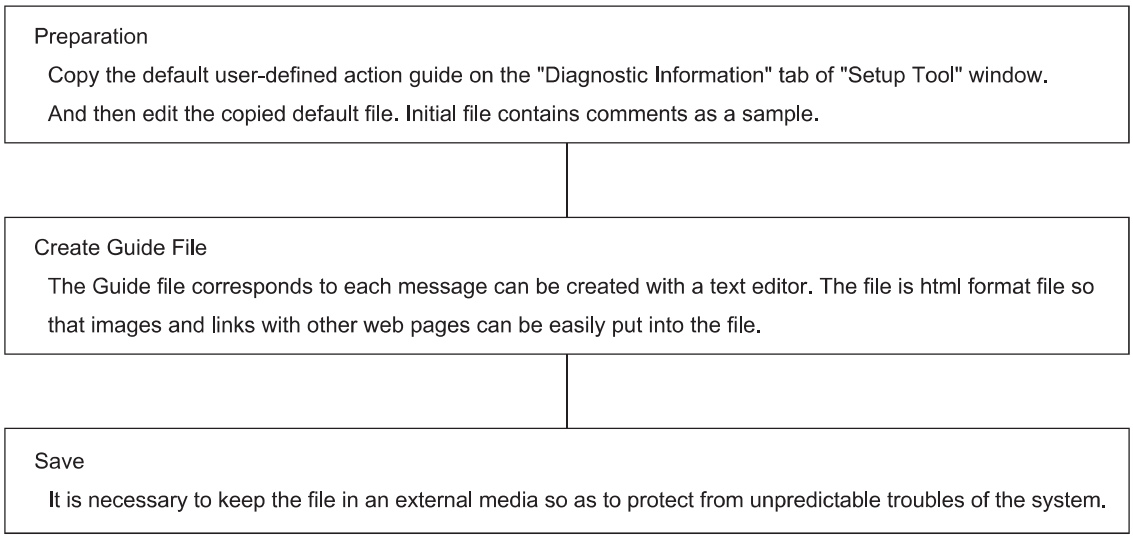


Figure H6.3-2 Create User-defined action guide

To display the file corresponding to the relevant message number by clicking the [Guide] button, it is necessary to label the created guide file with the corresponding message number. For example, (name="@0001") for message number 0001.
An example of a user-defined action guide file is shown as follows.

Table H6.3-1 User-defined action guide file

```
<b><a name="@0001"> Message Number: 1</a></b><BR>
CPU module error<BR>
Action: Replace the CPU module. <BR>
Memo: Please contact Mr. XX. xxx-xxxx-xxx
```

An example of display result of a user-defined action guide file is shown below.

Table H6.3-2 Display result of a User-defined action guide file

```
Message Number: 1
CPU module error
Action: Replace the CPU module.
Memo: Please contact Mr. XX. xxx-xxxx-xxx
```

H6.4 Printing diagnostic information messages

The diagnostic information message displayed in a window can be printed out. Click [Print] on the toolbar of the Diagnostic Information window. The class 1 and 2 alarms are printed out in red and class 3 and 4 alarms are printed out in black.
The information that is printed is described below.

Title

Window name, printing time and page number are printed on the title bar at the top of the page.

Header area

Search condition, message format and description of alarm condition are printed on the first page only.

Message

A printing image of a diagnostic information message is shown as follows.

12/20/2009 2:02:44 PM	page 1/1
Search condition	SCS0101 1.3
Format	Alarm mark,Message number,Date,Class,Message
Alarm mark	New Alarm:No mark,Acknowledged:A,Deleted:D

```
4129 12/20/2009 9:00:15.987 AM 2 SCS0101 GPS Interface Unit Error
0081 12/20/2009 9:00:15.980 AM 1 SCS0101 IOM Fail       FIO NODE 01 SLOT 05 Code = 5103
0083 12/20/2009 9:00:15.980 AM 2 SCS0101 IOM Configuration Error FIO NODE 01 SLOT 05
0081 12/20/2009 9:00:15.980 AM 1 SCS0101 IOM Fail       FIO NODE 01 SLOT 03 Code = 5103
0083 12/20/2009 9:00:15.980 AM 2 SCS0101 IOM Configuration Error FIO NODE 01 SLOT 03
0081 12/20/2009 9:00:15.980 AM 1 SCS0101 IOM Fail       FIO NODE 01 SLOT 01 Code = 5103
0083 12/20/2009 9:00:15.980 AM 2 SCS0101 IOM Configuration Error FIO NODE 01 SLOT 01
0451 12/20/2009 9:00:00.465 AM 2 SCS0101 LEFT       Control
0005 12/20/2009 9:00:00.465 AM 2 SCS0101 Power ON (Cold Start)
```

Figure H6.4-1 Printing image of diagnostic information messages

H7. Vnet/IP bus status

This chapter explains how to check the Vnet/IP bus communication status

Overview of Vnet/IP bus status

On the SCS State Management window of the SCS Maintenance Support Tool of SENG, the bus communication status of the SCSs in a domain can be displayed. Using an application logic with the control bus status indicator function block (SYS_NETST) can output the bus error alarm to external alarm lamps for notification.

If integrated with CENTUM system, statuses of all stations of all the domains connected to the Vnet/IP network as well the routing devices among the domains can be displayed. Vnet/IP bus status is displayed in the Network Status Display dialog box of the CENTUM HIS. When the bus status changes, a system alarm message will be generated and output to the HIS.

IMPORTANT

When the network switches are connected in a ring topology, even if one of the cables connecting between the switches is disconnected, the Vnet/IP bus status remain normal and no bus error system alarm will be issued.

To be notified of a ring status, you need to build an FCS application that uses the ring status signals from the network switches.

TIP

For more information about how to build such an FCS application, contact YOKOGAWA.

Elements of the Vnet/IP bus status

The Vnet/IP bus status shows the communication status of the stations in all domains connected to the Vnet/IP network as well as the devices (such as Layer 3 switches) connecting domains.

The Vnet/IP bus status consists of the following three elements:

- Bus status in own domain
- Communication status of devices connected between domains
- Bus statuses of other domains

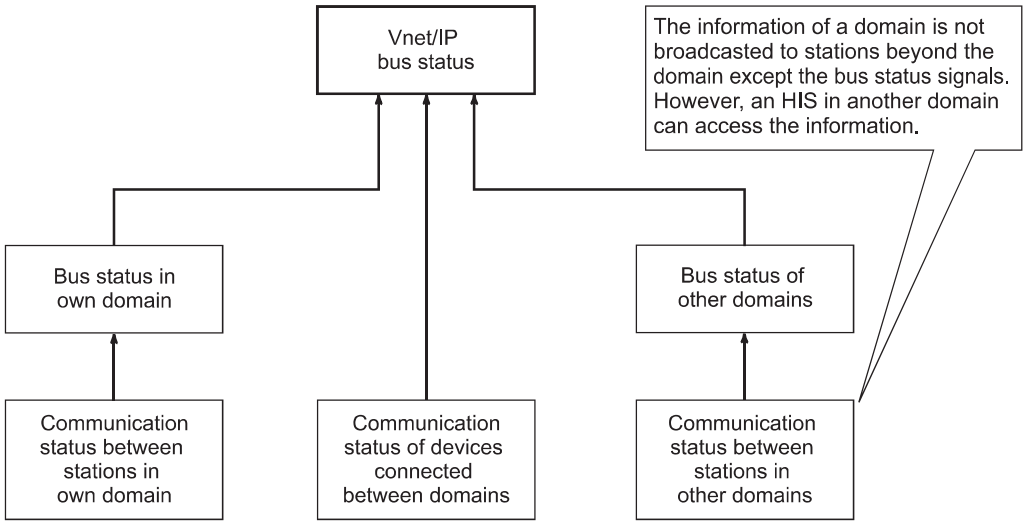


Figure H7-1 Elements of the Vnet/IP bus status

Displaying the station communication status of a domain

Each station in a Vnet/IP domain diagnoses bus statuses mutually using bus 1 and bus 2.

Communication statuses for a station are shown as follows. A station with duplex CPU modules has four types of communication status. The “control side station” mentioned here includes non-redundant stations such as SENG, HIS, and SCS with single CPU configuration.

- Control side communication status between stations
- Communication status when the control side station communicates with the standby side station
- Communication status when the standby side station communicates with the control side station
- Standby side communication status between the stations

Based on this diagnostic information the communication statuses of all stations in a domain can be displayed on the HIS Network Status Display dialog box.

Bus status in a domain

The bus status in a domain is created from the communication status among stations in each domain. If the bus status shows abnormality, the meaning varies with the type of failure:

- Either bus failure (either bus 1 or bus 2)
  When either bus 1 or bus 2 encounters communication error, the status of the bus will be indicated as abnormal.
- Both bus failure (both bus 1 and bus 2)
  If both buses encounter errors, the first one will be indicated as abnormal. Failure of both buses cannot be indicated.

TIP

If both buses are failed to communicate with a specific station, it will be indicated as the station failure, and the bus status will not be indicated as abnormal.

Communication statuses of devices connecting domains

The Vnet/IP domains communicate with each other using bus 1 and bus 2 and the communication status can be monitored. On the HIS Network Status Display dialog box, the communication statuses of devices on different domains can be displayed.

The bus status of one domain is broadcasted to all stations in all domains through the communication between domains.

Priority of the Vnet/IP bus status

The Vnet/IP bus status represents a summary of all communication statuses in the following order:

- Bus Status in Own Domain
  If the bus status of own domain is abnormal, it is reflected in the Vnet/IP bus status. In case of either bus failure, the status of the failed bus is handled as abnormal. In case of both bus failures, only the status of the bus in which abnormality is detected first is handled as abnormal.
- Communication Statuses of Devices Connecting Domains
  While the bus status of own domain is normal, the communication statuses of devices connecting domains are reflected in the Vnet/IP bus status. In case of either bus failure, the status of the failed bus is handled as abnormal. In case of both bus failures, only the status of the bus in which abnormality is detected first is handled as abnormal.
- Bus Statuses of Other Domains
  If the communication statuses of all devices connecting domains are normal, the bus statuses of other domains are reflected in the Vnet/IP bus status. However, even if a different bus is abnormal in different domains, the Vnet/IP bus statuses of both buses are not handled as abnormal, and only the status of the bus in which abnormality is detected first is handled as abnormal.

I. Maintenance

This section describes the procedures and precautions when maintaining ProSafe-RS devices and field devices, and how to set the system time. It also describes the tools that you can use during maintenance.

I1. Maintenance of devices

You must follow the procedures, precautions and all other information specified in this section with care and consideration when maintaining the ProSafe-RS equipment, software or field devices.

Before starting the maintenance work of devices, you need to take prior measures to avoid impact on the field devices due to maintenance. You can use the forcing function and override function for the prior measures and maintenance.

I1.1 Utilizing the forcing and override functions during maintenance

For the purpose of SCS maintenance, it may be necessary to fix or forcibly change the input/output values or values used in application logics. In such cases, the forcing and override functions can be used.

Forcing allows fixing channel input/output values of I/O modules (locking values) from the SCS Manager of SENG and forcibly changing the values (setting values). The following items are the targets of forcing.

- Input/output channels of AIO/DIO modules
- Subsystem communication data
- Safety subsystem communication data
- Variable included in application logic
- Inter-SCS safety communication data
- SCS link transmission data

In addition, it is possible to monitor the lock status in the application logics and forcibly cancel the lock status by using system function blocks (SYS_FORCE, SYS_FORCE_LT, SYS_FORCE_BD, SYS_FORCE_SC, SYS_FORCE_SF).

In the case of integration with CENTUM, variable values can be set by overriding them from HIS.

The following table shows the difference between forcing and override.

Table I1.1-1 Difference between forcing and override

Items where there is a difference between the two functions	Forcing	Override
Purpose	Maintenance of SCS and debugging of applications that are done through SENG	Maintenance of SCS through HIS in the CENTUM Integration Structure
SCS Security Level	The security level has to be set to 1 or 0.	An override is executable when the security level is 2.
Necessity of Programming	Programming is not necessary.	Application logic needs to be programmed with override function blocks.
Designation of output values	Output values can be specified in the I/O Lock Window, etc.	When an override is activated during execution of application, the preprogrammed value is output as an overridden value.
Conditions for locking a variable	Whether or not forcing can be performed depends on the SCS security level.	A program can be written that enables and disables override by using a mechanical key switch or other means.

I1.1.1 Override

In the CENTUM Integration structure, I/O values can be set to a specified value that is different from the actual I/O value by operation from HIS while the system is controlled normally by SCS. This operation is called override.

Override can be executed at an SCS security level of 2.

Executing override requires to create application logic with the override FB.

- There are two types of override FBs. One type is grouping override FB which can handle override actions in a group. The other is override FB which does not handle override in a group.
- If the total number of override FBs and grouping override FBs in the ready state for overriding exceeds the limit specified by the SYS_OVR function block, a diagnostic information message is issued to inform user of it.
- If the total number of overridden override FBs and grouping override FBs exceeds the limit specified beforehand by the SYS_OVR function block, a diagnostic information message is issued to inform user of it.
- If the duration in the ready state for overriding exceeds the limit specified beforehand by the SYS_OVR function block, a diagnostic information message is issued to inform user of it.
- If the duration of override exceeds the limit specified beforehand by the SYS_OVR function block, a diagnostic information message is issued to inform user of it.
- Using the SYS_OVR FB can forcefully cancel override for all variables.

SEE ALSO For more information about details on managing the override FBs, refer to:

B4.5, “Status management of function blocks used for override” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

I1.1.2 Utilization of the forcing function in SCS maintenance

The forcing function can be used for the following purposes, after all wiring is completed but before the start of actual operation, as well as during maintenance after starting the actual operation.

- Disconnection of Input/Output Modules
- Maintenance of Input/Output Channels
- Prevention of nuisance tripping caused by inter-SCS safety communication during online change downloading or offline downloading

SEE ALSO For more information about prevention of nuisance tripping caused by inter-SCS safety communication during online change downloading or offline downloading, refer to:

"■ Locking Inter-SCS safety communication and SCS link transmission data at online change" on page E1-27

■ Precautions for forcing functions

IMPORTANT

If you lock any internal variable in SCSP3/SCSL2/SCSP2, the application runtime becomes longer, that is, the CPU load increases. You should lock internal variables for engineering and maintenance purposes only.

- When physical data of an output channel are changed by forcing, consider possible effects on the field before performing forcing.
- During forcing, you should avoid conflict with the override operation from HIS.
  Check the output values of the SYS_OVR function block to see whether any overridden instances and instances in a status where they can be overridden exist.

  Check the diagnostic information messages indicating that the switch input of an override FB was turned ON and the diagnostic information messages showing that values were overridden, and make sure not to affect the same loop unintentionally.
- When displaying variable names in a system alarm, no more than 80 single-byte characters can be displayed. Choose variable names that do not exceed this maximum length, so that variables can be identified when locking/unlocking forcing and overriding.

SEE ALSO For more information about CPU load when internal variables are locked, refer to:

A7.3, "Locking of internal variables and performance in SCSP3/SCSL2/SCSP2" on page A7-10

■ Example of procedure for setting data with forcing

1. Set the security level of SCS to 1.
   Check that the security level of SCS is set to 1 with the Diagnostic Information Message
2. Lock I/O variables or internal variables.
   Check that the names of the locked variables are correct with the Diagnostic Information Message.
3. Set a value to the I/O variables or internal variables.
   Check that the variable names and the data set are correct with the Diagnostic Information Message.

4. Check applications with the set data.
5. Set the I/O variables and the internal variables so as not to cause any effects on the applications when another value to the variables are unlocked.
   - Check that the variable names and the data set are correct with the Diagnostic Information Message.
   - Check that the logical data of I/O variables are the same as the physical data and the data status is GOOD.
6. Unlock the I/O variables or the internal variables.
   Check that the unlocked variable names are correct with the Diagnostic Information Message.
7. Set the security level of SCS back to 2.
   Check that the security level of SCS is set to 2 with the Diagnostic Information Message

Locking for online change download

If online change of an I/O module and application logic is required while SCS is in operation, you must investigate whether there is a need to lock the I/O module to prevent a false trip, and lock the I/O module if necessary.

The following figure shows the procedure to lock the I/O module prior to online change download.

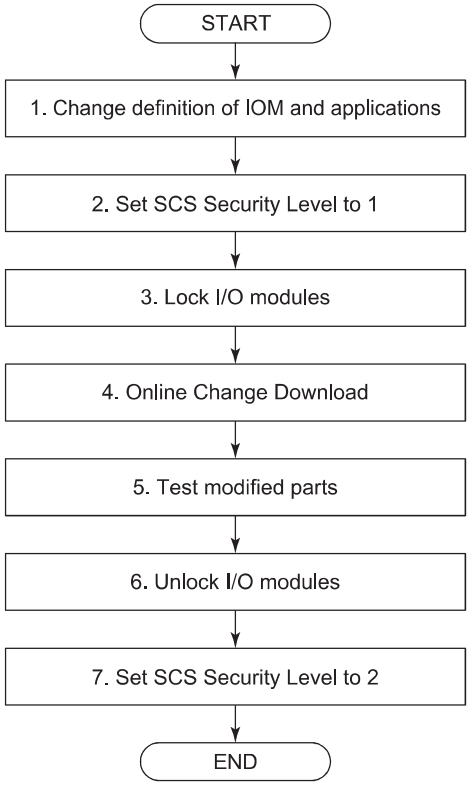


Figure I1.1.2-1 Procedure to lock I/O module prior to online change download

1. The engineer modifies the application and uses the Integrity Analyzer and Cross Reference Analyzer to analyze the modified application. If the application logic has also been modified, use the logic simulation test to check the modifications.
2. Change the SCS security level to Level 1 by using the SCS Security Level Operation Dialog.
3. Locking all I/O modules related to online change with the I/O Lock Window is recommended.

4. Perform an online change download.
5. Start the Debug mode for checking the modified parts.
6. Unlock all locked I/O modules with the I/O Lock Window. At this time, check with great care whether the output values are changed or not. Finish the Debug mode after unlocking the I/O modules.
7. Return the SCS security level to Level 2 by using the SCS Security Level Operation Dialog.

CAUTION

If you change some settings of an output module and perform an online change download to an SCS in R2.01 or earlier system program release number, you need to prevent the system from an unexpected shutdown when the value of the output module becomes 0. Preventive measure should be taken on the field device side in advance.

Maintenance of input/output channels

When performing maintenance of input/output channels, the forcing function is used to fix the values of the corresponding channels so as to prevent adverse effect on the operation of other applications.

Prevention of nuisance tripping when replacing a faulty module

If a channel of the input module fails in single configuration, the replacement of input module is required. The forcing function is used to fix input values of all channels to the current values to prevent nuisance tripping.

Similarly, if a channel of the output module fails in single configuration, the replacement of output module is required. The forcing function is used to fix the data status of all channels of the output module to the current values to prevent nuisance tripping in other output modules that refer to this channel.

Prevention of nuisance tripping due to online change download

When downloading online changes to the application logic or input/output modules, the forcing function is used to fix output values of all channels that may be influenced by this change, in order to prevent nuisance tripping.

In downloading online changes to an input/output module online, the forcing function is used to fix the input/output values of all channels of the corresponding input/output module to the current values in order to prevent nuisance tripping.

CAUTION

- For the output modules targeted for online change download, field bypasses are required so as to prevent plant shutdown.
- In online change download of output modules, if the channel status of the module is used as a reference by another output module, the channel of another output module may mistakenly generate a trip signal. To prevent this, the output modules linked to the online-changed module should be locked during online maintenance.

Prevention of nuisance tripping due to Inter-SCS safety communication errors at download

Nuisance tripping due to inter-SCS safety communication errors can be prevented by locking inter-SCS safety communication when performing online change download and offline download.

CAUTION

Be sure to check that LD (Logical Data) and PD (Physical Data) match when unlocking after the completion of download operation.

Unlocking in the status where LD and PD do not match may cause nuisance tripping.

At online change download

In the case of online change download, launch the Inter-SCS Communication Lock Window from an SCS project in which online change download is to be performed, and then lock stations on the producing and consuming sides. Nuisance tripping caused by online changes can be prevented.

Using Inter-SCS safety communication data lock function at offline download

When executing offline download of the producer SCS of inter-SCS safety communication, it is possible to prevent false trips caused by the offline download by locking inter-SCS safety communication at the consumer stations of the inter-SCS safety communication.
An overview of the locking and the procedure for executing offline download is described as follows.

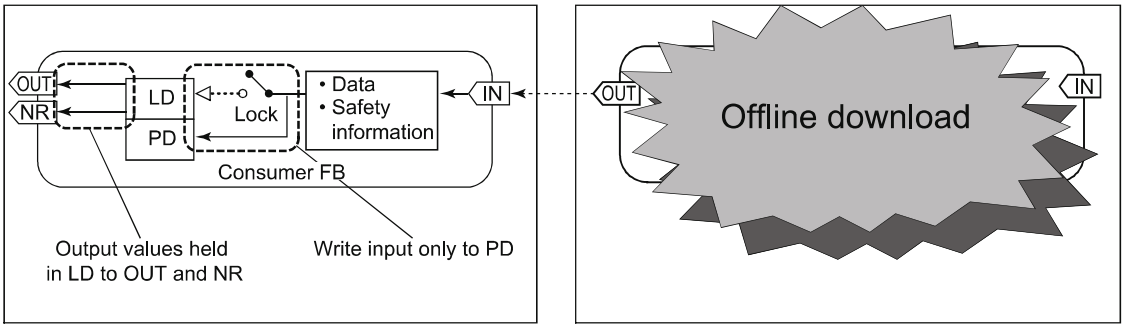


Figure I1.1.2-2 Example of locking Inter-SCS safety communication at offline download

1. Set the security level of SCS that receives inter-SCS safety communication data from the SCS that executes offline download to 1.
   Check that the security level of SCS is set to 1 with the diagnostic information messages.
2. Lock the consumer FB of the station where offline download is performed using the Inter-SCS Communication Lock window of the SCS that receives inter-SCS safety communication data.
   Check that inter-SCS safety communication has been locked with diagnostic information messages.
3. Set the security level of SCS that executes offline download to 0.
   Check that the security level of SCS is set to 0 with the diagnostic information messages.
4. Execute offline download.

5. Perform the output enable operation on the SCS that executed offline download.
   Check the output enabled status with diagnostic information messages.
6. Check that the logical data and physical data match and that the data status is GOOD in the Inter-SCS Communication Lock window of the SCS that receives inter-SCS safety communication data.
7. Unlock the consumer FB in the Inter-SCS Communication Lock window.
   Check that the inter-SCS safety communication is unlocked with diagnostic information messages.
8. Set the security level of the SCS that receives inter-SCS safety communication data to 2.
   Check that the security level of SCS is set to 2 with the diagnostic information messages.

I1.2 Maintenance for ProSafe-RS equipment

With SCS, procedures for maintenance vary depending on faults such as when dual-redundant CPU module or I/O module is replaced because of a fault or when a module in a single configuration fails. Take care for the maintenance procedure not to cause a nuisance tripping when maintenance is performed during running the plant.

Actions to be taken upon device errors

When you detect hardware errors by system alarms on HIS or alarm devices such as alarm lamps that indicate generation of diagnostic information messages, follow these steps:

1. Use the SCS Maintenance Support Tool of the SENG to identify the failed location and the cause for the error.
2. Repair the failed location.
   When a CPU module or I/O module of an SCS stops, you may be required to replace the module. Replace the module by following the procedure and precautions specified in the user's manual.
3. Confirm that all hardware devices are working properly either from the SCS State Management window or by ensuring that the alarm devices have been reset.

Precautions for ProSafe-RS device maintenance

During the maintenance of ProSafe-RS devices, you must be careful because the devices behave as follows:

- It takes about 8 seconds for an I/O module to get back to the normal state when it recovers from a failure such as when applying the power to I/O modules.
- When executing the APC operation for dual-redundant SCS, a COPY message is issued twice.
- When one power supply module of the "CPU node" fails, not only the CPU node but also I/O node 1 generates a signal that indicates failure of one power supply module. As a result, two diagnostic information messages are issued.

Workflow of CPU module maintenance

This section describes the workflow of CPU module maintenance. Before replacing the CPU module, read a whole description to understand the workflow of the maintenance and the precautions.

The procedure to be taken when the CPU module fails varies depending on whether the CPU module is of single configuration or dual-redundant configuration.

In addition, for the stand-alone ProSafe-RS system, you may need to clear the CPU module setting information before replacing the CPU module. For the CENTUM integration system, you may need to download the information of Domain Properties after replacing the CPU module. For detailed procedure, refer to the link included in each description.

Workflow of CPU module failure (Single configuration)

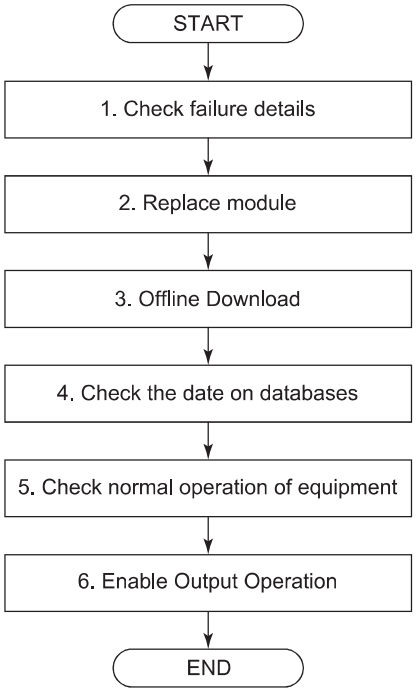


Figure I1.2-1 CPU module failure (Single configuration)

1. The engineer starts the SCS State Management window from SENG of the SCS where a fault occurs and confirms the diagnostic information message. Confirm the measures against the fault with the Help Dialog of Diagnostic Information Message and determine whether to replace the CPU module.
2. If the module needs to be replaced as a result of the step 1, the maintenance personnel removes the failed CPU module from the node and installs a new CPU module. Follow the instruction in the link included at the end of this section when you replace the CPU module.
3. The engineer executes master database offline download from SENG. (If downloading to the CPU module has been executed even once, the last application remains in the flash memory of the CPU module. Be sure to execute master database offline download after replacing the CPU module.)
4. The CPU module starts after the download is completed.
   The engineer displays date of each database for POU DB, Variable DB, System DB and Integration DB on the Database Validity Check Tool, when the SCS is in waiting mode, to confirm that latest version is loaded.
5. The maintenance personnel confirm that the CPU module has started normally from the SCS State Management window in SENG or from LED of the CPU module. Furthermore, the engineer confirms that all SCS equipment are in normal state with the SCS State Management window.
6. The maintenance personnel perform the enable output operation from the SCS State Management window.

SEE ALSO

For more information about details of Output enable operation, refer to:

C8., “Output enable operation” on page C8-1

For more information about procedure required before and after replacing CPU module, refer to:

I6., “Procedures and precautions for adding or replacing Vnet/IP devices” on page I6-1

Workflow of CPU module failure (Dual-redundant configuration)

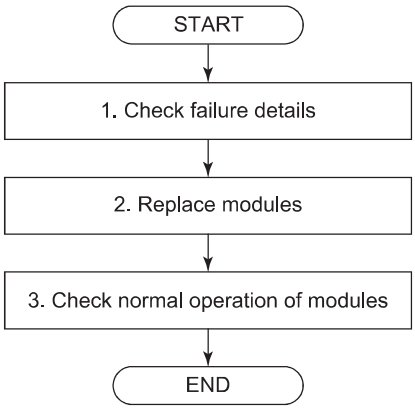


Figure I1.2-2 CPU module failure (Dual-redundant configuration)

1. The engineer starts the SCS State Management window from SENG of the SCS where a fault occurs and confirms the diagnostic information message. Confirm the measures against the fault with the Help Dialog of Diagnostic Information Message and determine whether to replace the CPU module.
2. If the module needs to be replaced as a result of the step 1, the maintenance personnel removes the failed CPU module (on standby) from the node and installs a new CPU module. Follow the instruction in the link included at the end of this section when you replace the CPU module.
3. When the new CPU module is installed, programs and databases of the CPU module on control are automatically copied to the new CPU module. The maintenance personnel confirms with LED of the module or the SCS State Management window in SENG that the module has started normally.

IMPORTANT

Do not pull out the CPU module online and turn off the power while the module is writing to the flash memory. Whether the CPU module is writing can be confirmed by using LED of the CPU module.

SEE ALSO For more information about procedure required before and after replacing CPU module, refer to:

I6., “Procedures and precautions for adding or replacing Vnet/IP devices” on page I6-1

Password setting in replacing CPU

- If CPU is in dual-redundant configuration and you must replace the standby side, there is no need to re-set passwords for the work. After the Standby side is replaced, the passwords for changing Security level stored in the control side are automatically copied to the standby side.
- In a single CPU configuration, if the CPU is replaced and programs remain in the memory on the new CPU module, the CPU starts. Its Operating mode is Waiting, so output value of application logic is not output to the field.
  In this status, press Reset switch, stop the CPU, and offline download the master database. After completion of the download and the CPU is started, set the passwords. The passwords in the memory on the CPU module is initialized, so there is no need to enter the previous passwords.

- In a single CPU configuration, if the CPU is replaced and no program remains in the CPU memory on the new CPU module, the CPU is in a halt status. In that status, offline downloads the master database. After completion of the download and the CPU is started, set the passwords. There is no need to enter the previous passwords.

Maintenance of I/O modules

If the I/O module generates an error, you must use the IOM Report to investigate the cause before commencing troubleshooting. Maintenance procedures vary depending on the error code reported in the IOM Report.

SEE ALSO For more information about details on IOM Report, refer to:

H3., “Checking diagnostic information by using IOM Report” on page H3-1

Overview of I/O module maintenance procedure and precautions

The precautions and maintenance procedure when an I/O module has stopped are described as follows:

IMPORTANT

Observe the following precautions when one of the redundant pair of I/O modules has failed and you must fix it:

- If you pull out the failed I/O module, do not insert it again.
- When you replace the I/O module, do not insert an I/O module that is not assured as normal.

If you do not observe these precautions, the field side may be adversely affected if the inserted module is faulty.

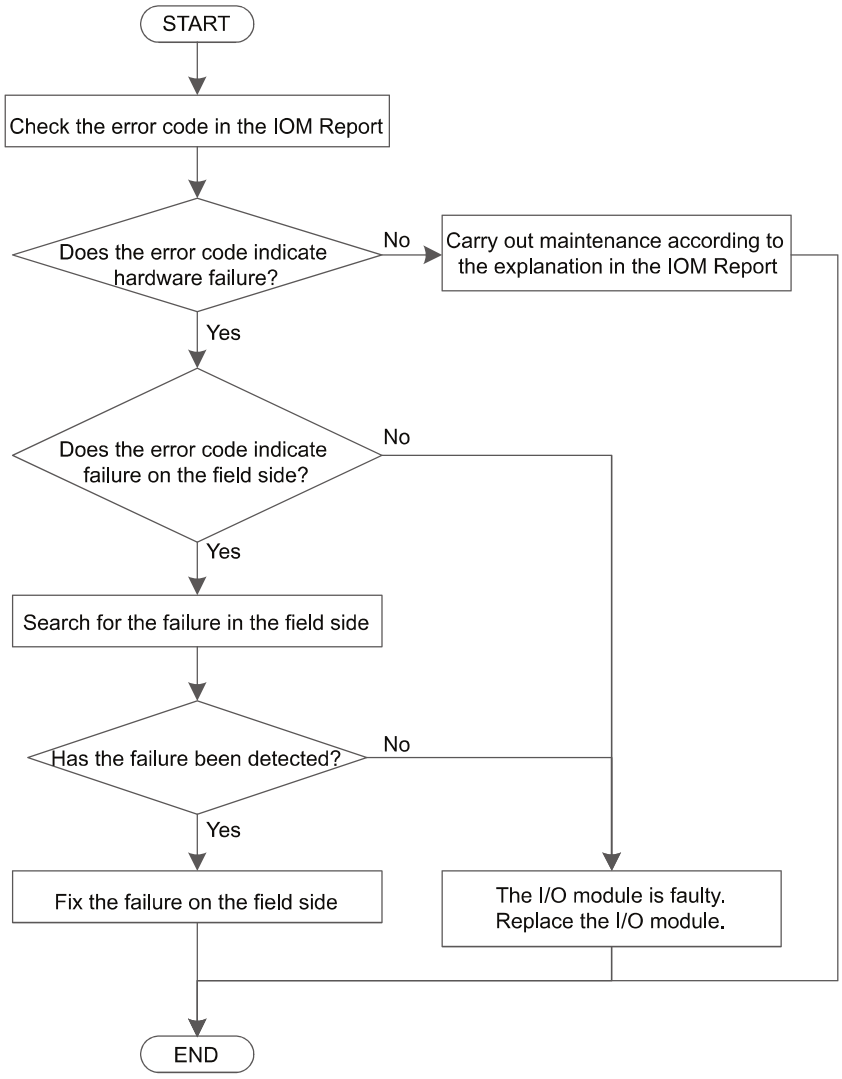


Figure I1.2-3 I/O module maintenance procedures

SEE ALSO For more information about procedures for replacing the I/O Module, refer to:

"● Procedure for when the I/O module is faulty" on page I1-15

● Hardware failure error codes possibly caused by failures on the field side

The cause of the I/O module stopping can be checked in the IOM Report.

Even when the IOM Report shows an error code for hardware failure, the module may have actually stopped due to a failure on the field side, not a hardware error. If the IOM Report shows any of the following error codes, follow the troubleshooting procedure that applies when there is a possibility of a failure on the field side.

Table I1.2-1 IOM Report error codes possibly caused by failures on the field side

Code (hexadecimal)	Display	Description
0101 5502 0401 5502 (*1)	Output Readback Error	An error has been detected in the readback process for the output value. Check the field wiring of the analog output module for any abnormality such as inter-channel short circuit, and also confirm that the total resistance of all connected cables and devices does not exceed the allowable output load resistance of the output module, which is specified in the General Specifications (GS).
0101 5504 0401 5504	Output Channel Stuck at ON	A failure that the output channel is unable to change from ON to OFF has been detected. Check if there are any field wiring errors such as inter-channel short circuit.
0107 5507 0407 5507 (*1)	IOM Channel Fail	There have been some errors with the channel area of the input/output module. Check if there is any input of a signal value at a level between ON and OFF or chattering.

*1: For a channel failure, the error code and the error status will vary depending on whether the I/O module is of a duplex configuration or a single configuration.
- The upper error code is for a redundantly configured I/O module, while the lower error code is for a non-redundantly configured I/O module.
- If the input/output module is in a redundant configuration, this error will be an IOM Fail error. In a non-redundant configuration, the error will occur only to the failed channel.

Troubleshooting procedure when error is possibly caused by failures on the field side

If the IOM Report shows an error code that may be caused by a failure on the field side, follow these steps to restore the I/O module:

1. Search for wiring error or failure on the field side.
2. Repair the wiring error or failure on the field side to remove the cause of error corresponding to the error code.

TIP

If the cause of error is not on the field side, it is a hardware failure of the I/O module. Follow the procedure for when the I/O module is faulty.

3. Reset the I/O module that has stopped. Perform one of the following actions based on the system program release number of the SCS:
   - SCS system program release number is R3.02.00 or later

     Select the stopped I/O module and run IOM download manually. IOM reset is performed at the same time.

TIP

IOM is reset only if the AIO/DIO modules are in single configuration or they are the standby side of duplex configuration and if their HRDY lamp is off.

   - SCS system program release number is earlier than R3.02.00
     Pull out and insert the I/O module again. IOM reset is performed.
4. Check that the I/O module has recovered to normal in the SCS State Management window.
5. After an output module has recovered to normal, perform the output enable operation in the SCS State Management window.

SEE ALSO

For more information about IOM Download operations, refer to:

I4.6, “IOM Download tool” on page I4-80

Procedure for when the I/O module is faulty

Follow these steps when you have determined that there is an I/O module hardware failure:

1. Replace the faulty I/O module with one that operates normally.
2. After replacing the module, perform IOM download.
   However, when replacing the standby side of the redundant AIO/DIO modules, you do not need to execute the IOM download manually if the automatic IOM download is enabled in the SCS.

TIP

To enable automatic IOM download, you must set "Automatic IOM Download" to Enable in the SCS Constants Builder. Once it's set, the SCS automatically downloads configuration information from the control side module to the standby side module after the module is replaced.

3. Confirm that the replaced module is working properly either from the SCS State Management window or by ensuring that the alarm device has been reset.

SEE ALSO

For more information about how to replace the I/O module of the FIO node, refer to:

E4.7, “Replacing FIO I/O modules” in Hardware User's Guide (IM 32P06C10-01EN)

For more information about how to replace the I/O module of the N-IO node, refer to:

E5.3, “Replacing N-IO I/O modules” in Hardware User's Guide (IM 32P06C10-01EN)

Replacing a fire and gas communication module

Follow these steps when you have determined that there is a fire and gas communication module failure:

1. In the Communication I/O Lock Window, lock the fire and gas communication module.
2. Remove the failed fire and gas communication module form the node.
3. Insert a new fire and gas communication module in the node.
4. Perform IOM download.
5. In the Communication I/O Lock Window, check that the physical data status of the input data is GOOD.
6. Release the lock of the fire and gas communication module.

Procedures for changing the single/redundant specification of AIO/DIO modules installed on the FIO node

Follow these steps to offline change the single/redundant specification of AIO/DIO modules installed on the FIO node:

1. Disconnect the I/O cables (or terminal blocks) of the modules.
2. If you change two adjacent existing single modules to dual-redundant configuration, pull out one of the modules and insert it again.
3. Perform either of the following operations:
   Operations differ, depending on the engineering method.
   - If you are performing RS original engineering, change the definition by using I/O Wiring View and perform offline download.
   - If you are performing I/O list engineering, change the definition by using the IOM Definition Editor and perform offline download.
4. Connect the I/O cables (or terminal blocks).

Maintenance specific to N-IO nodes

You can perform the following maintenance tasks for N-IO nodes through the NIU maintenance port.

Periodic maintenance

Follow these steps to stop the SCU for the periodic maintenance of the plant and perform maintenance of N-IO nodes:

IMPORTANT

Set the security level to 1 or below before stopping the SCU, and then enable the maintenance port.

1. Enable the maintenance port of NIU in the target NIU nodes for maintenance.
2. Perform maintenance work of N-IO nodes, which have an NIU with an enabled maintenance port, by using the FieldMate Validator.
3. Disable the maintenance port of the target NIU after the completion of the maintenance work, and prohibit access from the maintenance port.
4. Verify that the maintenance ports of all NIU are disabled on SENG or HIS.

Adding N-IO nodes

Follow these steps to add N-IO nodes to the existing SCU:

1. Configure the node numbers of the N-ESB bus and optical ESB bus in all NIUs that have been supplied.
2. Use the FieldMate Validator to perform the loop checking, to check the functionalities and to configure the field device and N-IO I/O module under the N-IO node.
3. Connect to the existing SCU.
4. Disable the maintenance port of the extended NIU to prohibit access from the maintenance port.
5. Verify that the maintenance ports of all NIU are disabled on SENG or HIS.

Replacing a faulty N-ESB bus module

When one of the redundant N-ESB bus modules installed on NIU has failed, follow these steps to replace the faulty module:

1. Remove the faulty N-ESB bus module from NIU.
2. Insert the replacement N-ESB bus module to NIU.
3. Disable the maintenance port of the replacement N-ESB bus module to prohibit access from the maintenance port.
   Note that the maintenance port of NIU is automatically disabled if the security level is 2. However, if the maintenance port is in the maintenance status, the maintenance port retains the maintenance status and does not go into the disabled state even when the security level is set to 2.
4. Verify that the maintenance ports of all NIU are disabled on SENG or HIS.

Behaviors during N-IO node maintenance mode and recovery procedure

This section describes the system behaviors when an N-IO node is placed in maintenance mode and the procedure when the node recovers from the maintenance mode.

Operations during the maintenance mode

When an N-IO node is placed in maintenance mode, the system operates as follows:

- CPU processing
  The CPU sets the "input value at error occurrence," which is the value pre-defined in an I/O parameter by the user, for all input channels of the I/O modules that were installed in the N-IO node (which is in maintenance mode), and changes the data status to "BAD".

  The CPU sets the fail-safe value, which is the value pre-defined in an I/O parameter by the user, on the physical data for all output channels of the I/O modules that were installed in the N-IO node (which is in maintenance mode), and places the output channels in output disable status. It also changes the data status to "BAD".

  The CPU stops the data update to the I/O module that was installed in the N-IO node (which is in maintenance mode).

- Error notification
  It sends a message when the safety control station status is changed to the maintenance mode. It also sends a message on recovery that the maintenance mode of the safety control station status is canceled.

Recovery procedures

1. Switch the N-IO node from the maintenance mode to the online mode.
   Data status returns to GOOD and a maintenance mode cancellation message is sent.

   Execute following operation if the output module is installed in the N-IO node.

2. From the SCS Maintenance Support Tool of the SENG, run the output enable operation.
   Output values from the application logic are output.

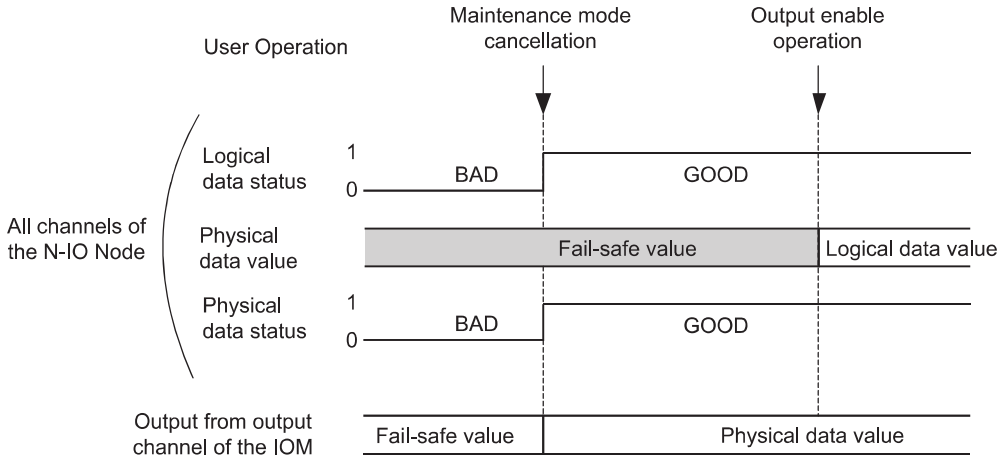


Figure I1.2-4 Operations during maintenance mode cancellation

TIP

Effective range of recovery operations are limited to I/O modules of N-IO nodes that are connected to NIU in maintenance mode. Other NIUs that are connected to the target NIU in a daisy chain are not affected.

I1.3 Maintenance of field devices

For maintenance of field devices, it is necessary to take measures on the ProSafe-RS side so as not to cause a nuisance tripping due to field signals changed by maintenance.
The procedure for maintenance of filed devices is as follows.

1. Take required bypass to avoid generating a nuisance tripping due to maintenance.
2. Perform maintenance of field devices.
3. Test field devices.
4. Remove the bypass taken in step 1.

In ProSafe-RS, I/O values related to maintenance are locked with either of the following ways to avoid a nuisance tripping during maintenance.

- Forcing from SENG
- Override from HIS in CENTUM Integration Structure

I1.4 Maintenance of field wireless system devices

The section describes the procedures for maintenance of field wireless system devices.

IMPORTANT

When you download settings to YFGW410 by using FWMC, the YFGW410, wireless field devices on the field wireless subnet, or GS01 may restart, depending on the changes made to the YFGW410 settings. Therefore, use FWMC to find the devices that will restart and lock the relevant communication data before you download settings to YFGW410 from FWMC.

A field wireless subnet refers to a field wireless network that consists of YFGW510 and its subordinate wireless field devices.

The devices that restart and the data to be locked are as follows:

- When YFGW410 will restart
  All communication data that is obtained through the YFGW410 that will restart
- When wireless field devices on the field wireless subnet will restart
  All communication data that travels through the wireless field devices that will restart
- When GS01 will restart
  All communication data of the GS01 that will restart

SEE ALSO

For more information about how to configure YFGW410 and functions of the field wireless management console (FWMC), refer to:

YFGW410 Field Wireless Management Station (IM 01W02D01-01EN)

For more information about tasks related to field wireless system devices, refer to:

YFGW410 Field Wireless Management Station Read Me First (IM 01W02D01-11EN)

I1.4.1 Changing the setting information of YFGW410

You must change the setting information of YFGW410 when you change the name of the PROFINET network name, the update cycle or Watch Dog Timer for PROFINET communication, or the PROFINET modules to assign to the YFGW410.

To change the setting information of YFGW410, you must download configuration data to YFGW410 by using FWMC.

When to download should be decided through discussion with the engineer of the field wireless system.

Follow these steps to change the setting information of YFGW410.

1. Reflect the information of the YFGW410 onto the safety communication I/O list, PROFINET definitions, communication definitions, and applications, etc.
2. In the Communication I/O Lock Window, lock the S2LP131 connected to the YFGW410.
3. Perform an online change download with SCS Manager.
4. In the Communication I/O Lock Window, check that the physical data status of the input data is GOOD.
5. Release the lock of the S2LP131 connected to the YFGW410.

I1.4.2 Replacing YFGW410

To replace YFGW410 when one of a redundant pair of YFGW410 has failed, you do not need to provide any curing measure on the ProSafe-RS system side.

When both of a redundant pair of YFGW410 have failed, you can replace the YFGW410 by using the same procedure that you follow to replace a non-redundant YFGW410.

Follow these steps to replace a non-redundant YFGW410:

1. In the Communication I/O Lock Window, lock all of the communication definitions applicable to the YFGW410 being replaced.
2. Remove the failed YFGW410.
3. Attach the new YFGW410.
4. In the Communication I/O Lock Window, check that the physical data status of the input data is GOOD.
5. Release the lock of all of the communication definitions applicable to the YFGW410 that was replaced.

I1.4.3 Replacing YFGW510

To replace YFGW510 when one YFGW510 in a DuoCast configuration has failed, you do not need to provide any curing measure on the ProSafe-RS system side.

When both YFGW510 in a DuoCast configuration have failed, you can replace the YFGW510 by using the same procedure that you follow to replace a non-DuoCast YFGW510.

Follow these steps to replace a non-DuoCast YFGW510:

1. In the Communication I/O Lock Window, lock the communications for all communication definitions relevant to the YFGW510 to be replaced.
2. Remove the failed YFGW510.
3. Install a new YFGW510.
4. In the Communication I/O Lock Window, check that the physical data status of the input data is GOOD.
5. Release the lock of the communications for all communication definitions relevant to the YFGW510 that was replaced.

I1.4.4 Removing YFGW510

When you remove YFGW510, you must download configuration data to the relevant YFGW410 by using FWMC.

When to download should be decided through discussion with the engineer of the field wireless system.

When you make a maintenance plan, consider that it will take a maximum of two minutes after S2LP131 is stopped until it restarts in order to update PROFINET definitions.

Follow these steps to remove a YFGW510:

1. Delete YFGW510 from the safety communication I/O list, PROFINET definitions, communication definitions, and other lists and definitions, and application logic.
2. In the Communication I/O Lock Window, lock the S2LP131 connected to the YFGW510 being removed.

TIP

The reason for locking S2LP131 is because S2LP131 will be restarted to delete the relevant communication definitions. The communication definitions must be deleted for the following reasons:

- It is assumed that GS01 is also removed when YFGW510 is removed. If GS01 is removed, communication definitions for gas concentration or other data must be deleted.
- Even if GS01 is not removed, deletion of communication definitions is required if the system is obtaining BBR_STATUS of YFGW510.

3. Remove the YFGW510.
4. Using SCS Manager, execute an online change download.
5. In the Communication I/O Lock Window, check that the physical data status of the input data is GOOD.
6. Release the lock of the S2LP131.

SEE ALSO

For more information about how to change PROFINET definitions, refer to:

E1.5.2, “Applying settings by using PROFINET Configurator” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

I1.4.5 Adding YFGW510

When you add YFGW510, you must download configuration data to the relevant YFGW410 by using FWMC.

When to download should be decided through discussion with the engineer of the field wireless system.

When you make a maintenance plan, consider that it will take a maximum of two minutes after S2LP131 is stopped until it restarts in order to update PROFINET definitions.

Follow these steps to add a YFGW510.

1. Reflect the information of the YFGW510 being added onto the safety communication I/O list, PROFINET definitions, communication definitions, and application logic.
2. Before you execute an online change download to the SCS, in the Communication I/O Lock Window, lock the S2LP131 that is connected to the YFGW510 being added.
3. Using SCS Manager, execute an online change download.
4. In the Communication I/O Lock Window, confirm that the physical data status of the input data is normal.
5. Release the lock of the S2LP131.

SEE ALSO For more information about how to change PROFINET definitions, refer to:

E1.5.2, “Applying settings by using PROFINET Configurator” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

I1.4.6 Changing the setting information (F-Parameter, communication period) of GS01

The setting information of GS01 includes F-Parameter, which needs to be downloaded to S2LP131, and the communication period, which needs to be downloaded to YFGW410.

TIP When you change only F-Parameters, downloading of configuration data to YFGW410 is not required.

Changing F-Parameter

Follow these steps to change the F-Parameter:

1. Reflect the setting information of GS01 onto the safety communication I/O list, PROFINET definitions, and other lists and definitions.
2. In the Communication I/O Lock Window, lock the S2LP131 connected to the GS01.
3. Using SCS Manager, execute an online change download.
4. When the online change download is complete, check that the physical data status of the input data is GOOD in the Communication I/O Lock Window.
5. Unlock the S2LP131 that you locked in step 2.

Changing the wireless communication period

When you change the wireless communication period, you must download configuration data to the relevant YFGW410 by using FWMC.

When to download should be decided through discussion with the engineer of the field wireless system.

TIP When you change the wireless communication period, you do not need to make any changes in the engineering of ProSafe-RS. Downloading to SCS and S2LP131 is not required, either.

Follow these steps to change the wireless communication period:

1. Before you download the configuration data to YFGW410 by using FWMC, lock the communication data of the GS01 for which you are changing the communication period from the Communication I/O Lock Window.
2. When the downloading of configuration data from FWMC is complete, check that the physical data status of the input data is GOOD in the Communication I/O Lock Window.
3. Unlock the communication data of GS01 that you locked in step 1.

I1.4.7 Replacing GS01

When you replace GS01, you must download configuration data to the relevant YFGW410 by using FWMC.

When to download should be decided through discussion with the engineer of the field wireless system.

Follow these steps to replace GS01 when it has failed:

1. In the Communication I/O Lock Window, lock all of the communication definitions applicable to the GS01 being replaced.
2. Remove the failed GS01.
3. Attach the new GS01.
4. In the Communication I/O Lock Window, check that the physical data status of the input data is GOOD.
5. Release the lock of all of the communication definitions applicable to the GS01 that was replaced.

I1.4.8 Removing GS01

When you replace GS01, you must download configuration data to the relevant YFGW410 by using FWMC.

When to download should be decided through discussion with the engineer of the field wireless system.

Follow these steps to remove a GS01:

1. Delete GS01 from the safety communication I/O list, PROFINET definitions, communication definitions, and other lists and definitions, and application logic.
2. In the Communication I/O Lock Window, lock the S2LP131 connected to the GS01 being removed.
3. Remove the GS01.
4. Perform an online change download with SCS Manager.
5. When the online change download is complete, check that the physical data status of the input data is GOOD in the Communication I/O Lock Window.
6. Release the lock of the S2LP131.

I1.4.9 Adding GS01

Follow these steps to add a GS01. This section explains the procedures for using a user-defined FB to which GASDTR, PSI_I, and PSI_R as shown in the following figure are embedded as an application for monitoring the gas concentration of GS01 and using the same user-defined FB with the GS01 being added as well.

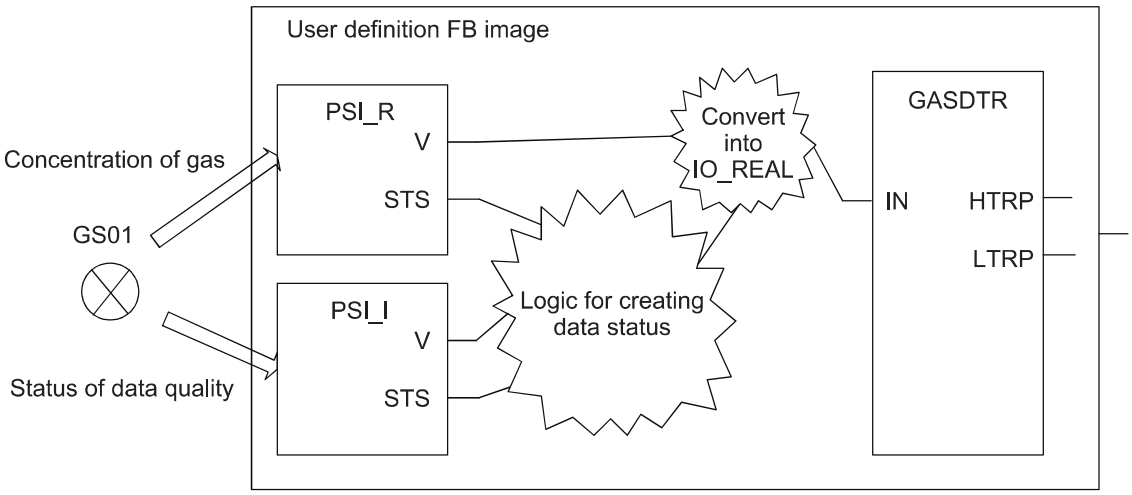


Figure I1.4.9-1 Image of user-defined FB

The flow of tasks is as follows. However, specific operation procedures vary depending on whether or not iDefine is used.

To add GS01, you must configure YFGW410 as well as ProSafe-RS. Therefore, you must download configuration data to the relevant YFGW410 by using FWMC.

When to download should be decided through discussion with the engineer of the field wireless system.

The wok flow for adding GS01 is described below. If you add GS01 without following this work flow, the operation starts from the state where GASDTR has latched a trip signal.

1. Perform an online download onto the SCS for a POU other than the one including the GS01 being added.
2. Perform a forcing of the communication definition being added.
3. Perform an online download onto the SCS for the POU that includes the GS01.

SEE ALSO For more information about how to configure YFGW410, refer to:

- YFGW410 Field Wireless Management Station Read Me First (IM 01W02D01-11EN)
- YFGW410 Field Wireless Management Station (IM 01W02D01-01EN)

When using iDefine

Follow these steps when adding a GS01 by using iDefine. Step 1 is a task to be performed before heading to the site. Step 2 and subsequent steps are tasks performed at the site.

1. Export the SCS project by using AD Organizer.
2. Import the SCS project by using AD Organizer.
   In the SCS Import dialog box, select the [Exclude SCS Project Files] check box and perform the import.
3. Using RS Generation Manager, select the check box for [Skip the reflection of program POUs] and then click [Build].

4. In the Communication I/O Lock Window of SCS Manager, lock the S2LP131 including the GS01 being added.
   Lock all inputs in bulk or lock all communication definitions.
5. Perform an online change download with SCS Manager.
   Release the lock of the existing GS01 at any time after this upon confirming that communication has been restored.
6. In the Communication I/O Lock Window of SCS Manager, run a forcing of the communication data wired to the GS01 being added into a normal value. At this time, check that the gas concentration with the physical data in the Communication I/O Lock Window is within a normal range.
   The values subjected to forcing are as follows:
   - PSI_R.v (gas concentration): A value which does not exceed the High/Low trip levels of GASDTR
   - PSI_R.sts (status of fire and gas communication): TRUE
   - PSI_I.v (data quality status of gas concentration): 128
   - PSI_I.sts (status of fire and gas communication): TRUE
7. Click [Build] in RS Generation Manager.
   A build process runs for the SCS project.
8. Using Project Comparing Tool, check that the following projects match.
   - The original SCS project exported in step 1
   - The SCS project that is to be downloaded at the site
9. Perform an SCS online change download by using SCS Manager.
10. Release the lock for every communication definition for which communication with the added GS01 has been restored.

SEE ALSO

For more information about exporting SCS projects, refer to:

"■ Importing SCS projects" on page E2-5

For more information about how to operate RS Generation Manager, refer to:

D4., "Overview of RS generation" on page D4-1

For more information about how to operate Communication I/O Lock Window, refer to:

F8.11, "Communication I/O Lock window" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about Project Comparing Tool, refer to:

F6.3, "Comparing two SCS projects" in Engineer's Reference Manual (IM 32P04B10-01EN)

■ When not using iDefine

Follow these steps when adding a GS01 without using iDefine. Procedure 1 is a task to be performed before heading to the site. Procedure 2 and beyond are tasks performed at the site.

1. Perform the following tasks:
   - Export the SCS project by using AD Organizer.
   - Using SCS Manager, export the CSV file of Dictionary, the CSV file of Tag Name Builder, and the PXF file of the entire project.
2. Perform the following tasks:
   - Import the SCS project by using AD Organizer. In the SCS Import dialog box, select the [Exclude SCS Project Files] check box and perform the import.

- Using SCS Manager, import Dictionary.
- Using RS Generation Manager, run the build process.

3. In the Communication I/O Lock Window of SCS Manager, lock the S2LP131 including the GS01 being added.
   Lock all inputs in bulk or lock all communication definitions.
4. Perform an online change download by using SCS Manager.
   Release the lock of the existing GS01 at any time after this upon confirming that communication has been restored.
5. In the Communication I/O Lock Window of SCS Manager, run a forcing of the communication definition wired to the GS01 being added.
   The values subjected to forcing are as follows:
   - PSI_R.v (gas concentration): A value that does not exceed the setting level for the HI and LO trips of GASDTR
   - PSI_R.sts (status of fire and gas communication): TRUE
   - PSI_I.v (data quality status of gas concentration): 128
   - PSI_I.sts (status of fire and gas communication): TRUE
6. Using SCS Manager, import the PXF file of the entire project.
7. Using SCS Manager, import the CSV file of Tag Name Builder.
8. Perform the build by using SCS Manager.
9. Using Project Comparing Tool, check that the following projects match.
   - The original SCS project exported in step 1
   - The SCS project that is to be downloaded at the site
10. Perform an SCS online change download by using SCS Manager.
11. Release the lock for every communication definition for which communication with the added GS01 has been restored.

SEE ALSO

For more information about exporting SCS projects, refer to:

"■ Importing SCS projects" on page E2-5

For more information about how to operate RS Generation Manager, refer to:

D4., "Overview of RS generation" on page D4-1

For more information about how to operate Communication I/O Lock Window, refer to:

F8.11, "Communication I/O Lock window" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about Project Comparing Tool, refer to:

F6.3, "Comparing two SCS projects" in Engineer's Reference Manual (IM 32P04B10-01EN)

I2. Maintenance of the system

This section explains proof tests necessary for maintenance of the system and tests for improving the rate of operation.

I2.1 Proof test

Proof tests are periodic tests for verifying that the functions of safety loops consisting of sensors, logic solvers, and final elements are functioning without failure.

This section explains the proof test for logic solvers (ProSafe-RS).

The subject of this proof test is the operation of each channel of input/output modules.

Change the input value or output value of each channel of the modules and check if the modules work as intended.

For dual-redundant configurations, conduct the check on both modules.

I2.2 Tests for improving the rate of operation

For dual-redundant configurations, check that the dual-redundant switchover takes place properly in order to improve the rate of operation. This section explains how to check the dual-redundant switchover of the CPU module and I/O modules.

Checking the dual-redundant switchover of the CPU module

1. Press the [START/STOP switch] on the front of the control-side CPU module once to stop it and make a switchover.
2. Press the [START/STOP switch] of the stopped CPU module again to restart it and place it in the standby mode.

SEE ALSO For more information about details on the START/STOP switch of the CPU module and the status display, refer to:

B4.2, “Processor module” in Hardware User's Guide (IM 32P06C10-01EN)

Checking the dual-redundant switchover of I/O modules

Using IOM Control Right Switching Tool, check the control right switchover of an AIO/DIO module in a dual-redundant configuration.

By using this tool, the AIO/DIO module on the control side will switch over to the standby side while the AIO/DIO module on the standby side will switch over to the control side.

This tool is launched from SENG.

SEE ALSO For more information about details on the IOM Control Right Switching Tool, refer to:

I4.7, “IOM Control Right Switching Tool” on page I4-83

I3. Setting system time

The system date and time can be set using the Adjust Time dialog box. The date and time specified in the Adjust Time dialog box are reflected on the SCS connected to the same domain and other SENGs. In the case of the CENTUM integration structure, the set date and time are also reflected on its FCS and HIS. Moreover, when multiple domains are connected through BCV or CGW and it so specified by the builder, the same date and time can be applied to the stations in the connected domains too.

The set date and time is applied to the following connected stations:

- Date/time of the local SENG (Windows date/time)
- Date/time of all SCS, FCS and HIS
- Date/time of other SENGs

If an HIS is connected, the time settings made on the HIS are applied to these stations as well.

IMPORTANT

- If Vnet/IP is applied as the control bus, using SNTP server standard time for time synchronization cannot change the system time from SENG and HIS.
- If V net is applied as the control bus, the Adjust Time dialog box should be used to set time regardless of what type of time synchronization is applied. When a V net network and a Vnet/IP network are connected through a V net router that is earlier than style S3, if the V net router system time transfer is set to [Transfer lower], the system time cannot be changed from an SENG or HIS on the V net. Moreover, if multiple domains are connected together through BCV or CGW, and if the BCV system time transfer is set to [Transfer lower], or the CGW is set to [Receive System Time], the system time cannot be changed from an SENG or HIS in the lower level domain.

Adjust Time dialog box

Click [Time Setup] button on the toolbar of the SCS Status Overview window or the SCS State Management window. The Adjust Time dialog box appears.

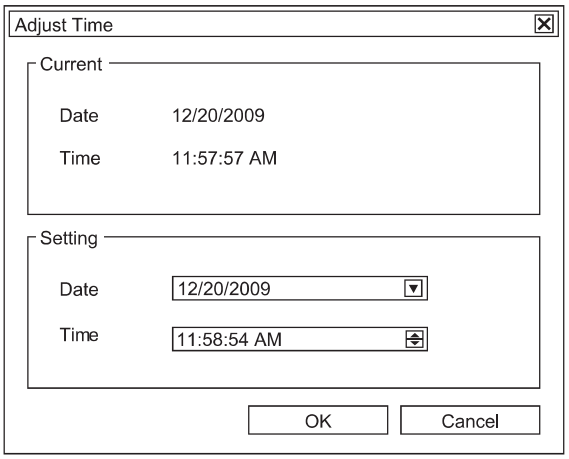


Figure I3-1 Adjust Time dialog box

The following items are displayed in the Adjust Time dialog box:

- Current
  The current system time is displayed in this area.

- Setting
  The system time can be set in this area.

How to set the system date and time

The system date and time can be adjusted using the spin boxes in the dialog box and then click the [OK] button. Click the [Cancel] button if you want to cancel the setting.
If you set the date/time, the date/time of the stations connected to the system are changed.
Note that the date/time format conforms to the Windows standard.

I4. Tools for operations and maintenance

You can use the following tools and functions for cause investigation when a system abnormality occurs, or while maintaining SCS devices.

- Forced I/O Viewer and Forced I/O Viewer Setup Tool
  You can use Forced I/O Viewer to collect and display the variables locked by using the forcing function.

  You can use Forced I/O Viewer Setup Tool to make the settings of the Forced I/O Viewer for collecting and displaying the information such as locked variables.
- Message Cache Tool
  You can use this tool for carrying out the collection settings of diagnostic information messages, which are displayed in the Diagnostic Information window or SOE Viewer.
- SOE Viewer
  You can use this tool to examine SOE events that are generated in the SCS.
- Master database offline download
  You can use this to perform offline download of the SENG master database to the SCS.
- NIU maintenance port setting tool
  You can use this tool for switching between the enable and disable status of the NIU maintenance port.
- IOM Download Tool
  You can use this tool to download the configuration information that is stored in the Master database to the I/O module.
- IOM Control Right Switching Tool
  You can use this tool for switching the control rights of AIO/DIO modules that are operating in a redundant configuration.

I4.1 Forced I/O Viewer function

Forced-I/O information is a collection of information such as variables that are locked in the Lock window of SENG by using the forcing function.

Forced I/O Viewer function is a function to display the forced-I/O information in a list. Forced-I/O information of multiple SCSs can be displayed collectively.

Forced I/O Viewer function consists of Forced I/O Viewer that displays the forced-I/O information and Forced I/O Viewer Setup Tool that makes the setting for collecting the forced-I/O information.

I4.1.1 Operation environment of Forced I/O Viewer function

This section describes the necessary licenses for using Forced I/O Viewer function and the operation environment such as conditions of SCS and SENG.

SEE ALSO

For more information about hardware requirements of the Forced I/O Viewer function, refer to:

A1.1, “Hardware requirements” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

For more information about software requirements of the Forced I/O Viewer function, refer to:

A1.2, “Software requirements” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

License

Forced I/O Viewer function runs in a computer that the following licenses has been assigned.

Table I4.1.1-1 Licenses necessary for Forced I/O Viewer function

Type	Name
RS4E5100	Safety System Engineering and Maintenance Function
RS4H2300	Forced I/O Viewer Package

SENG that the license of Safety System Engineering and Maintenance Function has been assigned can use Forced I/O Viewer Setup Tool and Forced I/O Viewer.

Computer that is connected to the control bus, such as HIS that the license of Forced I/O Viewer Package has been assigned can use Forced I/O Viewer.

IMPORTANT

Safety System Engineering and Maintenance Function and Forced I/O Viewer Package cannot be coexisted on the same computer.

TIP

To use Forced I/O Viewer in SENG, assign the license of Safety System Engineering and Maintenance Function instead of Forced I/O Viewer Package.

Conditions of SENG and SCS

The Forced I/O Viewer function runs in the following SENG and SCS.

For SCS that supports SIL 3

- SENG: SENG of software R4.05.00 or later
- SCS: SSC50, SSC57, SSC60, and S2SC70 of system program R4.05.00 or later

For SCS that supports SIL 2

- SENG: SENG of software R4.06.00 or later
- SCS: L1SC70 of system program R4.06.00 or later

I4.1.2 Forced-I/O information

Information, such as locked variables in various windows, that is displayed in Forced I/O Viewer is called forced-I/O information.

This section describes the display items of forced-I/O information.

Display items of forced-I/O information

The following forced-I/O information is displayed in the Forced I/O Viewer:

- Header
- Summary
- I/O Variables/Internal Variables
- SCS Link Transmission (sending and receiving)
- Inter-SCS Safety Communication (sending and receiving)
- Subsystem Communication
- Safety Subsystem Communication

In Forced I/O Viewer, a summary of forced-I/O information is displayed in brackets next to the item name of forced-I/O information. Detailed information about the forced-I/O information appears by expanding the item name of forced-I/O information.

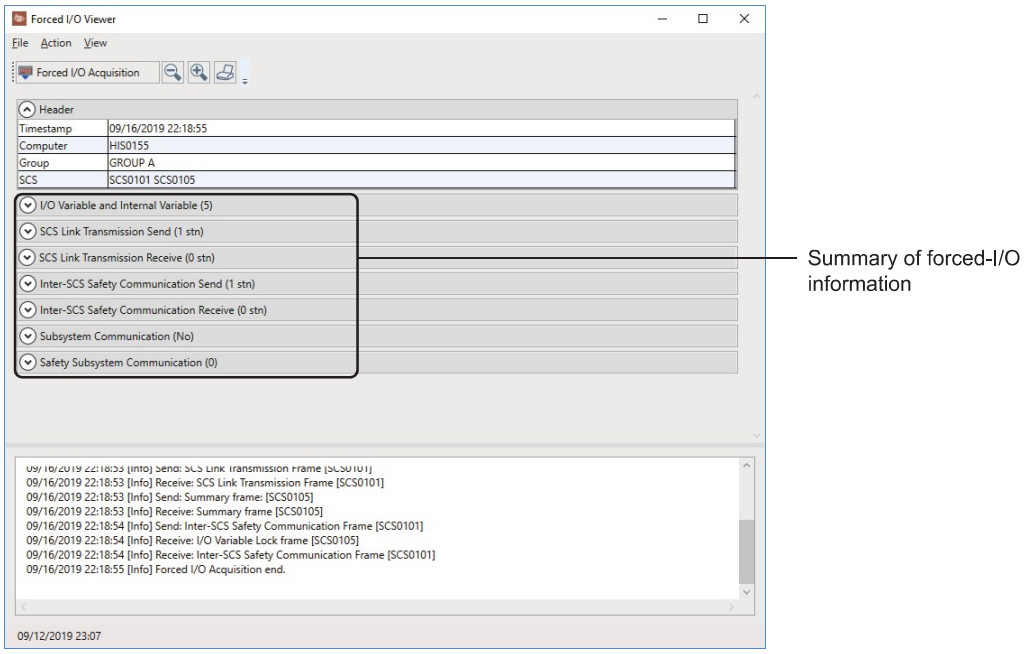


Figure I4.1.2-1 Summary of forced-I/O information

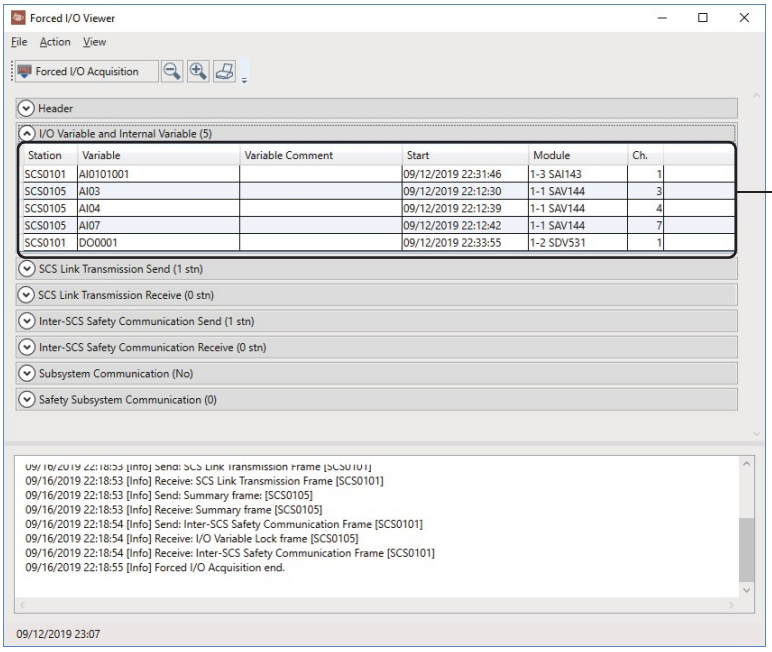


Figure I4.1.2-2 Detailed information of forced-I/O information

Header

The following table shows the header items of forced-I/O information.

Table I4.1.2-1 Header items of forced-I/O information

Item name	Description	Example
Timestamp	Date and time when the acquisition of forced-I/O information by Forced I/O Viewer was started	11/5/2019 19:30:10
Computer	Name of a computer that runs Forced I/O Viewer	HIS0164
Group	Name of a group where the forced-I/O information is acquired	Equipment 1
SCS	Station name of SCS that belongs to the group where the forced-I/O information is acquired	SCS0101 SCS0102

Summary

In the Summary of forced-I/O information, the number of locks and whether it is locked are displayed by each forced-I/O information. In the Summary, the forced-I/O information of multiple SCSs can be displayed collectively. The displayed number of locks is the total number of locked items. As for subsystem communication, whether it is locked or not is displayed. "Yes" is displayed when at least one subsystem communication is locked, and "No" is displayed when it is not locked.

Table I4.1.2-2 Items of Summary of forced-I/O information

Item name	Description
I/O Variable and Internal Variable	Total number of locked I/O variables and internal variables
SCS Link Transmission Send	Number of SCSs that have locked the sending data of SCS link transmission for local station
SCS Link Transmission Receive	Number of SCSs that have locked the receiving data of the SCS link transmission
Inter-SCS Safety Communication Send	Number of SCSs that have locked the sending data of inter-SCS safety communication for local station

Continues on the next page

Table I4.1.2-2 Items of Summary of forced-I/O information (Table continued)

Item name	Description
Inter-SCS Safety Communication Receive	Number of SCSs that have locked the receiving data of the inter-SCS safety communication
Subsystem Communication	Whether or not the subsystem communication is locked
Safety Subsystem Communication	Number of communication definitions locked in the safety subsystem communication

I/O Variable and Internal Variable

The I/O variable name and the internal variable name, which are locked from windows such as the I/O Lock window and the Dictionary View are displayed. The following table shows the items of I/O variable/internal variable.

Table I4.1.2-3 Items of I/O variable/internal variable of the forced-I/O information

Item name	Description	Example
Station	Station name of the locked SCS	SCS0101
Variable	I/O variable name and internal variable name	DO0001
Variable Comment	Comment entered for the variable	
Start	Date and time when the lock was started	11/5/2019 19:30:10
Module	I/O module name for the I/O variable (*1) (*2)	1-5 SDV531
Ch.	Channel number for the I/O variable (*1)	1

*1: This item is displayed for I/O variable.
*2: If it is FIO, the node number-slot number is added in front of the module name, and if it is N-IO, the node number-unit number-slot number is added.

SCS Link Transmission Send

The station name of SCS that have locked the sending data of the local station specified by using the SCS Link Transmission Lock window appears. The following table shows the SCS Link Transmission Send items.

Table I4.1.2-4 Items of SCS Link Transmission Send of the forced-I/O information

Item name	Description	Example
Station	Station name of the SCS that have locked the sending data	SCS0101
Instance	Instance name	sndb01
Instance Comment	Comment entered for the instance	
Start	Date and time when the lock was started	11/5/2019 19:30:10

SCS Link Transmission Receive

The station name of SCS that have locked the receiving data specified by using the SCS Link Transmission Lock window appears. The following table shows the SCS Link Transmission Receive items.

Table I4.1.2-5 Items of SCS Link Transmission Receive of the forced-I/O information

Item name	Description	Example
Station	Station name of the SCS that have locked the receiving data	SCS0101
Instance	Instance name	rcvi01

Continues on the next page

Table I4.1.2-5 Items of SCS Link Transmission Receive of the forced-I/O information (Table continued)

Item name	Description	Example
Instance Comment	Comment entered for the instance	
Start	Date and time when the lock was started	11/5/2019 19:30:10
Station (from)	Station name of the SCS from which received data is locked	SCS0102

Inter-SCS Safety Communication Send

Station name of SCS that have locked the sending data from the local station specified by using the Inter-SCS Communication Lock window appears. The following table shows the Inter-SCS Safety Communication Send items.

Table I4.1.2-6 Items of Inter-SCS Safety Communication Send of the forced-I/O information

Item name	Description	Example
Station	Station name of the SCS that have locked the sending data	SCS0101
Variable	Binding variable name	P0101001
Variable Comment	Comment entered for the binding variable	
Start	Date and time when the lock was started	11/5/2019 19:30:10
Instance	Instance name	PROD_R01

Inter-SCS Safety Communication Receive

Station name of the SCS that have locked the receiving data specified by using the Inter-SCS Communication Lock window appears. The following table shows the Inter-SCS Safety Communication Receive items.

Table I4.1.2-7 Display Items of Inter-SCS Safety Communication Receive of the forced-I/O information

Item name	Description	Example
Station	Station name of the SCS that have locked the receiving data	SCS0101
Variable	Binding variable name	C0102001
Variable Comment	Comment entered for the binding variable	
Start	Date and time when the lock was started	11/5/2019 19:30:10
Instance	Instance name	CONS_R01
Station (from)	Station name of the SCS from which received data is locked	SCS0102

Subsystem Communication

Communication module name that is locked by using the Communication I/O Lock window of subsystem communication mode appears. The following table shows the subsystem communication items.

Table I4.1.2-8 Items of subsystem communication of the forced-I/O information

Item name	Description	Example
Station	Station name of the SCS whose communication module is locked	SCS0101
Instance	Instance name	DI0000
Instance Comment	Comment entered for the instance	

Continues on the next page

Table I4.1.2-8 Items of subsystem communication of the forced-I/O information (Table continued)

Item name	Description	Example
Start	Date and time when the lock was started	11/5/2019 19:30:10
Module	Communication module name (*1)	3-1 ALR111

*1: Node number-slot number is added before the module name.

● Safety Subsystem Communication

PROFINET module name that is locked by using the Communication I/O Lock window of safety subsystem communication mode appears. The following table shows the safety subsystem communication items.

Table I4.1.2-9 Items of safety subsystem communication of the forced-I/O information

Item name	Description	Example
Station	Station name of the SCS whose communication module is locked	SCS0101
Instance	Instance name	DI0000
Instance Comment	Comment entered for the instance	
Start	Date and time when the lock was started	11/5/2019 19:30:10
Module	Communication module name (*1)	10-8 S2LP131
PN-Module	PROFINET module name	GS01_SAFE_RS

*1: Node number-slot number is added before the module name.

■ Displaying, printing, and saving the forced-I/O information

The forced-I/O information can be displayed in the main window of Forced I/O Viewer, and the displayed forced-I/O information can be printed and saved.

● Display

The forced-I/O information appears in the forced-I/O information display area of main window of Forced I/O Viewer. Each forced-I/O information item is displayed in tabular format. In this display, you can perform the following operations:

- Changing the order of items in the table
- Sorting the data of items in the table
- Changing the character size

SEE ALSO For more information about how to display the forced-I/O information, refer to:

"■ Step 1: Acquiring and displaying the forced-I/O information" on page I4-35

● Printing

Forced-I/O information displayed in the main window of Forced I/O Viewer can be printed. However, even if you change the order of items in the table in Forced I/O Viewer, it is not reflected in printing. The data is printed in the order in which they appear on the screen.

SEE ALSO For more information about how to print the forced-I/O information, refer to:

"■ Step 2: Printing the forced-I/O information" on page I4-36

Saving

Forced-I/O information displayed in the main window of Forced I/O Viewer can be saved in a CSV format file.

Even if you change the order of items in the table in Forced I/O Viewer, it is not reflected in the file. The data is saved in the order sorted by the mounting position.

SEE ALSO For more information about how to save the forced-I/O information, refer to:

"■ Step 3: Saving the forced-I/O information in a CSV format file" on page I4-37

I4.1.3 Grouping and registering SCS

By using Forced I/O Viewer Setup Tool, multiple SCSs can be grouped and registered.

By grouping and registering the SCSs, the forced-I/O information of all SCSs that belong to the group can be displayed collectively in the Forced I/O Viewer.

Specifications of grouping

The specifications of grouping are as follows:

- You can register multiple groups and give them unique names.
- The named groups are listed as options in Forced I/O Viewer. By selecting any group from the list, the forced-I/O information of SCSs that belong to the group can be displayed collectively.
- To list only the necessary groups as options in Forced I/O Viewer, you can assign groups to each computer that uses Forced I/O Viewer.
- One SCS can belong to multiple groups.
- One group can assign to multiple computers.
- Assignment of group cannot be changed for each user account of computer.

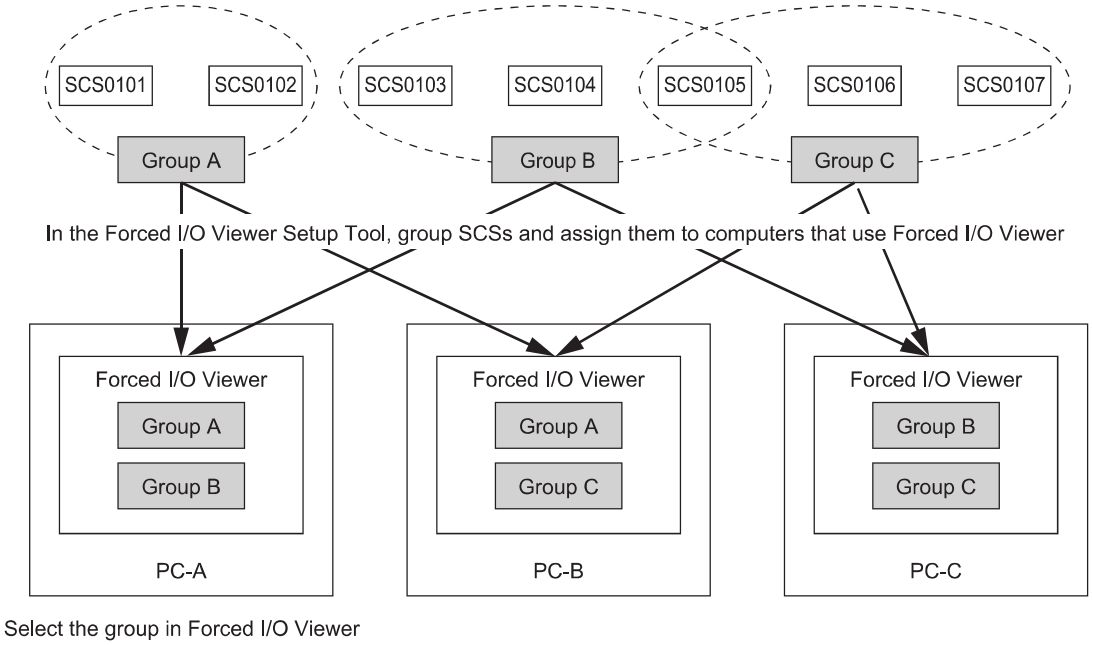


Figure I4.1.3-1 Example of SCS group

The number of groups and the specifications for the group name that can be registered in Forced I/O Viewer Setup Tool are as follows:

- The number of groups that can be registered: 32 groups
- Characters that can be used for the group name: Single-byte alphanumeric characters, space, under score, and hyphen

  The first character must be an alphabet and the last character must be other than a space.
- The number of characters for the group name: Up to 32 characters

I4.1.4 Distributing a registration file and SCS projects

To display the forced-I/O information, information that is obtained from SCS and the SCS project in SENG are required. The computer where the SCS projects are saved might be turned off, so files that saved the registered information necessary for obtaining the forced-I/O information by using Forced I/O Viewer Setup Tool (Registration file) and the SCS projects must be distributed to the computer that uses the Forced I/O Viewer.

The following figure shows the example of how to distribute the SCS projects.

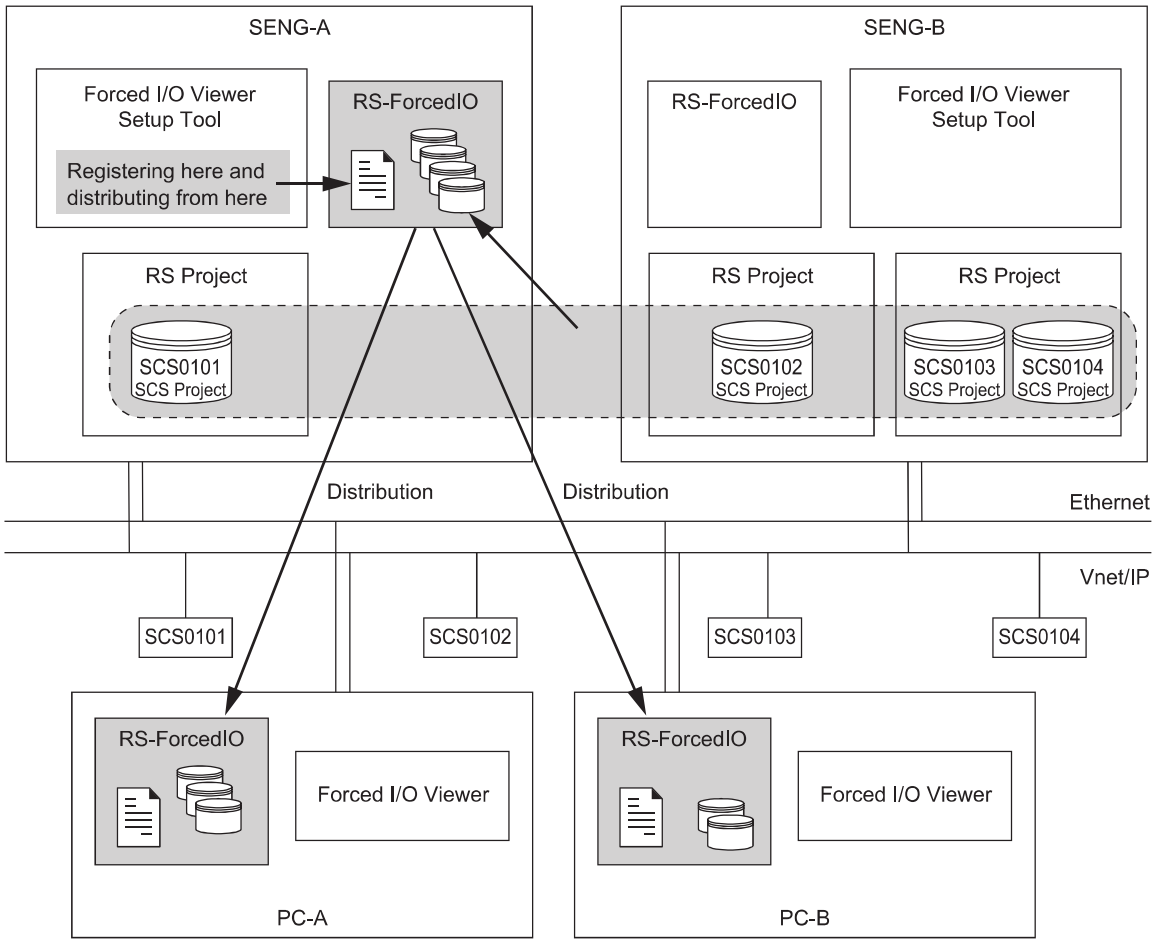


Figure I4.1.4-1 Distribution example of SCS projects

This figure is an example of distributing the registration file and SCS projects after you make the setting to use Forced I/O Viewer by each PC-A computer and PC-B computer from Forced I/O Viewer Setup Tool in the SENG-A computer.

The distribution destination is the following folder where a shared name RS-ForcedIO was assigned in the computer that uses Forced I/O Viewer.

```
<ProSafe-RS install drive>:\Program Files (x86)\ProSafe-RS\YOKOGAWA\hmi\ForcedIO
```

You can distribute the registration file and SCS projects together to all registered computers, distribute them to specific computers, or distribute only specific SCS projects.

For example, if a computer is added, distribute the registration file and SCS projects only to the added computer. If an SCS is added, distribute the registration file and the SCS projects of the added SCS to the computers which require to monitor the added SCS.

By distributing the registration file to other SENGs, you can also change and distribute the registration information by using the Forced I/O Viewer Setup Tool in other SENGs.

TIP

In the following cases, register the computer that uses Forced I/O Viewer Setup Tool from the Computer dialog box of Forced I/O Viewer Setup Tool and distribute the registration file and SCS projects to the computer itself:

- Using Forced I/O Viewer Setup Tool and Forced I/O Viewer on one computer
- Changing registration file from other SENGs

When the registration file is redistributed to a computer that has already been distributed, it is overwritten.

IMPORTANT

To distribute the registration file and SCS projects, setup specific to this function is required.

SEE ALSO

For more information about setup specific to this function, refer to:

B4.4, “Settings Required to Use the Forced I/O Viewer Function” in Installation Guide (IM 32P01C50-01EN)

For more information about how to distribute the registration file and SCS projects, refer to:

“■ Step 4: Distributing a registration file and SCS projects” on page I4-27

I4.1.5 Precautions for Forced I/O Viewer function

This section describes the precautions when using the Forced I/O Viewer function.

Display when forced-I/O information cannot be acquired

If the forced-I/O information cannot be acquired by the communication error or other reasons, a character that indicates an error is added after the station name of SCS of header.

Table I4.1.5-1 Error display of the header of forced-I/O information

Display	Error	Cause
(E)	Information cannot be acquired due to SCS.	• Communication error occurs.
(P)	Information cannot be acquired due to SCS project.	• SCS project is not distributed. • The distributed SCS project is different from the SCS project downloaded to SCS.

Example: SCS0101 SCS0102(E) SCS0103(P) SCS0104

In case (E) or (P) is added to the station name of SCS, the forced-I/O information of the corresponding SCS does not appear.

SEE ALSO For more information about display example of the forced-I/O information, refer to:

"● Display example of forced-I/O information" on page I4-35

When used computer is changed

In case of using the setup data by other computers or replacing a computer in which Forced I/O Viewer or Forced I/O Viewer Setup Tool is installed, perform the following operation:

- If the computer name is not changed
  Copy all files in the following folder and paste them to the target computer.

  ```
  <ProSafe-RS install drive>:\Program Files (x86)\ProSafe-RS\YOKOGAWA\hmi\ForcedIO
  ```

- If the computer name is changed
  - Copy all files in the following folder and paste them to the target computer.
    ```
    <ProSafe-RS install drive>:\Program Files (x86)\ProSafe-RS\YOKOGAWA\hmi\ForcedIO
    ```
  - Change the computer name in the Computer dialog box of Forced I/O Viewer Setup Tool.
  - By using the Distribution dialog box, distribute the registration file to the computer whose name has been changed.

I4.1.6 Screen configuration of Forced I/O Viewer Setup Tool

In Forced I/O Viewer Setup Tool, perform the following settings required to acquire and display the forced-I/O information in the Forced I/O Viewer.

- Registration of SCS:
  By using the SCS dialog box and the SCS Project Path dialog box, register the SCS and the SCS project path from which the forced-I/O information to be acquired.
- Registration of group:
  By using the Group dialog box, register groups and SCSs that belong to the group.
- Registration of computer:
  By using the Computer dialog box, register a computer that displays the forced-I/O information and groups to assign to the computer.
- Distribution of the registration file and SCS projects:
  By using the Distribution dialog box, distribute the registration file and the SCS projects to the computer.

The following figure shows a screen structure of Forced I/O Viewer Setup Tool.

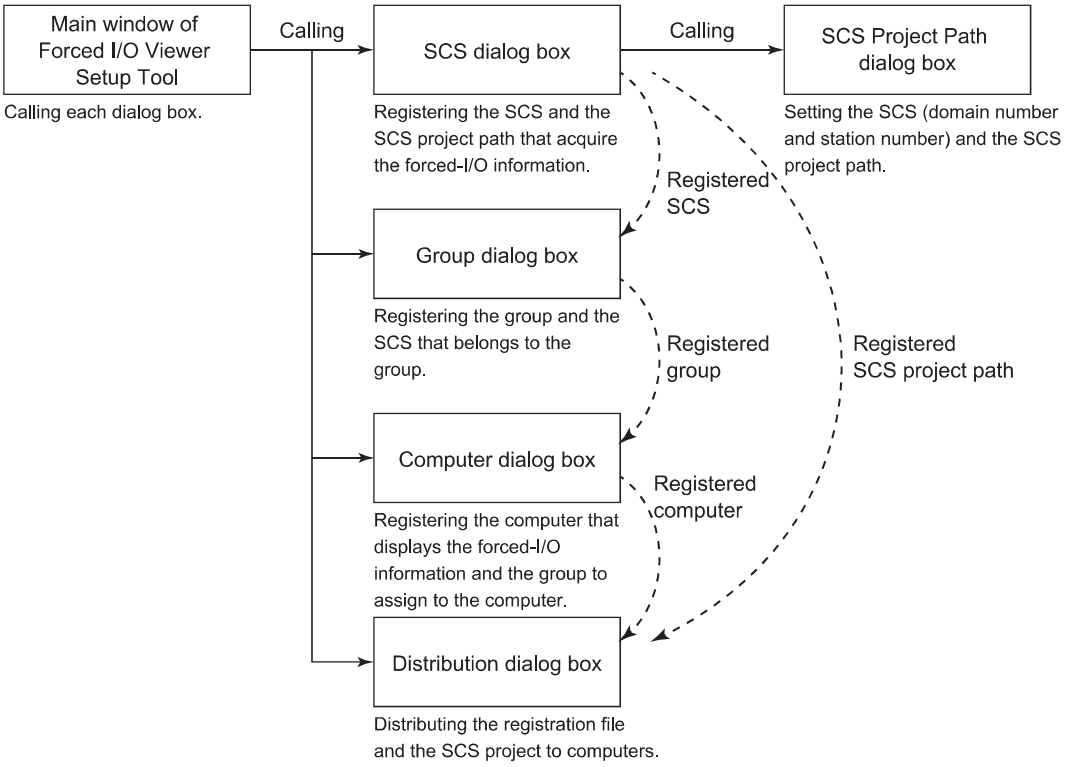


Figure I4.1.6-1 Screen configuration of Forced I/O Viewer Setup Tool

Main window

When you start the Forced I/O Viewer Setup Tool, main window of Forced I/O Viewer Setup Tool appears.

The following figure shows a main window of Forced I/O Viewer Setup Tool.

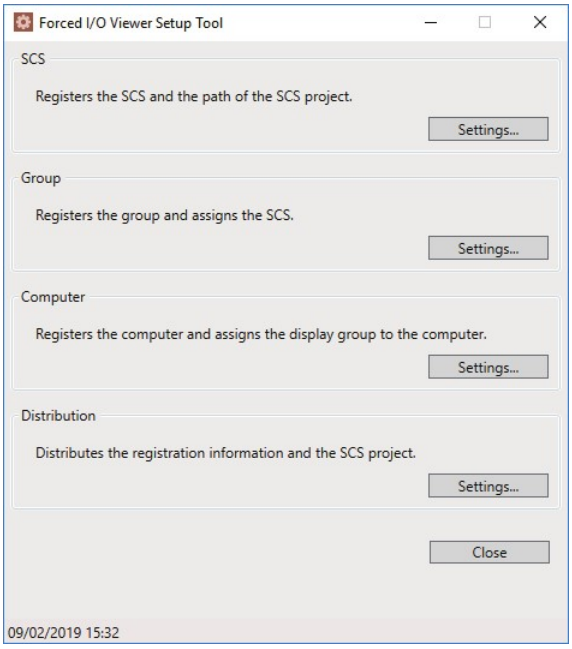


Figure I4.1.6-2 Main window of Forced I/O Viewer Setup Tool

IMPORTANT

Multiple Forced I/O Viewer Setup Tools cannot be started on one computer.

In the following cases, a message dialog box appears when you start the Forced I/O Viewer Setup Tool:

- When there are a saved registration file and a distributed registration file
- When there is only a distributed registration file

If a message dialog box appears, check the displayed message and select an appropriate registration file.

Buttons to open a dialog box

If you click [Settings...] in each area of the main window of Forced I/O Viewer Setup Tool, the corresponding dialog box opens.

Table I4.1.6-1 Buttons to open a dialog box in the main window

Area	Button	Description
SCS	Settings...	Opens the SCS dialog box.
Group	Settings...	Opens the Group dialog box.
Computer	Settings...	Opens the Computer dialog box.
Distribution	Settings...	Opens the Distribution dialog box.

Button related to a whole window

Table I4.1.6-2 Button for the whole main window

Button	Description
Close	Closes the Forced I/O Viewer Setup Tool.

Status bar

Table I4.1.6-3 Status bar of the main window

Display item	Description
Date and time when the registration file was updated	The Forced I/O Viewer Setup Tool displays the date and time that the loaded registration file was updated. Updated date and time: The date and time when the registration file is saved by the SCS dialog box, the Group dialog box, and the Computer dialog box

SCS dialog box

The SCS dialog box is used to register SCSs that you want to acquire the forced-I/O information.

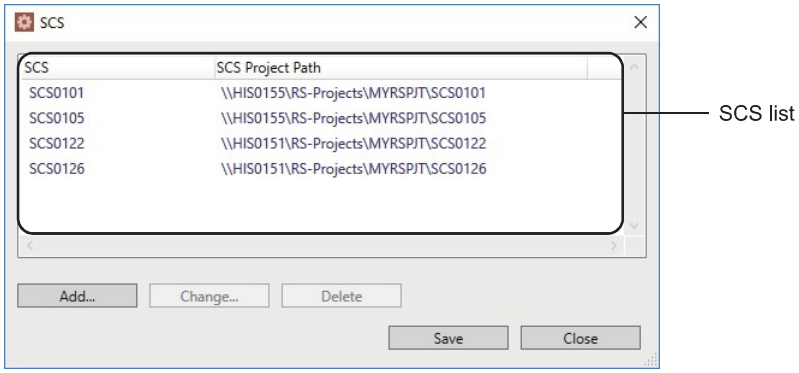


Figure I4.1.6-3 SCS dialog box

SEE ALSO For more information about procedure of registering SCSs, refer to:

"■ Step 1: Registering SCSs" on page I4-24

SCS list

SCSs registered in the SCS list appear in ascending order of the station name.

Table I4.1.6-4 Display of SCS list in the SCS dialog box

Display	Description
SCS	Station name of the SCS that you want to acquire the forced-I/O information appears. Example: SCS0101 • Set in the SCS Project Path dialog box. • It cannot be entered directly. • Station name of the SCS that is registered with SCS list cannot be changed.
SCS Project Path	Path of the SCS project that you want to acquire the forced-I/O information appears. Example: `\\SENG0151\RS-Projects\MYRSPJT\SCS0101` • Set in the SCS Project Path dialog box. • It cannot be entered directly.

Table I4.1.6-5 Buttons of SCS list in the SCS dialog box

Button	Description
Add...	Adds an SCS that you want to acquire the forced-I/O information. If you click [Add...], the SCS Project Path dialog box appears.

Continues on the next page

Table I4.1.6-5 Buttons of SCS list in the SCS dialog box (Table continued)

Button	Description
Change...	Sets and changes the SCS project path displayed in the SCS list. If you select a row of SCS to set or change and click [Change...], the SCS Project Path dialog box appears.
Delete	Deletes the selected SCS from the SCS list.

● Buttons related to a whole dialog box

Table I4.1.6-6 Buttons for the whole SCS dialog box

Button	Description
Save	Saves the registration information and closes the dialog box.
Close	Closes the dialog box without saving the registration information.

■ SCS Project Path dialog box

The SCS Project Path dialog box is opened from the SCS dialog box. The SCS Project Path dialog box is used to add the SCS and set the SCS project path to the SCS list in the SCS dialog box.

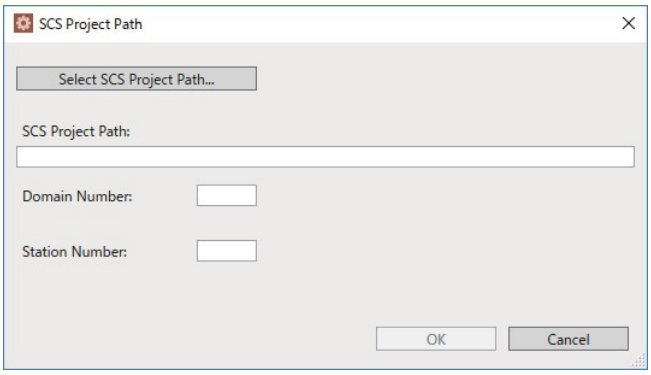


Figure I4.1.6-4 SCS Project Path dialog box

Take note on the following cautions when using the SCS Project Path dialog box:

- Make sure to set the domain number and the station number.
- Make sure to set the SCS project path before distributing the registration file and the SCS project from the Distribution dialog box.
- SCS project path can be selected from the Folder Selection dialog box after clicking [Add...] in the SCS dialog box, followed by clicking [Select SCS Project Path...] in the SCS Project Path dialog box. After a path is selected in the Folder Selection dialog box, the domain number and the station number of SCS automatically appear on the SCS Project Path dialog box.
- The domain number and the station number of SCS cannot be changed after registering them as a station name of SCS on the SCS list in the SCS dialog box.
  Delete that SCS station name from the SCS list in the SCS dialog box first and register a new SCS station name.
- If you display the SCS Project Path dialog box from [Change...] in the SCS dialog box, the domain number and the station number of the SCS appear, but you cannot edit them.

SCS Project Path

Table I4.1.6-7 Button of the SCS Project Path dialog box

Button	Description
Select SCS Project Path	Selects an SCS project path. If you click [Select SCS Project Path], the Folder Selection dialog box appears. In the Folder Selection dialog box, select a path in UNC format through the shared name RS-Projects. When you use an SCS project on the local computer, select a path in UNC format through the shared name RS-Projects as well. UNC format: `\\Computer name\Shared name\RS-Projects name\SCS project name` Example: `\\SENG0151\RS-Projects\MYRSPJT\SCS0101`

Table I4.1.6-8 Input area of the SCS Project Path dialog box

Display	Description
SCS Project Path:	Set the SCS project path. Perform either of the following operations: • Select a path in the Folder Selection dialog box that is displayed by clicking [Select SCS Project Path]. • Directly enter it. Set in UNC format (`\\Computer name\Shared name\RS-Projects name\SCS project name`) through the shared name RS-Projects. Example: `\\SENG0151\RS-Projects\MYRSPJT\SCS0101`
Domain Number:	Set the domain number of SCS.
Station Number:	Set the station number of SCS.

Buttons related to a whole dialog box

Table I4.1.6-9 Buttons for the whole SCS Project Path dialog box

Button	Description
OK	Reflects the settings in this dialog box to the SCS list in the SCS dialog box and closes the dialog box.
Cancel	Cancels the input and closes the dialog box.

Group dialog box

The Group dialog box is used to register the group name and the SCS that belong to the group.

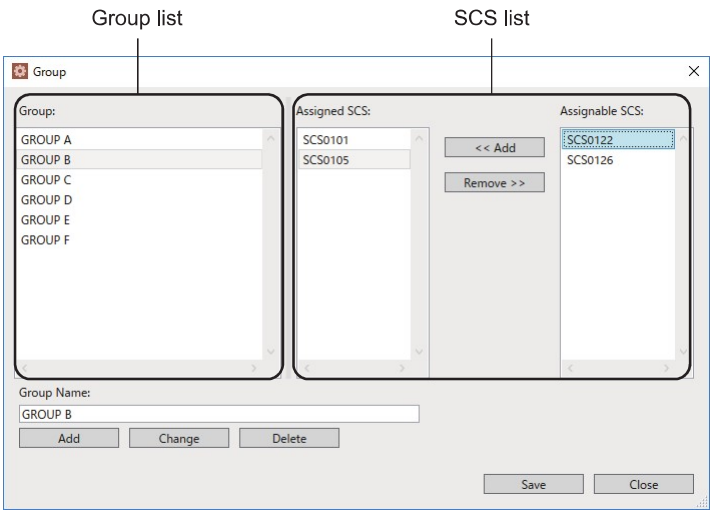


Figure I4.1.6-5 Group dialog box

SEE ALSO For more information about procedure of registering groups, refer to:

"■ Step 2: Registering groups" on page I4-24

Group list

Table I4.1.6-10 Display of the Group list and the input area in the Group dialog box

Display	Description
Group:	Registered groups are listed. • It cannot be entered directly. • Multiple selection is not available.
Group Name:	Enter a group name when adding a group or changing the group name. When you select a group from the Group list, the name of the selected group appears. • Directly enter it.

Table I4.1.6-11 Buttons of the Group list in the Group dialog box

Button	Description
Add	Adds a group. The added group appears in the Group list.
Change	Changes the group name selected from the Group list.
Delete	Deletes the group selected from the Group list.

SCS list

Table I4.1.6-12 Display of SCS list in the Group dialog box

Display	Description
Assigned SCS:	The SCSs assigned to the group selected in the Group list are listed. Example: SCS0101 • It cannot be entered directly. • Multiple selection is available.
Assignable SCS:	Among the SCSs registered in the SCS dialog box, the SCSs not assigned to the group selected in the Group list are listed. Example: SCS0102 • It cannot be entered directly. • Multiple selection is available.

Table I4.1.6-13 Buttons of the SCS list in the Group dialog box

Button	Description
<<Add	Assigns SCSs to the group selected in the Group list. The assigned SCSs are listed in the SCS list of Assigned SCS:.
Remove>>	Removes the assigned SCSs from the group selected in the Group list. The removed SCSs are removed from the SCS list of Assigned SCS:.

● Buttons related to a whole dialog box

Table I4.1.6-14 Buttons for the whole Group dialog box

Button	Description
Save	Saves the registration information and closes the dialog box.
Close	Closes the dialog box without saving the registration information.

■ Computer dialog box

The Computer dialog box is used to register a computer name that uses Forced I/O Viewer, and groups displayed as options when running the Forced I/O Viewer on that computer. The registration file and the SCS projects are distributed to the computer that is registered in the Computer dialog box.

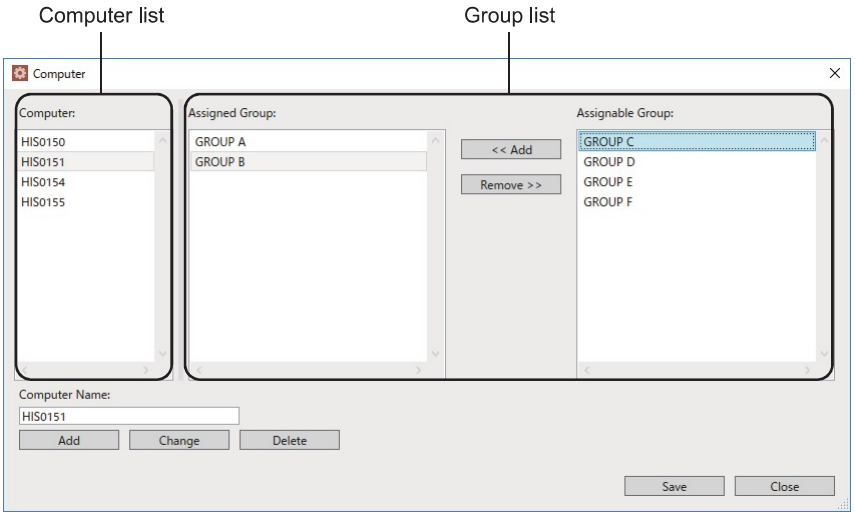


Figure I4.1.6-6 Computer dialog box

If the NetBIOS over TCP/IP is disabled, you must configure the LMHOSTS file to resolve names.

SEE ALSO

For more information about procedure of registering computers, refer to:

"■ Step 3: Registering computers" on page I4-26

For more information about LMHOSTS file settings, refer to:

"■ Notes on the Case when NetBIOS over TCP/IP is Disabled" in B3.6.1, "Running the IT Security Tool" in Installation Guide (IM 32P01C50-01EN)

Computer list

Table I4.1.6-15 Display of the Computer list and the input area in the Computer dialog box

Display	Description
Computer:	Registered computer names are listed. Example: PC0161 • It cannot be entered directly. • Multiple selection is not available.
Computer Name:	Enter the computer name when adding a computer or changing the computer name. When you select a computer from the Computer list, the name of the selected computer appears. • Directly enter it.

Table I4.1.6-16 Buttons of the Computer list in the Computer dialog box

Button	Description
Add	Adds a computer. The added computer appears in the Computer list.
Change	Changes the computer name selected from the Computer list.
Delete	Deletes the computer from the Computer list

Group list

Table I4.1.6-17 Display of Group list in the Computer dialog box

Display	Description
Assigned Group:	The groups assigned to the computer selected in the Computer list are listed. • It cannot be entered directly. • Multiple selection is available.
Assignable Group:	Among the groups registered in the Group dialog box, the groups not assigned to the computer selected in the Computer list are listed. • It cannot be entered directly. • Multiple selection is available.

Table I4.1.6-18 Buttons of the Group list in the Computer dialog box

Button	Description
<<Add	Assigns groups to the computer selected in the Computer list. The assigned groups are listed in the Group list of Assigned Group:.
Remove>>	Removes the assigned groups from the computer selected in the Computer list. The removed groups are removed from the Group list of Assigned Group:.

Buttons related to a whole dialog box

Table I4.1.6-19 Buttons for the whole Computer dialog box

Button	Description
Save	Saves the registration information and closes the dialog box
Close	Closes the dialog box without saving the registration information

Distribution dialog box

The Distribution dialog box is used to distribute the registration file and the SCS projects to the computers that are registered in the Computer dialog box.

The computers registered in the Computer dialog box and the SCSs registered in the SCS dialog box are listed. Select destination computers and SCS projects of the SCSs to distribute from the list and distribute them.

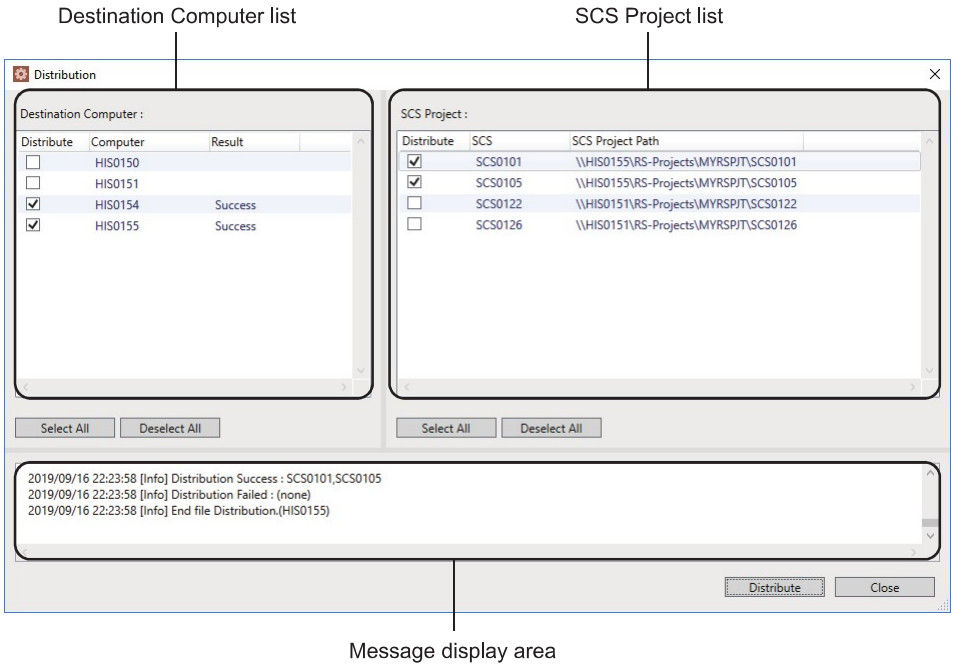


Figure I4.1.6-7 Distribution dialog box

IMPORTANT

If you build the SCS project data with SENG and download it to SCS after the distribution, distribute it again. If you perform build and offline download without engineering, distribute it again.

SEE ALSO For more information about procedure of distributing to computers, refer to:

"■ Step 4: Distributing a registration file and SCS projects" on page I4-27

● Destination Computer list

Table I4.1.6-20 Display of Destination Computer list in the Distribution dialog box

Display	Description
Distribute	Select a check box of the computer to distribute to.
Computer	The computer name registered in the Computer dialog box appears. Example: PC0161
Result	Distribution result appears. Success Error

Table I4.1.6-21 Buttons of the Destination Computer list in the Distribution dialog box

Button	Description
Select All	Selects the check boxes of all Distribute columns in the Destination Computer list.
Deselect All	Clears the check boxes of all Distribute columns in the Destination Computer list.

SCS Project list

Table I4.1.6-22 Display of SCS Project list in the Distribution dialog box

Display	Description
Distribute	Select a check box of the SCS project to distribute.
SCS	The station name of SCS registered in the SCS dialog box appears. Example: SCS0101
SCS Project Path	SCS project path of SCS registered in the SCS dialog box appears. Example: `\\SENG0151\RS-Projects\MYRSPJT\SCS0101`

Table I4.1.6-23 Buttons of the SCS Project list in the Distribution dialog box

Button	Description
Select All	Selects the check boxes of all Distribute columns in the SCS Project list.
Deselect All	Clears the check boxes of all Distribute columns in the SCS Project list.

Message display area

Table I4.1.6-24 Message display area of the Distribution dialog box

Display	Description
Message display area	During the distribution process, the progress of the action appears.

Buttons related to a whole dialog box

Table I4.1.6-25 Buttons for the whole Distribution dialog box

Button	Description
Distribute (*1)	Distributes the registration file and the SCS projects (*2) that the Distribute check boxes in the SCS Project list are selected to the computers that the Distribute check boxes in the Destination Computer list are selected. If the Distribute check boxes in the Destination Computer list are selected but the Distribute check boxes in the SCS Project list are not selected, only the registration file is distributed.
Cancel	Stops the distribution.
Close	Closes the dialog box.

*1: This button acts as Cancel button during the distribution process.
*2: If the SCS belongs to the group that is assigned to the destination computer, these are distributed.

I4.1.7 Operations in Forced I/O Viewer Setup Tool

This section describes how to use the Forced I/O Viewer Setup Tool.

Preparation: Turning on the computer

In Forced I/O Viewer Setup Tool, the registration file and the SCS projects are distributed to the computer that uses Forced I/O Viewer. Before starting the setting of Forced I/O Viewer by using the Forced I/O Viewer Setup Tool, turn on the following computers. Make sure to not turn off the computers until the setting of Forced I/O Viewer Setup Tool is completed.

- Computer where the SCS projects are saved
- Destination computer

Step 1: Registering SCSs

IMPORTANT

If you distribute a registration file from another Forced I/O Viewer Setup Tool while using the Forced I/O Viewer Setup Tool, restart the Forced I/O Viewer Setup Tool that you are using.

Follow these steps to register the SCSs for which you want to acquire the forced-I/O information:

1. Start the Forced I/O Viewer Setup Tool.
   The main window appears.
2. Click [Settings...] in the SCS area.
   The SCS dialog box appears.
3. Click [Add...].
   The SCS Project Path dialog box appears.
4. Click [Select SCS Project Path...].
   The Folder selection dialog box appears.
5. Select the SCS project path.
   The selected path appears in the input area of SCS Project Path:. In addition, the domain number appears in the input area of Domain Number: and the station number appears in the input area of Station Number:.
6. Click [OK].
7. Repeat step 3 to 6 to add all SCSs to register.
8. Click [Save].
   The settings are saved.

Step 2: Registering groups

Follow these steps to register groups:

1. Start the Forced I/O Viewer Setup Tool.
   The main window appears.
2. Click [Settings...] in the Group area.
   The Group dialog box appears.
3. Enter a group name to be added in the input area of Group Name:, and click [Add].
   The entered group name is added to the Group list.

4. Repeat step 3 to add all groups you want to register to the Group list.
5. Select the target group from the Group list, select all SCSs to assign from the SCS list of Assignable SCS:, and then click [<<Add].
   The SCSs are added to the SCS list of Assigned SCS:.

TIP Multiple SCSs can be selected from the SCS list of Assignable SCS:.

6. Repeat step 5 to assign SCSs to all groups.
7. Click [Save].
   The settings are saved.

Changing the group name

Follow these steps to change the group name:

1. Open the Group dialog box.
2. From the Group list, select a group name to rename, change the name displayed in the input area of Group Name:, and then click [Change].

Deleting a group

Follow these steps to delete a group:

1. Open the Group dialog box.
2. From the Group list, select the group to delete, and click [Delete].
   The confirmation dialog box appears.
3. Click [OK].
   The group is deleted.

Assigning SCSs to a group

Follow these steps to assign SCSs to a group:

1. Open the Group dialog box.
2. Select the target group from the Group list, select all SCSs to assign from the SCS list of Assignable SCS:, and then click [<<Add].
   The assigned SCSs are added to the SCS list of Assigned SCS: of the selected group.

TIP Multiple SCSs can be selected from the SCS list of Assignable SCS:.

3. Repeat step 2 to assign SCSs to all groups.

Removing the assigned SCSs from the group

Follow these steps to remove the assigned SCSs from the group:

1. Open the Group dialog box.
2. Select the target group from the Group list, select SCSs that you want to remove the assignment from the SCS list of Assigned SCS:, and then click [Remove>>].
   The SCSs are removed from the SCS list of Assigned SCS: of the selected group.

TIP Multiple SCSs can be selected from the SCS list of Assigned SCS:.

Saving the settings

Perform this step to save the settings:

- Click [Save].

The settings are saved.

Step 3: Registering computers

Follow these steps to register computers that use the Forced I/O Viewer:

1. Start the Forced I/O Viewer Setup Tool.
   The main window appears.
2. Click [Settings...] in the Computer area.
   The Computer dialog box appears.
3. Enter a computer name to be added in the input area of Computer Name:, and click [Add].
   The entered computer name is added to the Computer list.
4. Repeat step 3 to add all computers you want to register to the Computer list.
5. Select the target computer from the Computer list, select all groups to assign from the Group list of Assignable Group:, and then click [<<Add].
   The assigned groups are added to the Group list of Assigned Group: of the selected computer.

TIP Multiple groups can be selected from the Group list of Assignable Group:.

6. Repeat step 5 to assign groups to all computers.
7. Click [Save].
   The settings are saved.

Changing the computer name

Follow these steps to change the registered computer name:

1. Open the Computer dialog box.
2. From the Computer list, select a computer name to rename, change the name displayed in the input area of Computer Name:, and then click [Change].

Deleting a computer

Follow these steps to delete a registered computer:

1. Open the Computer dialog box.
2. Select a computer to delete from the Computer list, and click [Delete].
   The confirmation dialog box appears.
3. Click [OK].
   The computer is deleted.

Assigning groups to a computer

Follow these steps to assign groups to a computer:

1. Open the Computer dialog box.
2. Select the target computer from the Computer list, select all groups to assign from the Group list of Assignable Group:, and then click [<<Add].
   The assigned groups are added to the Group list of Assigned Group: of the selected computer.

TIP Multiple groups can be selected from the Group list of Assignable Group:.

3. Repeat step 2 to assign groups to all computers.

Removing the assigned groups from the computer

Follow these steps to remove the assigned groups from the computer:

1. Open the Computer dialog box.
2. Select the target computer from the Computer list, select groups that you want to remove the assignment from the Group list of Assigned Group:, and then click [Remove>>].
   The groups are removed from the Group list of Assigned Group: of the selected computer.

TIP

Multiple groups can be selected from the Group list of Assigned Group:.

Saving the settings

Perform this step to save the settings:

- Click [Save].
  The settings are saved.

Step 4: Distributing a registration file and SCS projects

There are several ways to distribute a registration file and SCS projects to a computer.

This section describes each method.

IMPORTANT

You cannot distribute to the computer where Forced I/O Viewer is collecting forced-I/O information. If you attempt distribution, an error will result. Distribution is also not possible while the Forced I/O Acquisition (Select) dialog box or Forced I/O Acquisition (Start) dialog box is displayed on Forced I/O Viewer.

Distributing a registration file and SCS projects to all computers

Follow these steps to distribute a registration file and SCS projects to all computers:

1. Start the Forced I/O Viewer Setup Tool.
   The main window appears.
2. Click [Settings...] in the Distribution area.
   The Distribution dialog box appears.
3. Click [Select All] under the Destination Computer list.
   The check boxes of all Distribute columns in the Destination Computer list are selected.
4. Click [Select All] under the SCS Project list.
   The check boxes of all Distribute columns in the SCS Project list are selected.
5. Click [Distribute].
   The distribution result for each computer appears in the Result column of Destination Computer list. If there is an error, the error information appears in the message display area.

Distributing a registration file and SCS projects by selecting a specific computer

When a computer is added or a distribution to a specific computer is failed, you can distribute a registration file and SCS projects to the specific computer.

Follow these steps to distribute a registration file and SCS projects to the specific computer:

1. Start the Forced I/O Viewer Setup Tool.

The main window appears.

2. Click [Settings...] in the Distribution area.
   The Distribution dialog box appears.
3. Click [Deselect All] under the Destination Computer list.
   The check boxes of all Distribute columns in the Destination Computer list are cleared.
4. Select the check boxes of Distribute columns in the Destination Computer list that you want to distribute.
5. Click [Select All] under the SCS Project list.
   The check boxes of all Distribute columns in the SCS Project list are selected.
6. Click [Distribute].
   The distribution result for each computer appears in the Result column of Destination Computer list. If there is an error, the error information appears in the message display area.

Distributing selected specific SCS projects to all computers

When you add an SCS, when you re-build SCS project data with SENG and download it to the SCS after the distribution, or when it fails the distribution of only specific SCS projects, you can distribute the specific SCS projects to all computers.

Follow these steps to distribute the specific SCS projects to all computers:

1. Start the Forced I/O Viewer Setup Tool.
   The main window appears.
2. Click [Settings...] in the Distribution area.
   The Distribution dialog box appears.
3. Click [Select All] under the Destination Computer list.
   The check boxes of all Distribute columns in the Destination Computer list are selected.
4. Click [Deselect All] under the SCS Project list.
   The check boxes of all Distribute columns in the SCS Project list are cleared.
5. Select the check boxes of Distribute columns in the SCS Project list that you want to distribute.
6. Click [Distribute].
   The distribution result for each computer appears in the Result column of Destination Computer list. If there is an error, the error information appears in the message display area.

Distributing only the registration file to all computers

When the settings are changed in the Group dialog box or the Computer dialog box, you can distribute only the registration file to all computers.

Follow these steps to distribute only the registration file to all computers:

1. Start the Forced I/O Viewer Setup Tool.
   The main window appears.
2. Click [Settings...] in the Distribution area.
   The Distribution dialog box appears.
3. Click [Select All] under the Destination Computer list.
   The check boxes of all Distribute columns in the Destination Computer list are selected.
4. Click [Deselect All] under the SCS Project list.
   The check boxes of all Distribute columns in the SCS Project list are cleared.
5. Click [Distribute].
   The confirmation dialog box appears.

6. Click [Yes].
   The distribution result for each computer appears in the Result column of Destination Computer list. If there is an error, the error information appears in the message display area.

I4.1.8 Screen configuration of Forced I/O Viewer

The Forced I/O Viewer acquires and displays the forced-I/O information.

The following figure shows a screen configuration of the Forced I/O Viewer.

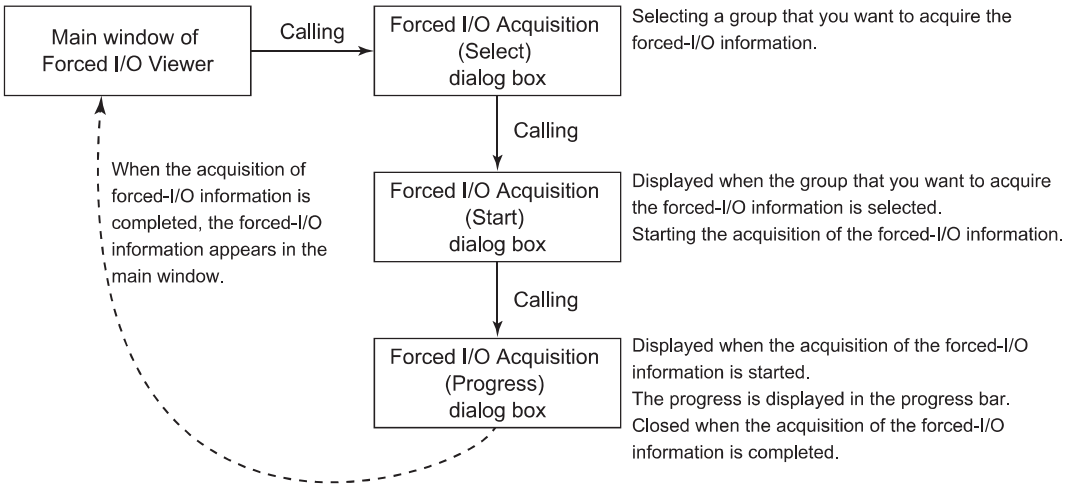


Figure I4.1.8-1 Screen configuration of Forced I/O Viewer

Main window

When you start the Forced I/O Viewer, main window of Forced I/O Viewer appears.

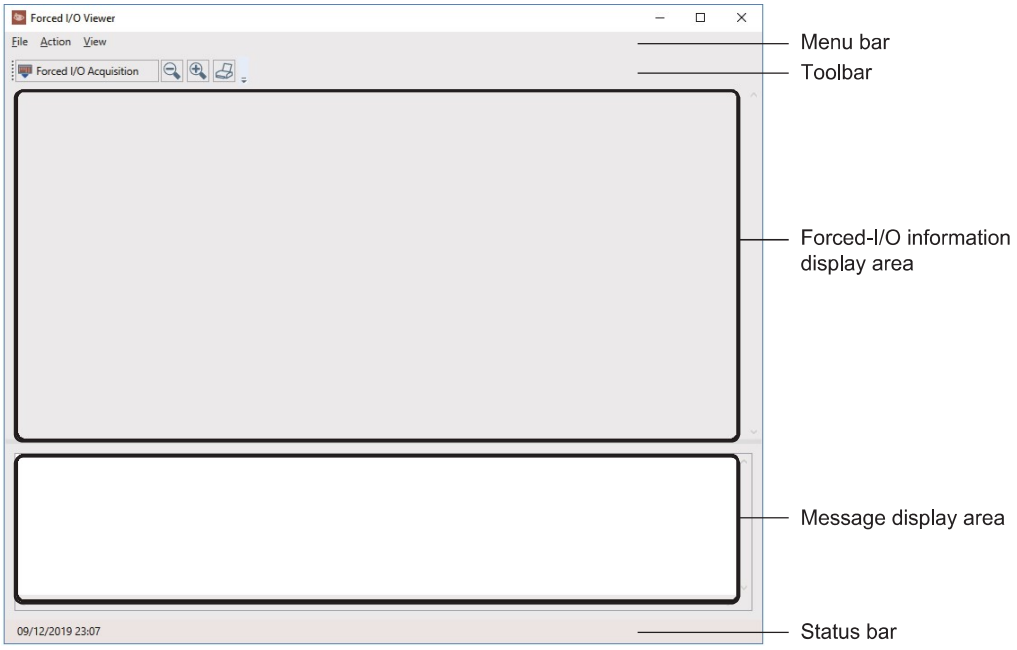


Figure I4.1.8-2 Main window of Forced I/O Viewer

Multiple Forced I/O Viewers cannot be started on one computer.

If the Forced I/O Viewer is started on the computer where the registration file and SCS projects are not distributed from the Forced I/O Viewer Setup Tool, a message dialog box appears, and the Forced I/O Viewer exits.

Menu bar

In the Menu bar, File menu, Action menu, and View menu are displayed.

Table I4.1.8-1 File menu

Item	Description
Print...	Prints the forced-I/O information shown in the forced-I/O information display area.
Output CSV File...	Outputs the forced-I/O information shown in the forced-I/O information display area to CSV format file.
Exit	Exits the Forced I/O Viewer.

Table I4.1.8-2 Action menu

Item	Description
Forced I/O Acquisition...	Opens the Forced I/O Acquisition (Select) dialog box.

Table I4.1.8-3 View menu

Item	Description
Zoom in	Enlarges the character size in the forced-I/O information display area.
Zoom out	Reduces the character size in the forced-I/O information display area.

Toolbar

There are toolbars of Forced I/O Acquisition, Zoom In, Zoom out, and Print.

Forced-I/O information display area

In the forced-I/O information display area, a header that is the handling information of forced-I/O information acquisition and the acquired forced-I/O information appear.

Summary is displayed in the title of forced-I/O information. If you click the title of forced-I/O information, the detailed information appears. If you click the title of forced-I/O information while the detailed information is displayed, the detailed information closes.

The following table shows the classification and the title of forced-I/O information.

Table I4.1.8-4 Classification of the forced-I/O information area and the title of forced-I/O information

Classification	Title of forced-I/O information
Header	Header
I/O variable and Internal variable	I/O Variable and Internal Variable (Number of locks)
SCS Link Transmission Send	SCS Link Transmission Send (Number of locks)
SCS Link Transmission Receive	SCS Link Transmission Receive (Number of locks)
Inter-SCS Safety Communication Send	Inter-SCS Safety Communication Send (Number of locks)
Inter-SCS Safety Communication Receive	Inter-SCS Safety Communication Receive (Number of locks)
Subsystem communication	Subsystem Communication (Locked/Not locked)
Safety subsystem communication	Safety Subsystem Communication (Number of locks)

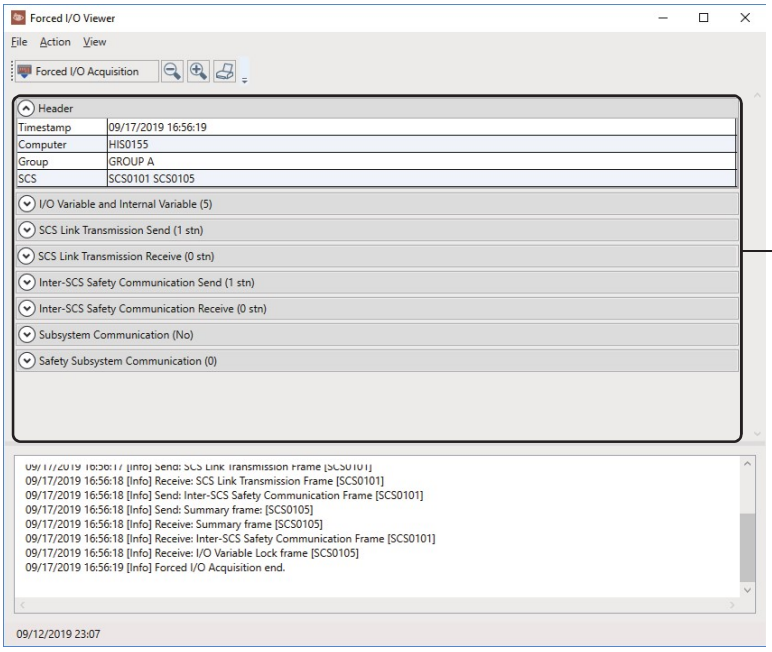


Figure I4.1.8-3 Forced-I/O information display area of main window

The specifications of forced-I/O information display area are as follows:

- The forced-I/O information display area is not displayed when the forced-I/O information is not acquired, such as when soon after starting the Forced I/O Viewer.
- When the acquisition of forced-I/O information is completed, the header and the forced-I/O information appear in the forced-I/O information display area.
- The details of forced-I/O information are displayed in tabular format as detailed information.
- If you click the column title of the table of detailed information, the table can be sorted in ascending or descending order. If you drag the column title and drop it on the desired position, the position of the column can be changed.
- If there is no locked item, “0” is displayed for the number of locks and “No” is displayed for the Locked/Not locked status in the summary of forced-I/O information. In addition, the table of detailed information is not displayed, but "not exist" is displayed.

Message display area

During the acquisition of forced-I/O information, the progress of the action appears in the message display area.

Status bar

The status bar displays the date and time that the registration file loaded to the Forced I/O Viewer was updated.

Forced I/O Acquisition (Select) dialog box

The Forced I/O Acquisition (Select) dialog box is used to select a group that displays the forced-I/O information. When the Forced I/O Viewer is started, it is automatically displayed on top of the main window.

The group names assigned to that computer in the Computer dialog box of Forced I/O Viewer Setup Tool are listed. From that list, select a group that you want to display the forced-I/O information.

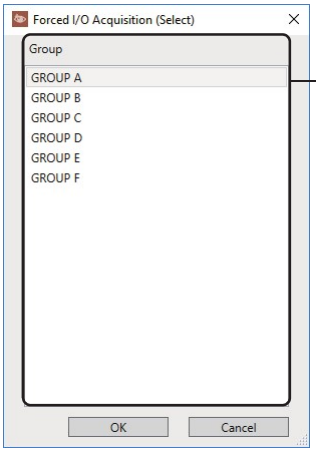


Figure I4.1.8-4 Forced I/O Acquisition (Select) dialog box

● Group list

Table I4.1.8-5 Group list of the Forced I/O Acquisition (Select) dialog box

Display	Description
Group	Names of groups (*1) are listed. • From this list, select a group that you want to display the forced-I/O information. • Multiple selection is not available.

*1: The names of groups assigned to that computer in the Computer dialog box of Forced I/O Viewer Setup Tool

● Buttons related to a whole dialog box

Table I4.1.8-6 Buttons for the whole Forced I/O Acquisition (Select) dialog box

Button	Description
OK	Fixes the selected group in the Group list and displays the Forced I/O Acquisition (Start) dialog box.
Cancel	Closes the dialog box without starting the acquisition of the forced-I/O information.

■ Forced I/O Acquisition (Start) dialog box

The Forced I/O Acquisition (Start) dialog box appears after the group is fixed in the Forced I/O Acquisition (Select) dialog box. This dialog box is used when starting the acquisition of the forced-I/O information.

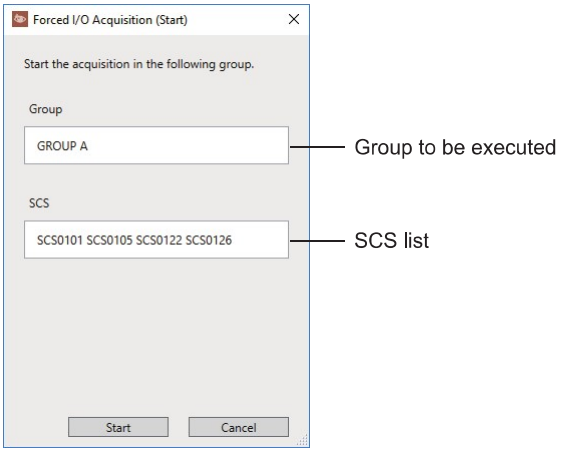


Figure I4.1.8-5 Forced I/O Acquisition (Start) dialog box

Details displayed in the dialog box

Table I4.1.8-7 Details displayed in the Forced I/O Acquisition (Start) dialog box

Display	Description
Group	The group name that will start the acquisition appears. The group name selected from the Group list in the Forced I/O Acquisition (Select) dialog box appears.
SCS	Station names of SCSs (*1) that belong to the group are listed.

*1: The SCSs assigned to that group in the Group dialog box of Forced I/O Viewer Setup Tool

Buttons related to a whole dialog box

Table I4.1.8-8 Buttons for the whole Forced I/O Acquisition (Start) dialog box

Button	Description
Start	Starts the acquisition of the forced-I/O information.
Cancel	Closes the dialog box without starting the acquisition of the forced-I/O information.

Forced I/O Acquisition (Progress) dialog box

The Forced I/O Acquisition (Progress) dialog box appears during the acquisition of forced-I/O information.

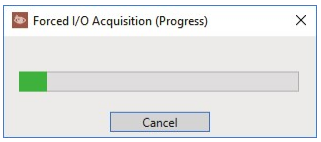


Figure I4.1.8-6 Forced I/O Acquisition (Progress) dialog box

Table I4.1.8-9 Button for the whole Forced I/O Acquisition (Progress) dialog box

Button	Description
Cancel	Stops the acquisition of the forced-I/O information.

I4.1.9 Operations in Forced I/O Viewer

This section describes how to use the Forced I/O Viewer.

Step 1: Acquiring and displaying the forced-I/O information

1. Start the Forced I/O Viewer.
   The main window and the Forced I/O Acquisition (Select) dialog box are displayed by overlapping.

TIP

- To display the Forced I/O Acquisition (Select) dialog box again, click [Forced I/O Acquisition] in the main window.
- If a registration file is distributed from Forced I/O Viewer Setup Tool while the Forced I/O Viewer is used, when the Forced I/O Acquisition (Select) dialog box is displayed, the contents of the distributed registration file are reflected.

2. Select the group that you want to acquire the forced-I/O information from the Group list, and click [OK].
   The Forced I/O Acquisition (Start) dialog box appears.
3. After you confirm that the selected group name is displayed in the Group, click [Start].
   Acquisition of the forced-I/O information is started, and the Forced I/O Acquisition (Progress) dialog box appears.

   When the acquisition of the forced-I/O information is completed, the Forced I/O Acquisition (Progress) dialog box closes. The acquired forced-I/O information appears in the forced-I/O information display area of main window.

TIP

To stop the acquisition while acquiring the forced-I/O information, click [Cancel].

4. Click the title of forced-I/O information that you want to display the detailed information.
   The table of detailed information appears.

Display example of forced-I/O information

- When the information was successfully acquired:
  The following figure shows the display example when the information was successfully acquired from SCS and SCS project.

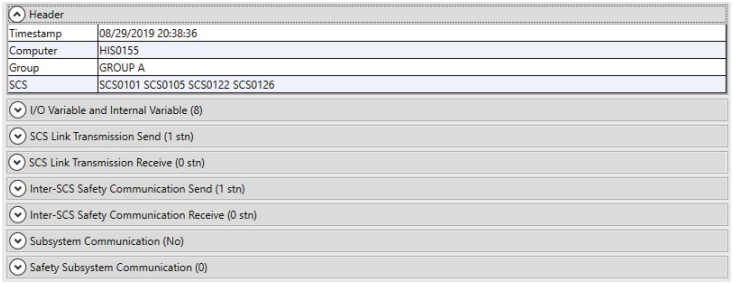


Figure I4.1.9-1 Display example when the information was successfully acquired

- When the information could not be acquired due to SCS:
  The following figure shows the display example when the information could not be acquired from SCS by the communication error or other reasons.

  When the information could not be acquired from SCS, (E) is added to the station name of SCS.

  The following figure shows the example of failure in SCS0101 and SCS0102. The failed SCS information is not output to the summary and the detailed information.

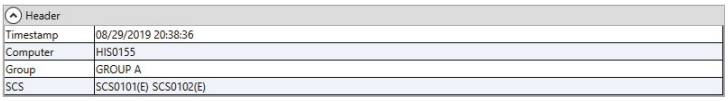


Figure I4.1.9-2 Display example when the information could not be acquired due to SCS

- When the information could not be acquired due to SCS project:
  The following figure shows the display example when the information could not be acquired from SCS project.

  When the information could not be acquired from SCS project, (P) is added to the station name of SCS.

  The following figure shows the example of failure in SCS0101 and SCS0102. The failed SCS information is not output to the summary and the detailed information.

  This situation occurs when the latest SCS project is not distributed. If this situation occurs, distribute the latest SCS project from the Forced I/O Viewer Setup Tool.

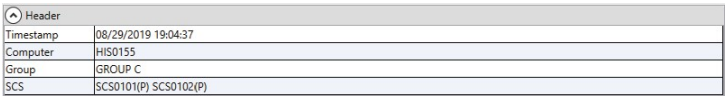


Figure I4.1.9-3 Display example when the information could not be acquired due to SCS project

Step 2: Printing the forced-I/O information

When the forced-I/O information is displayed in the forced-I/O information display area, the forced-I/O information can be printed.

Follow these steps to print the forced-I/O information:

1. Select [File] > [Print] from the main window of Forced I/O Viewer.
   The Print dialog box appears.
2. Set a printer to output and the printing conditions, and click [Print].
   The forced-I/O information is printed.

Example of printing the forced-I/O information

- When the information was successfully acquired:
  The following figure shows the example of printing when the information was successfully acquired from SCS and SCS project.

ProSafe-RS Forced I/O Viewer

Timestamp : 11/05/2019 21:00:10
Computer : HIS0155
Group : GROUP B
Station : SCS0101 SCS0105 SCS0121 SCS0126

Summary:

I/O Variable and Internal Variable (Variable)	5
SCS Link Transmission Send (Station)	1
SCS Link Transmission Receive (Station)	1
Inter-SCS Safety Communication Send (Station)	7
Inter-SCS Safety Communication Receive (Station)	7
Subsystem Communication (Exist)	Yes
Safety Subsystem Communication (PN-Module)	4

I/O Variable and Internal Variable:

Station	Start	Module	Ch.
Variable Name			
Variable Comment			
SCS0102	11/05/2019 21:00:10	2-3 SDV144	1
DI0001XXXXXXXXXXXXXXXXXXXXXXXXXXXX			
DI0001VariableCommentXXXXXXXXXXX			
SCS0102	11/05/2019 21:00:10	2-3 SDV144	2
DI0002XXXXXXXXXXXXXXXXXXXXXXXXXXXX			
DI0002VariableCommentXXXXXXXXXXX			

Figure I4.1.9-4 Example of printing when the information was successfully acquired

- When the information could not be acquired due to SCS:
  The same information as the screen is printed.
- When the information could not be acquired due to SCS project:
  The same information as the screen is printed.

Step 3: Saving the forced-I/O information in a CSV format file

When the forced-I/O information is displayed in the forced-I/O information display area, the forced-I/O information can be saved in a CSV format file.

Follow these steps to save the forced-I/O information in a CSV format file.

1. Select [File] > [Output CSV File] from the main window of Forced I/O Viewer.
   The Save As dialog box appears.
2. Set the file name and the save destination, and click [Save].
   The forced-I/O information is saved in a CSV format file.

I4.2 Message Cache Tool

Diagnostic information messages displayed in the Diagnostic Information window, and SOE event messages and trip information displayed in the SOE Viewer, are collected from SCS stations using the Message Cache Service.

Message Cache Tool is used to display the status of collecting diagnostic information messages, SOE event information and tripping information, to make various settings of Message Cache Service and to maintain cache data collected by Message Cache Service including storage and deletion. It also allows checking the volume of cache data stored on the hard disk.

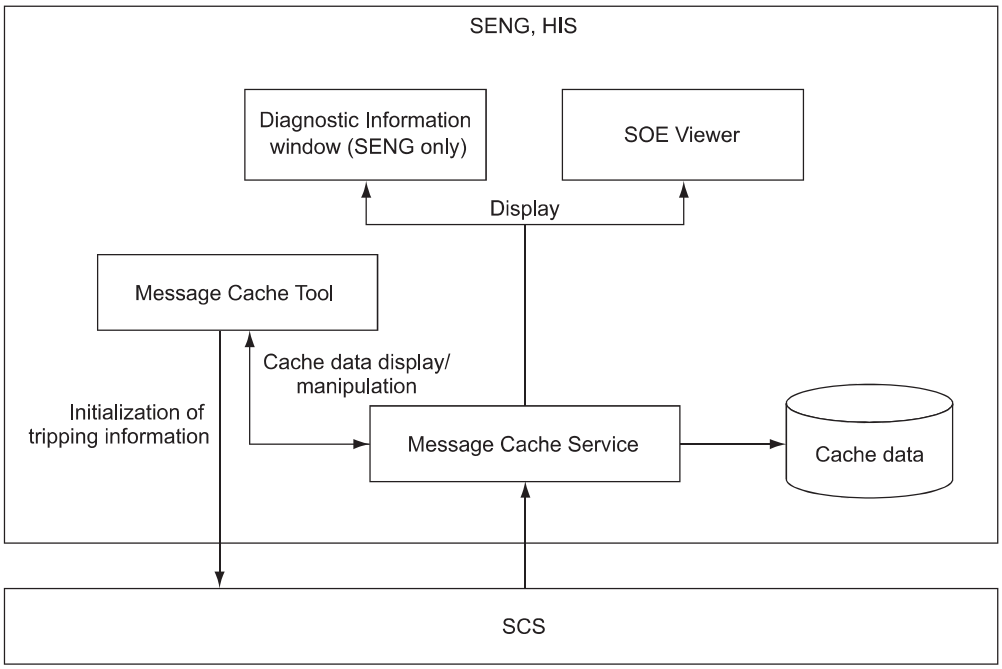


Figure I4.2-1 Positioning of Message Cache Tool

Message Cache tool

Message Cache Tool allows you to make the following settings and maintenance operations:

- Setting stations
  This setting is required only when caching the messages collected by other stations. The settings for the local station were completed beforehand.
- Acquisition setting
  Make settings related to the SCS selected as the target of collection by Message Cache Service and the volume of the hard disk to be used
- Display of data acquisition status
  Display acquisition status of diagnostic information messages, SOE event messages and tripping information collected from the SCS by Message Cache Service
- Initialization of tripping information
  Initialize tripping information in the SCS
- Manipulation of cache data
  Store cache data collected by Message Cache Service in a different folder or delete the data

How to launch Message Cache Tool

1. Start Message Cache Tool.

Before the tool is launched, a password check for SCS Maintenance Support Tool is performed.

2. Enter your password.
When Windows authentication mode is set, enter a password. When the Access Control and Operation History Management Package is applied, enter the name and password of the engineer.

Message Cache Tool window

The Message Cache Tool window is shown in the figure as follows.

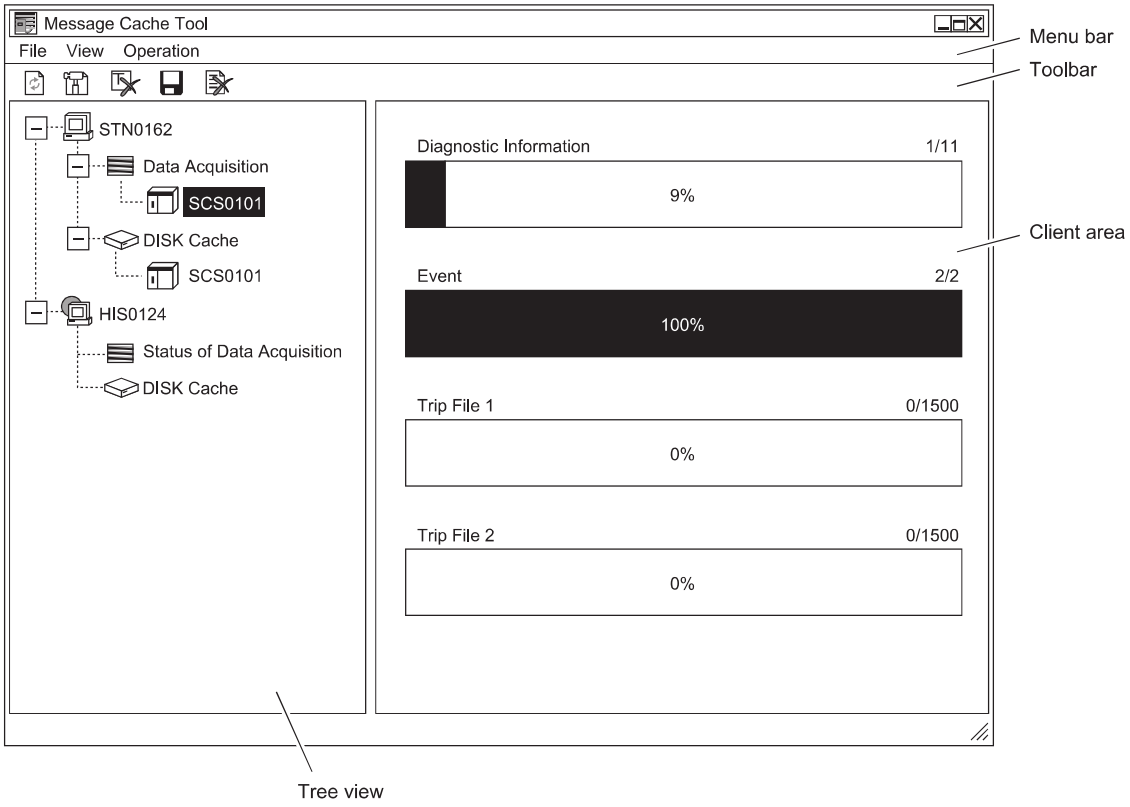


Figure I4.2-2 Data Acquisition Status window of Message Cache Tool

The components of the window are explained next.

Menu bar

The following menus are provided on the menu bar:

- [File] Menu
- [View] Menu
- [Operation] Menu

Menu items provided on each menu are explained as follows.

File menu

Table I4.2-1 File menu

Menu item	Function
Setup	Display a dialog box for making various settings related to Message Cache Service.
Close	Close the Message Cache Tool.

View menu

Table I4.2-2 View menu

Menu item	Function
Toolbar	Hide/show the toolbar
Status Bar	Hide/show the status bar
Station Setup	Display the Station Setup dialog box for selecting one or more stations on which Message Cache Service should run
Update	Update the window display to the latest status

Operation menu

Table I4.2-3 Operation menu

Menu item	Function
Initialize Trip Information	Display the Initialize Trip Information dialog box for the initialization of tripping information maintained in SCS.
Save Disk Cache	Display the Save Disk Cache dialog box for saving the contents of the disk cache in an arbitrary folder.
Delete Disk Cache	Display the Delete Disk Cache dialog box for deleting the contents of the disk cache.

IMPORTANT

Do not delete the disk cache. If disk cache is deleted by selecting the [Delete Disk Cache] menu, the cached diagnostic messages and the SOE events will be lost and cannot be displayed.

SEE ALSO

For more information about Initialize Trip Information dialog box, refer to:

I4.2.5, “Initialization of tripping information” on page I4-48

For more information about the Save DISK Cache dialog box, refer to:

I4.2.6, “Saving disk cache” on page I4-49

Toolbar

The following buttons are provided on the toolbar.

Table I4.2-4 Toolbar buttons

Button	Name	Description
	Update	Same function as [Update] on the [View] menu
	Setup	Same function as [Setup] on the [File] menu
	Initialize Trip Information	Same function as [Initialize Trip Information] on the [Operation] menu
	Save Disk Cache	Same function as [Save Disk Cache] on the [Operation] menu
	Delete Disk Cache	Same function as [Delete Disk Cache] on the [Operation] menu

IMPORTANT

Do not delete the disk cache. If disk cache is deleted by selecting the menu [Delete Disk Cache], the cached diagnostic messages and the SOE events will be lost and cannot be displayed.

Tree view

The tree view displays a list of stations (SENG, HIS) on which Message Cache Service runs.

The following items are displayed for each station.

Table I4.2-5 Display of tree view

Item	Description
Data Acquisition	Click this item to display a list of SCSs that are targets of engineering or operation and monitoring on each station (SENG or HIS). Click the name of an SCS to display the acquisition status of data of the selected SCS in the client area.
DISK Cache	Click this item to display a list of SCSs that are targets of engineering or operation and monitoring on each station (SENG or HIS). Click [Disk Cache] to display the disk cache usage status (all) for the entire station in the client area on the right side. Click the name of an SCS to display the disk cache usage status (SCS) of the selected SCS in the client area.

Client area

The display in the client area varies depending on the target selected in the tree view.

Table I4.2-6 Display of Client area

Selected target	Display
Data Acquisition- SCS	Displays the data acquisition status for each SCS.
Disk Cache	Displays the disk cache usage status (all) for all SCSs defined as data acquisition targets.
Disk Cache - SCS	Displays the disk cache usage status (SCS) for each SCS.

SEE ALSO

For more information about the details displayed in the data acquisition status, refer to:

I4.2.3, “Displaying data acquisition status” on page I4-44

For more information about the details displayed in the disk cache usage status, refer to:

I4.2.4, “Displaying disk cache usage status” on page I4-45

I4.2.1 Setting stations

This setting is required only when caching the messages collected by other stations. The settings for the local station were completed beforehand.

Displaying the Station Setup dialog box

Select [Station Setup] from the [View] menu; the Station Setup dialog box appears.

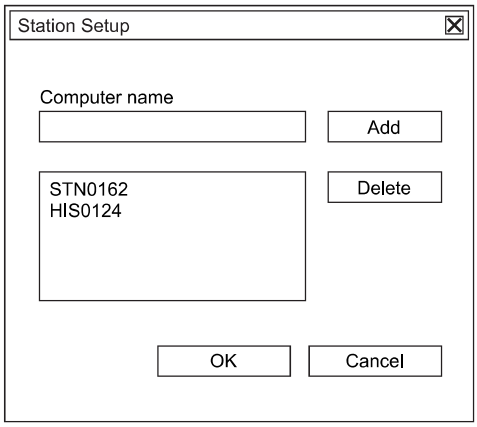


Figure I4.2.1-1 Station Setup dialog box

Station setting operations

Adding stations

1. To add the station (SENG or HIS), enter the computer name of the station in the [Computer name] field.
2. Click the [Add] button.
3. Click the [OK] button.
   The computer name of the station you entered is added to the tree view.

Deleting stations

1. Click one of the computer names displayed in the list in the Station Setup dialog box.
2. Click the [Delete] button.
3. Click the [OK] button.
   The selected station is deleted from the tree view.

I4.2.2 Setting Message Cache Service

Message Cache Service collects diagnostic information messages, SOE event messages and tripping information from the displayed SCS while the Diagnostic Information window or SOE View is running. If an SCS is set as the target of automatic data acquisition, data is automatically acquired regardless of the running of these windows.

The SCS to be the target of automatic acquisition and the maximum disk cache usage are set in the Setup dialog box.

Displaying the Setup dialog box

From the [File] menu of the Message Cache Tool window, select [Setup]. The Setup dialog box appears.

Setting items

The following describes the Items that should be set in the Setup dialog box.

- Target of automatic acquisition
  Specify an SCS to be the target of acquisition by Message Cache Service. Diagnostic information messages and SOE event messages of the SCS specified here are collected at the same time Message Cache Service starts up.
- Maximum Capacity of Disk
  The maximum message cache service size needs to be specified according to the actual usage. Up to the maximum disk capacity can be used for Message Cache Service.

IMPORTANT

Make sure that the disk used for DISK Cache by the Message Cache Service always has enough free space. (Default Max. Disk capacity: 800 MB) Monitoring for the Maximum Capacity is performed every 30 seconds. If the disk usage for the disk cache exceeds the Maximum Capacity, oldest files are deleted to keep the usage rate of the disk cache at 98 % to 100 %. For your information, 1 MB can contain about 8000 Diagnostic Information messages or 16000 events. The cache file is stored for each station. "SOE including Trip" and "Diagnostic Information messages" are stored separately in the cache file. If you want to keep the old cache files undeleted, save the files in a separate folder or media from the Save Disk Cache dialog box. To view the disk cache usage rate, use the Message Cache Tool: click [DISK Cache] in the tree view.

SEE ALSO

For more information about the details displayed in the disk cache usage status, refer to:

I4.2.4, “Displaying disk cache usage status” on page I4-45

For more information about Saving disk cache, refer to:

I4.2.6, “Saving disk cache” on page I4-49

I4.2.3 Displaying data acquisition status

Acquisition status of diagnostic information messages, SOE event messages and tripping information collected from an SCS by Message Cache Service are displayed.

How to display data acquisition status

To display the data acquisition status, click and expand [Data Acquisition] in the tree view on the left pane of the window, and then click the name of SCS. The acquisition status of data collected from the selected SCS by Message Cache Service is displayed in the client area on the right.

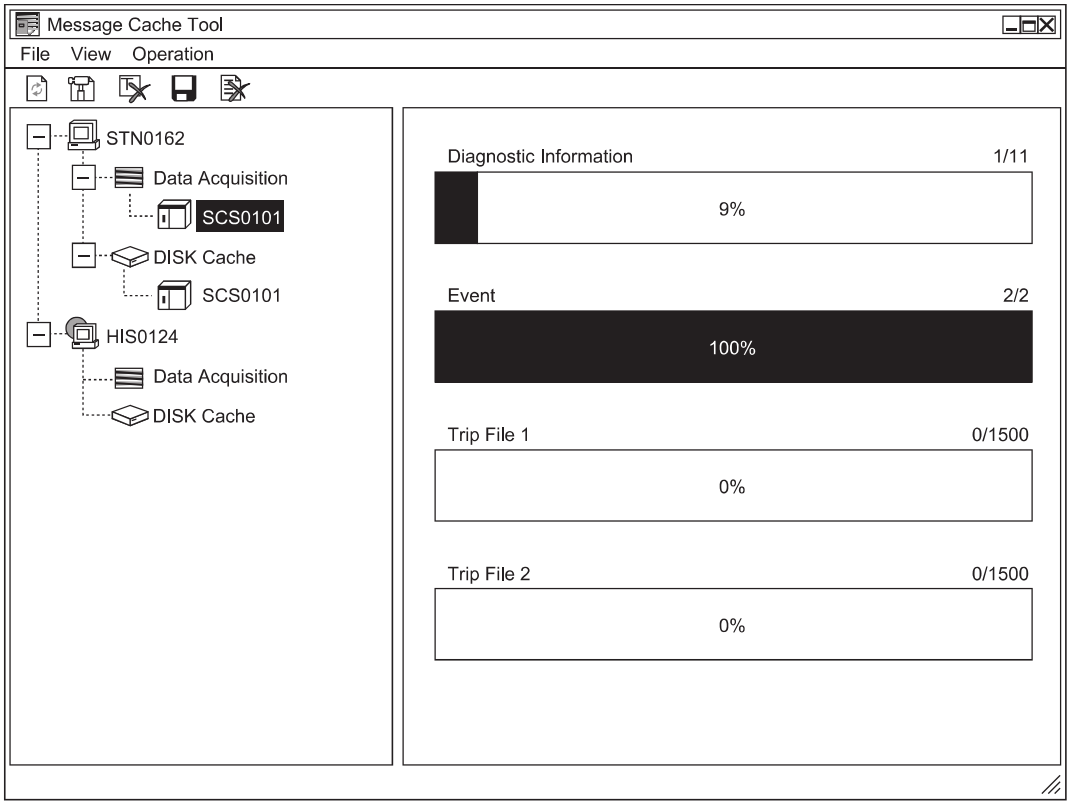


Figure I4.2.3-1 Data acquisition status

Items displayed for data acquisition status

The table below shows the items displayed for data acquisition status.

Table I4.2.3-1 Items displayed for data acquisition status

Displayed item	Description
Data Type	Displays the type of cache data (diagnostic information messages, SOE event messages and two types of tripping information).
Acquisition Status (Value)	Displays the number of items of diagnostic information messages, SOE event messages and tripping information acquired by Message Cache Service before "/", the diagnostic information messages, SOE event messages and tripping information that can be maintained by the SCS are displayed after the "/."
Acquisition Status (Bar Display)	Displays the percentage of data acquired by Message Cache Service with a bar. If no data is maintained by the SCS, "0%" is displayed on the bar. And, the bar is grayed out if data maintained by the cache service has not been updated for a certain period of time.

I4.2.4 Displaying disk cache usage status

With Message Cache Service, the cache data is stored on the hard disk until the data volume reaches the maximum disk cache usage set in the Setup dialog box. This function allows monitoring the disk cache (hard disk) usage status of Message Cache Service for all SCSs or each SCS managed by the station (SENG or HIS).

How to display disk cache usage status

The disk cache usage status is displayed using the following procedure for all or individual SCSs.

- Display for all SCSs
  Click [Disk Cache] in the tree view; the disk cache usage status for all SCSs managed by the station (SENG or HIS) is displayed.
- Display for each SCS
  Select the name of an SCS from the list of SCSs displayed by clicking [Disk Cache] in the tree view; the disk cache usage status for the selected SCS will be displayed.

Display for all SCSs

The disk cache usage status for the entire Message Cache Service running on each station (SENG or HIS) is displayed.

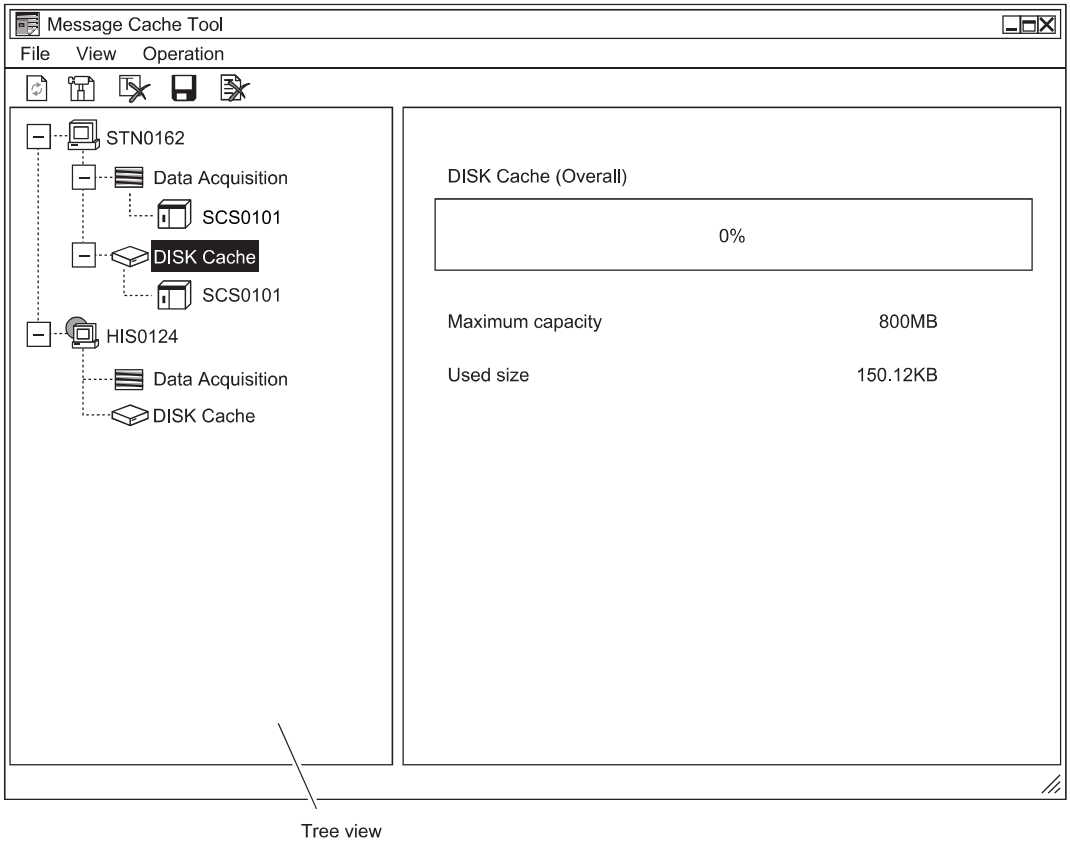


Figure I4.2.4-1 Disk cache usage status (display for all SCSs)

The table below shows the items displayed for the total disk cache usage status.

Table I4.2.4-1 Disk cache (display for all SCSs)

Displayed item	Description
Status of use (Bar Display)	Displays the percentage of the currently used disk space with a bar.
Maximum capacity	Displays the maximum disk space that can be used as disk cache. The maximum capacity is set in the Setup dialog box.
Used size	Displays the currently used disk cache space.

SEE ALSO For more information about the Setup dialog box, refer to:

I4.2.2, “Setting Message Cache Service” on page I4-43

Display for each SCS

The disk cache usage status for the selected SCS is displayed.

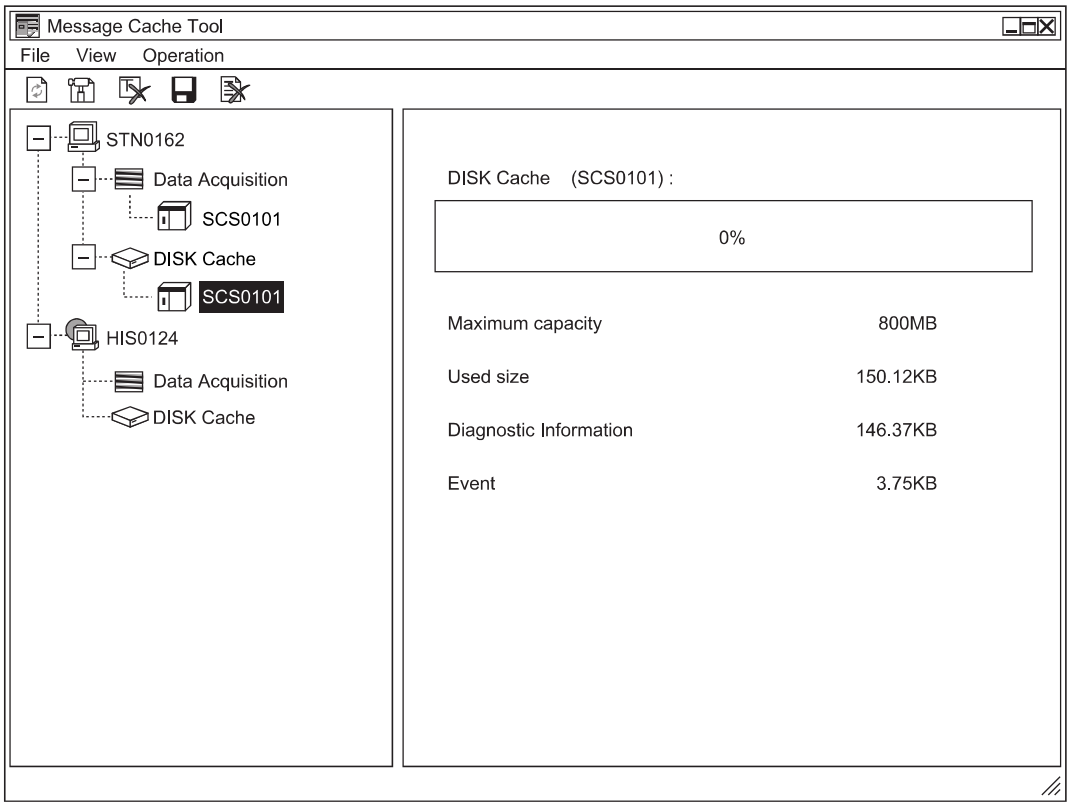


Figure I4.2.4-2 Disk Cache usage status (Display for each SCS)

The table below shows the items displayed for the each disk cache usage status.

Table I4.2.4-2 Disk cache (Display for each SCS)

Displayed item	Description
Status of use (Bar Display)	Displays the percentage of data acquired from the selected SCS out of the disk space with a bar.
Maximum capacity	Displays the maximum disk space that can be used as disk cache. The maximum capacity is set in the Setup dialog box.
Used size	Displays the volume of cache data acquired from the selected SCS.
Diagnostic Information	Displays the disk cache space used for diagnostic information messages.
Event	Displays the disk cache space used for SOE event messages.

SEE ALSO For more information about the Setup dialog box, refer to:

I4.2.2, “Setting Message Cache Service” on page I4-43

I4.2.5 Initialization of tripping information

Use the Initialize Trip Information dialog box to initialize the two types of tripping information held by the SCS.

After initialization, the SCS will get ready for collecting the tripping information in case the SCS trip occurs again.

Displaying the Initialize Trip Information dialog box

Select [Initialize Trip Information] from the [Operation] menu. The Initialize Trip Information dialog box appears.

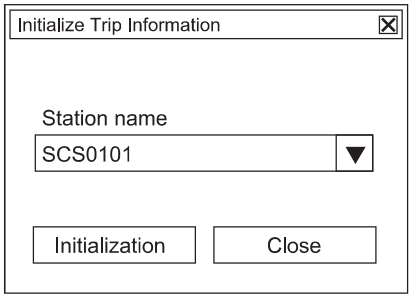


Figure I4.2.5-1 Initialize Trip Information dialog box

Initialize trip information operation

1. Select the SCS whose tripping information you want to initialize from the drop-down list box.
2. Click the [Initialization] button.
3. Click the [OK] button in the confirmation dialog box to initialize the tripping information.

IMPORTANT

When initializing the tripping information in a SCS, two files of SCS tripping information will be initialized together. Before initialization, make sure that the tripping information is saved in the SENG.

I4.2.6 Saving disk cache

Use this function to save the disk cache maintained in Message Cache Service to a separate folder or medium. The storage destination folder of the disk cache is specified by the Save Disk Cache dialog box. Saved disk cache can be viewed from SOE Viewer.

Displaying the Save DISK Cache dialog box

Select [Save Disk Cache] from the [Operation] menu. The Save DISK Cache dialog box appears.

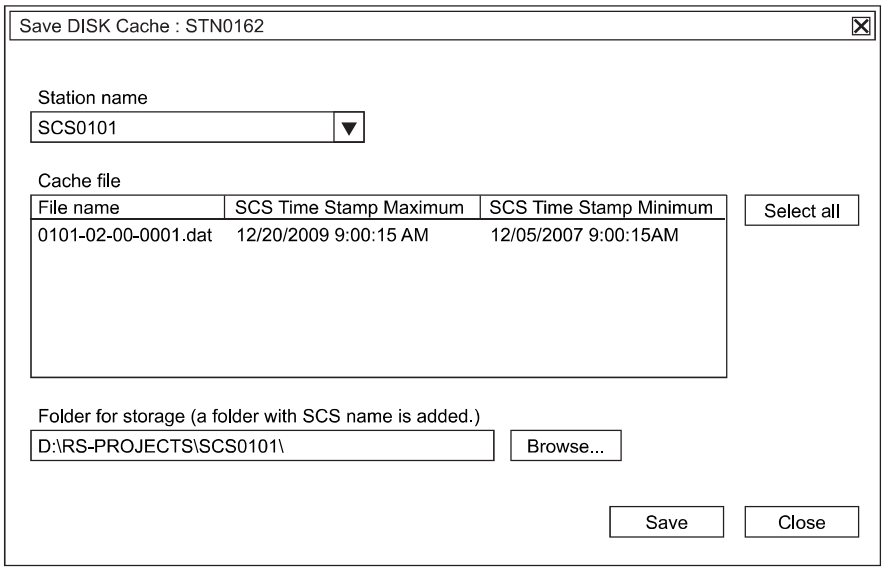


Figure I4.2.6-1 Save DISK Cache dialog box

How to specify the disk cache storage destination

1. Select a station name in the "Station name" field.
   Specify [All SCSs] in the "Station name" box to save the cache data of all SCSs.
2. Select the cache file to be saved from the "Cache file" field.
   Specify [Select All] to select all cache files of the specified SCS.
   If you have specified [All SCSs] in the "Station name" box , the cache files are grayed out.
3. Select a destination folder in which the disk cache is saved in the "Folder for storage" field. The folder with the selected SCS name is automatically created.
4. Click the [Save] button.
   The disk cache is saved in the specified folder.

SEE ALSO For more information about how to view the saved disk cache data, refer to:

"● Server Connection" on page I4-63

I4.3 SOE Viewer

On the SOE Viewer, events of ProSafe-RS can be analyzed. The event log in the specified SCS is uploaded to be displayed as event messages.

The SOE Viewer functions are as follows.

- The Event log (SOE event information and Diagnostic Information message) stored in SCS is uploaded to be displayed as event messages.
- Data sources of eight SCSs (including HIS for CENTUM Integration Structure) can be specified.
- Only event messages that you want to see can be filtered.
- A trip report can be generated. The report can be printed or exported as a CSV file.
- In case of CENTUM Integration Structure, process alarm messages from SCS can also be displayed.

The SOE Viewer has the following operation modes.

- Event Mode Operation
  It displays a list of event messages of SCS.

  In the case of CENTUM Integration Structure, HIS historical messages (process alarm messages of SCS) can also be displayed.
- Trip Mode Operation
  It displays a list of trip events of SCS. Detailed information about trip signals are also displayed.

I4.3.1 SOE Viewer window

The information managed by SOE Viewer is displayed in either the event mode or the trip mode. The window structure used in the event and trip modes is the same. This section explains the structure used for both modes.

Displaying SOE Viewer

Select [YOKOGAWA ProSafe] > [SOE Viewer].
SOE Viewer is displayed in the event mode.

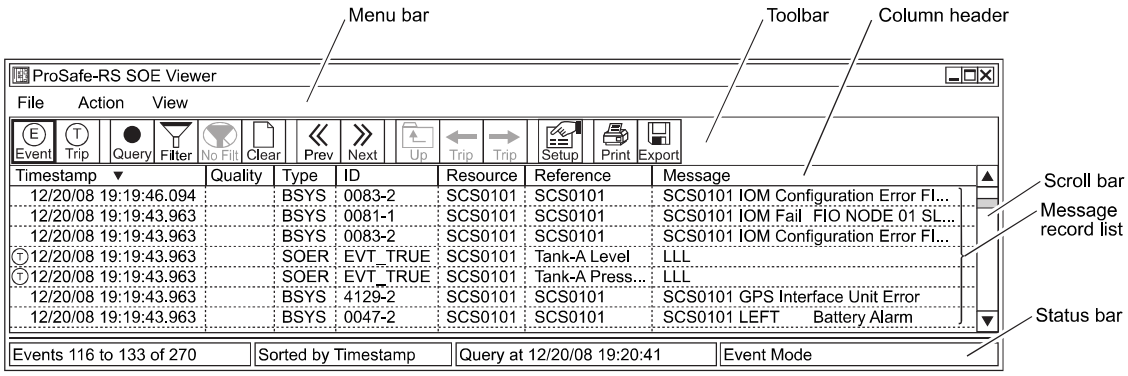


Figure I4.3.1-1 SOE Viewer (Event mode)

After starting the SOE Viewer, no event message is displayed in the message record list since no data source is specified. The event messages are displayed only after specifying the data source and running the query.

SEE ALSO For more information about setting the data source, refer to:

I4.3.2, “SOE Viewer configuration” on page I4-59

Menu bar

The menu bar provides the following menus.

- [File] menu
- [Action] menu
- [View] menu

Some of the commands in the menu bar are also provided in the toolbar. In addition to the commands available in the toolbar, the menu bar allows loading and saving property setting information (SOE Viewer configuration file) of SOE Viewer as well as setting the maximum number of message records.

File menu

Table I4.3.1-1 File menu

Menu item	Description
Load Configuration	Loads the settings made in the SOE Viewer Properties dialog box, which was saved by Save Configuration
Save Configuration	Saves current settings (SOE Viewer configuration) made in the SOE Viewer Properties dialog box
Print	Prints all or selected records from the message record list
Export List to file	Exports all records from the message record list to a CSV format file

Continues on the next page

Table I4.3.1-1 File menu (Table continued)

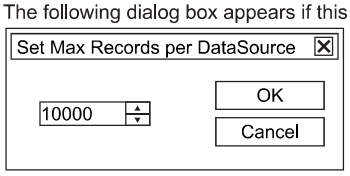
Menu item	Description
Exit	Closes SOE Viewer

Action menu

Table I4.3.1-2 Action menu

Menu item	Description
Execute Query	Executes queries based on the current settings made in the SOE Viewer Properties dialog box because the message record list is not updated automatically
Clear List	Deletes the current message record list
Filter Results	Applies filtering set in the SOE Viewer Properties dialog box to the current message record list
No Filter/Remove Filter	Removes filter restrictions from the current message record list
Set Max Records	Sets the maximum number of message records that can be retrieved by a query from one data source. If this limit is exceeded, remaining records are discarded and a warning message is generated (the setting range is from 10 to 65535, the default value is 10000). (*1)

*1: The following dialog box appears if this menu item is selected.



View menu

Table I4.3.1-3 View menu

Menu item	Description
Event Mode	Changes the SOE Viewer display to the event mode
Trip Mode	Changes the SOE Viewer display to the trip mode
Prev Page	Scrolls the list to display records in the previous page
Next Page	Scrolls the list to display records in the next page
Go up one level	Returns the display to the trip mode from the trip detail display
Prev Trip	Displays trip detailed display of the previous trip trigger event
Next Trip	Displays trip detailed display of the next trip trigger event
Toolbar	Shows or hides the toolbar
Status Bar	Shows or hides the status bar
Warning/Error Log	Displays the Warning/Error Log dialog box of SOE Viewer
Properties	Displays the SOE Viewer Properties dialog box

Toolbar

The toolbar of SOE Viewer has the following buttons.

Table I4.3.1-4 Toolbar buttons

Button	Name	Button	Name
	[Event Mode] Button		[Next Page] Button
	[Trip Mode] Button		[Up to Trigger List] Button
	[Execute Query] Button		[Prev Trip Detail] Button
	[Filter data] Button		[Next Trip Detail] Button
	[Clear Filter] Button		[Properties] Button
	[Clear List] Button		[Print] Button
	[Prev Page] Button		[Export data] Button

Event Mode button

This button provides the same function as [Event Mode] in the [View] menu.

The [Event Mode] button switches the display of SOE Viewer to the event mode. SOE Viewer remains in the event mode until the [Trip Mode] button is clicked. The [Event Mode] button cancels the operation activated by clicking the [Trip Mode] button. In the event mode, if a query is made, messages are retrieved from up to eight data sources specified in advance.

SEE ALSO For more information about Event mode, refer to:

I4.3.3, “Event mode operation” on page I4-68

Trip Mode button

This button provides the same function as [Trip Mode] in the [View] menu.

The [Trip Mode] button switches the display of SOE Viewer to the trip mode. SOE Viewer remains in the trip mode until the [Event Mode] button is clicked. The [Trip Mode] button cancels the operation activated by clicking the [Event Mode] button. In the trip mode, if a query is made, trip trigger events are retrieved from the trip signal file of SCS and displayed.

SEE ALSO For more information about Trip mode, refer to:

I4.3.4, “Trip mode operation” on page I4-71

Execute Query button

This button provides the same function as [Execute Query] in the [Action] menu.

The [Execute Query] button uploads all event logs matching the date/time and data source parameters specified in the SOE Viewer Properties dialog box from an SCS. Event logs are filtered and displayed in the message record list of SOE Viewer as event messages.

If one or more data sources have been set, the [Execute Query] button can be used in both the event mode and the trip mode.

Filter Data button

This button provides the same function as [Filter Results] in the [Action] menu.

The [Filter data] button displays in the message record list only event messages matching the filter parameters specified in the SOE Viewer Properties dialog box. If the filtering is set anew or changed, it is applied to the result of the current query and the display is updated. The [Filter data] button is only enabled when there are event messages in the message record list.

- ### Clear Filter button

  This button provides the same function as [No Filter/Remove Filter] in the [Action] menu.

  The [Clear Filter] button displays all event logs uploaded from an SCS as the result of the previous query as event messages in the message record list. It is not necessary to perform a query anew. The [Clear Filter] button is only enabled when the display has been filtered.

- ### Clear List button

  This button provides the same function as [Clear List] in the [Action] menu.

  The [Clear List] button deletes the message record list. Generate a new query command to retrieve and display event messages from an SCS again.

  The [Clear List] button is only enabled when there are messages in the message record list.

- ### Prev Page button

  This button provides the same function as [Prev Page] in the [View] menu.

  The [Prev Page] button scrolls the display so that the records in the previous page of the message record list are shown.

- ### Next Page button

  This button provides the same function as [Next Page] in the [View] menu.

  The [Next Page] button scrolls to the records on the next page of the message record list.

- ### Up to Trigger List button

  This button provides the same function as [Go up one] level in the [View] menu.

  The [Up to Trigger List] button returns the display from the trip detail display to the trip mode. The [Up to Trigger List] button is active in the Trip Detail display only.

- ### Prev Trip Detail button

  This button provides the same function as [Prev Trip] in the [View] menu.

  The [Prev Trip Detail] button displays the previous trip trigger event generated in the trip detail display. The [Prev Trip Detail] button is active in the Trip Detail display only.

- ### Next Trip Detail button

  This button provides the same function as [Next Trip] in the [View] menu.

  The "Next Trip Detail" button displays the next trip trigger event generated in the trip detail display. The "Next Trip Detail" button is active in the Trip Detail display only.

- ### Properties button

  This button provides the same function as [Properties] in the [View] menu.

  The ["Properties] button displays the SOE Viewer Properties dialog box. This dialog box is used to configure properties for the operations of SOE Viewer.

SEE ALSO For more information about the SOE Viewer Properties dialog box, refer to:

I4.3.2, “SOE Viewer configuration” on page I4-59

Print button

This button provides the same function as [Print] in the [File] menu.

The [Print] button prints out event messages included in the message record list. The [Print] button is only enabled when there are messages in the message record list.

SEE ALSO For more information about Print button, refer to:

"■ Printing" on page I4-68

Export data button

This button provides the same function as [Export List to file] in the [File] menu.

The [Export data] button exports event messages included in the message record list, to a CSV format file. The [Export data] button is only enabled when there are messages in the message record list.

SEE ALSO For more information about Export button, refer to:

"■ Exporting" on page I4-69

Message record list

The message record list executes queries and displays event messages uploaded from an SCS in response to the queries. Each line represents one event message.

Message color

The messages of trip trigger events are colored so that they can easily be distinguished from other event messages. User can specify the colors in the SOE Viewer Properties dialog box.

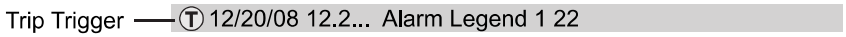


Figure I4.3.1-2 SOE message color code

Table I4.3.1-5 SOE message colors

Record type	Background color	Icon	Text color
Trip Trigger	Yellow (default)	Yellow circle with black "T"	Black
All Others	White (Windows default color)	None	Black

SEE ALSO For more information about the SOE Viewer Properties dialog box, refer to:

I4.3.2, "SOE Viewer configuration" on page I4-59

Sorting messages

Messages can be sorted in ascending or descending order using the upward and downward arrows in the column header.

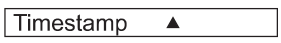


Figure I4.3.1-3 Sorting by timestamp (sorting in ascending order)

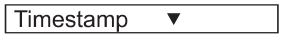


Figure I4.3.1-4 Sorting by timestamp (sorting in descending order)

Changing column width

If the width of a column or column header is too narrow to display the entire data and/or caption, as many characters as possible are displayed and the omitted characters are represented by an omission symbol (...).
The width of the columns can be changed by dragging the vertical boundary line between column headers.

Double-click the boundary line between column headers to adjust to the optimum width.

Changing display order of a column

To change the display order of a column, click the column header, keep the mouse button pressed and drag and drop it to the desired position.

TIP

The specified sorting order, column width and column order are saved in the SOE configuration file. These settings are restored when the SOE Viewer configuration file is uploaded using [Load Configuration] of the [File] menu.

Status bar

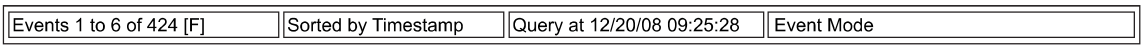


Figure I4.3.1-5 Status bar

The status bar is displayed at the bottom of the window. The status bar has four frames that display information related to the currently displayed message record list. The user can change the display width of the frames.

The information shown in each frame is explained as follows, starting from the leftmost frame.

- The total number of messages uploaded by a query from an SCS and the range of messages currently displayed
  If one or more filters are applied to the event messages displayed in the message record list, [F] is added at the end of the first status bar frame.

  For example, if a filter restricts the records to be displayed to 424 messages and each page displays 6 messages, the first frame of the status bar shows "Events 1 to 6 of 424 [F]."
- The column name currently used as the sorting key
- Date and time when the query was executed
- Display mode
  There are two display modes: fixed messages and temporary messages.

  The fixed messages indicate the current operating mode.

Table I4.3.1-6 Fixed messages

Message	Description
Event Mode	Indicates that SOE Viewer is in the event mode.
Trip Trigger Mode	Indicates that SOE Viewer is in the trip mode.
Trip Detail [Reference]	Indicates that SOE Viewer displays trip details. Reference information related to the current trip trigger event is also displayed.

The temporary messages indicate the current status during execution of a query.

Table I4.3.1-7 Temporary messages

Message	Description
Processing Query..	A query to a data source is being executed and SOE Viewer is waiting for the query result.
Loading Data..	Results of a query have been received and the Viewer is loading the messages into the dedicated memory.
Filtering Data..	The Viewer is filtering messages for display.

If a warning or error condition is generated during the operation of SOE Viewer, an exclamation mark icon is displayed in the display mode frame of the status bar.

Double-click the exclamation icon; the Warning/Error Log dialog box appears and displays warning and error message information. Click a message displayed in the Warning/Error Log dialog box to see the detailed information.



Figure I4.3.1-6 Exclamation icon

SEE ALSO For more information about warnings and error messages, refer to:

I4.3.5, “Troubleshooting SOE Viewer” on page I4-73

Event Detail dialog box

The Event Detail dialog box displays detailed information about event messages selected in the message record list. To display the Event Detail dialog box for messages displayed in the event mode or the Trip Detail Display window, double-click an event message or press the [Enter] key on the keyboard in the message record list.

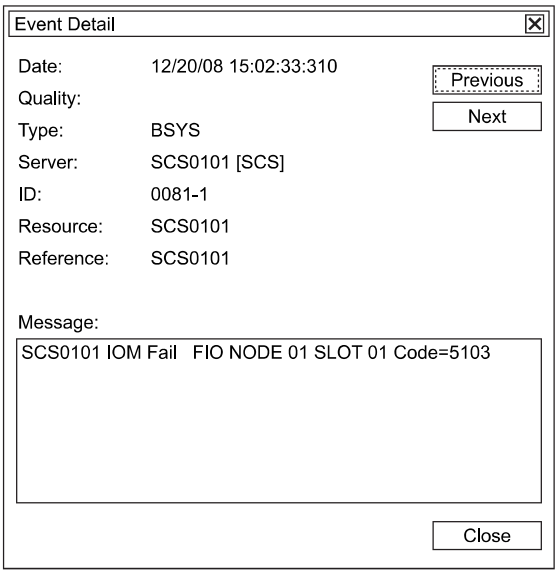


Figure I4.3.1-7 Event Detail dialog box

The information of data sources displayed in the Event Detail dialog box is summarized as follows.

Table I4.3.1-8 Event detail items

Event detail items	Description	SOE event information				Diagnostic information	HIS historical information
		DI	DO	AI	Internal variable		
Date (*1)	Date and time when a message is generated. The date format is specified in the SOE Viewer Properties dialog box. The time is displayed using the format hh:mm:ss:ttt where: hh = hours (24 hours), mm = minutes, ss = seconds and ttt = ms.	Time at which the SOE event information was generated in the SCS				Time at which the alarm is generated in an SCS	Time at which the alarm is generated in an SCS
Quality	Time synchronization information when an event occurs	I, B, V, <Blank> (*2)	-			-	-
Type	Message type	SOER (SOE event information)				BSYS (diagnostic information message)	Message category (Example: BSYS, BPRO) (*3)
Server [Type]	Name and type of the server that output a message	SCSddss [SCS](*4)				SCSddss [SCS] (*4)	HIS computer name [HIS]
ID	Message identifier	EVT_TRUE EVT_FALSE				Message ID-alarm class (e.g., 0047-2)	Message ID-alarm class or alarm priority (e.g., 1101-1)
Resource	Message reference station name	Station name (SCSddss) (*4)					
Reference	Special reference point of message	Comment entered for the input/output variable		Any character string assigned to a function block		Station name	Station name, tag name
Message	Message itself	Data value, numerical value (TRUE, FALSE)		Data value, character string (e.g., HTRP)	Data value, numerical value, BOOL, DINT, REAL	Message character string	Message character string

*1: "Timestamp" is displayed in the SOE Viewer window either in event mode or trip mode.
*2: The status of time synchronization on DI event generation is indicated with the following characters.
I: Not synchronized with the standard time.
B: Synchronized with the standard time but synchronization signals are not provided for some reason.
V: Not synchronized with the time on the SNTP server.
<Blank>: Synchronized with the IRIG-B signal when connected to an IRIG-B. Synchronized with the time on the SNTP server when an SNTP server is used on Vnet/IP.
*3: BSYS indicates a system alarm message and BPRO indicates a process alarm message.
*4: In SCSddss, dd indicates the domain number and ss indicates the station number.

To see event details of the previous message in the message record list, click the [Previous] button or press the [P] key on the keyboard. To see event details of the next message in the message record list, click the [Next] or press the [N] key on the keyboard. Click the [Close] button to close the Event Detail dialog box.

I4.3.2 SOE Viewer configuration

The data source settings for SOE Viewer is made in the SOE Viewer Properties dialog box. This section explains the operations performed in the SOE Viewer Properties dialog box: specifying of data sources and date ranges, filtering standards to be applied and general settings for SOE Viewer.

How to display the SOE Viewer Properties dialog box

Click [Properties] button in the toolbar or select [Properties] in the [View] menu; the SOE Viewer Properties dialog box appears.

General tab

The following items are specified in the "General" tab.

- Display or hide the Toolbar
- Select the toolbar icons to use small or large
- Display or hide the Status Bar
- Choose the SOE message color settings
- Display/suppress the Warning/Error Log dialog box

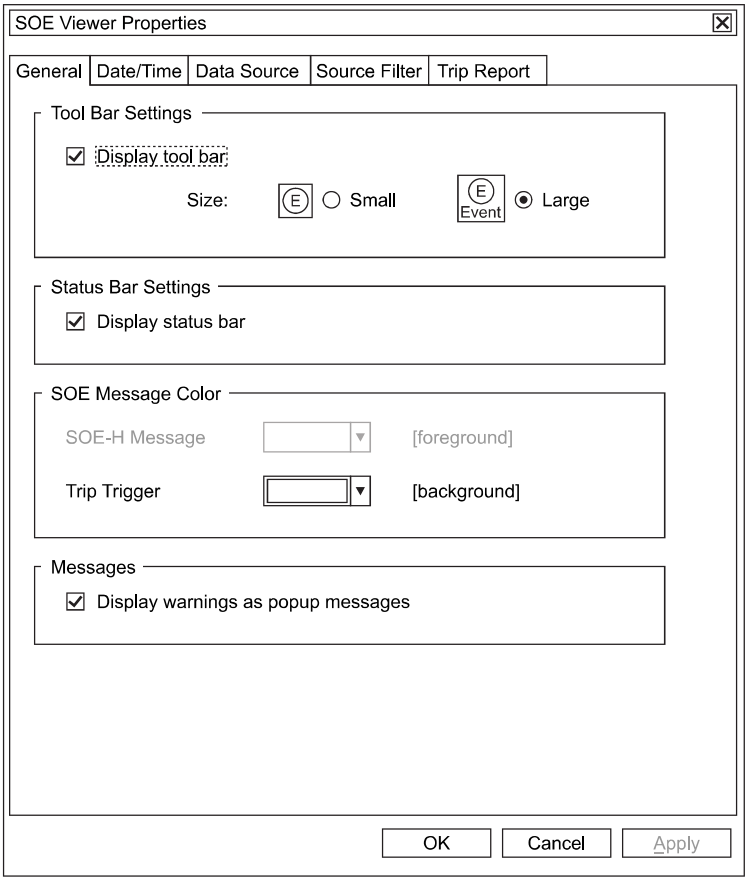


Figure I4.3.2-1 General tab of SOE Viewer Properties dialog box

Tool bar settings

To display the toolbar, select the [Display tool bar] check box. To display only tool buttons on the toolbar, select the [Small] radio button for "Size." To display tool buttons along with an identifying caption, select the [Large] radio button for "Size."



Figure I4.3.2-2 Small button



Figure I4.3.2-3 Large button

● Status bar settings

To display the status bar, check the [Display status bar] check box.

● SOE message color

Select the background color of trip trigger events in this section. Click the downward arrow to display the color picker. Use the color picker to select the desired color. The default background color for trip trigger events is yellow.



Figure I4.3.2-4 Color picker

● Messages

Select the [Display warnings as popup messages] check box to notify about query warnings via an interactive pop-up dialog box. If this check box is not selected, it becomes necessary to display the Warning/Error Log dialog box to view query warnings.

■ Date/Time tab

The "Date/Time" tab is used to specify the range of date and time of messages uploaded from an SCS by the query in the event mode or the trip mode. The date/time format is also specified in this tab.

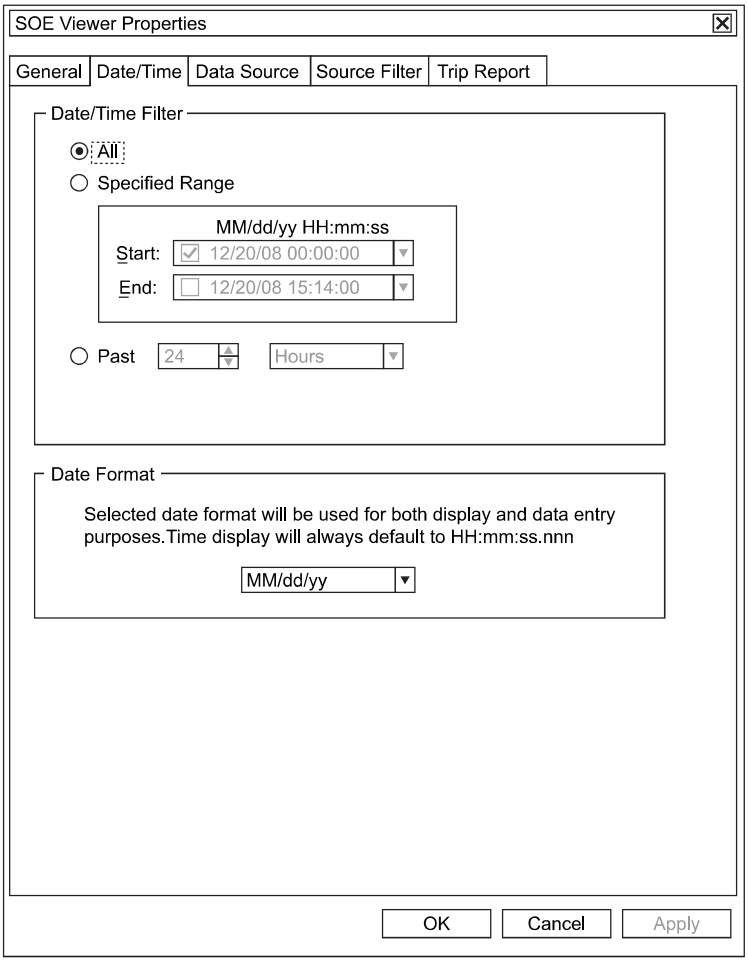


Figure I4.3.2-5 Date/Time tab of the SOE Viewer Properties dialog box

Date/Time Filter

The date/time filter can be specified in the following manners:

- [ALL]
- No date range is specified. All event messages that have occurred within the past one year are displayed as a result of query for each data source. Note that the number of event messages displayed is limited by the maximum number of records. When the number of total messages exceeds the maximum number of records for display, the latest messages cannot be displayed. In this case, a criterion with specified dates should be used for displaying the messages. Select [Specified Range] or [Past] if you want to display messages that have occurred within a specific period.
- [Specified Range]
  A specific date/time range is specified as the target period of queries. This range can be specified by the start date/time or the end date/time, or both. To include a start or end date/time in the definition of the specific range, select the relevant check box. If the start date/time is not specified, the date/time of the oldest event saved in an SCS is set as the start date/time. If the end date/time is not specified, the date/time of the most recently generated event message is set as the end date/time.

  To change the start or end date, enter a new date or click the downward arrow on the right side of date/time; a calendar appears. The current date is highlighted in red. Click the desired date.



To change the start time or end time, enter the time using 24-hour format.

Figure I4.3.2-6 Calendar

TIP

The values of currently selected date/time unit (i.e., hours or minutes) can be increased or decreased by pressing the [+] or [-] key on the keyboard.

- [Past]
  A range of messages generated in the past is specified as the target period of queries as the time span of hours or days. The time span is specified in units of minutes, hours, or days. If 0 days are specified, events and alarms generated at 0:00 a.m. of the current day and onward are uploaded from the SCS in question. If a number of days is specified, the target hours start from 0:00 of the day. For example, if 1 day is specified, the target hours start from 0:00 a.m. the day before.

Date Format

All dates within SOE Viewer are displayed using the date format specified here. Select a desired date format from the pop-up list. The following formats are available.
MM/dd/yy, dd/MM/yyyy, MM/dd/yyyy,

d-MMM-yy, dd/MM/yy, d-MMM-yyyy

Example 1: 30/10/2009

Example 2: 30-OCT-2009

TIP

If the message record list or the Event Detail dialog box is being displayed, the setting of the date format is reflected the next time a query is executed.

Data Source tabs

Eight "Data Source" tabs are prepared for the data sources; they are used to specify the data source and type of event messages.

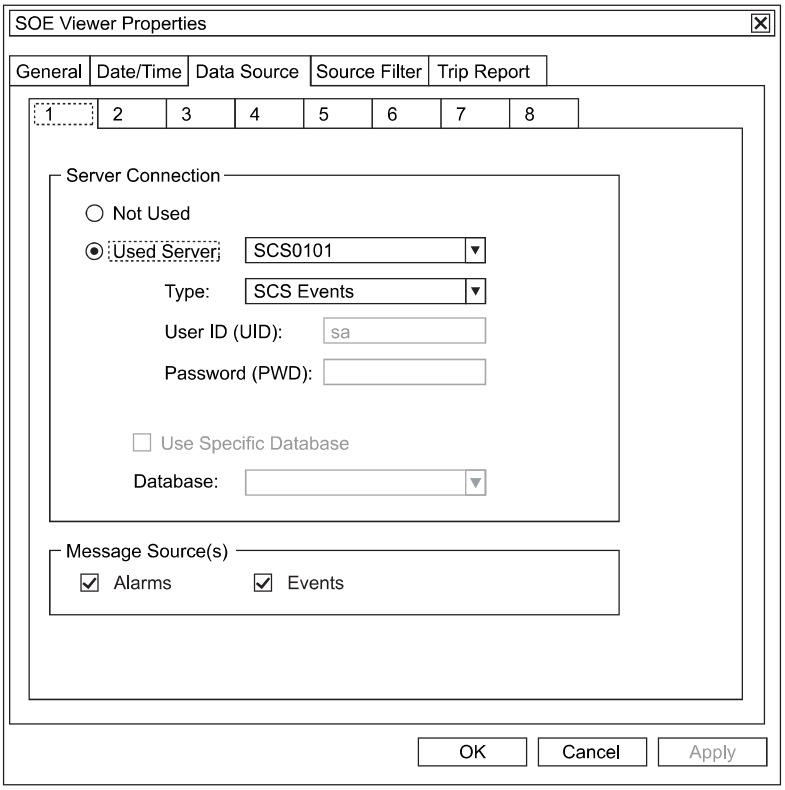


Figure I4.3.2-7 Data Source tab of SOE Viewer Properties dialog box

TIP To disable a server temporarily, select [Not Used]. Other settings made for the server are not deleted.

Server Connection

A data source is specified by entering a station name of an SCS. When the user executes a query, event logs are uploaded from the specified SCS and displayed in the event mode in SOE Viewer as event messages. To specify a data source, select [Used Server].

In the case of a CENTUM integration structure, HIS historical information (process alarms of an SCS) can also be specified as the data source. To do so, enter the computer name of HIS into the [Used Server] field. If you want to view the cached data saved using the Message Cache Tool, enter into the [Used Server] field the full path to the folder where the cash data is stored.

The setting items for Server Connection are shown in the table as follows.

Table I4.3.2-1 Server Connection setting items

Setting item	SCS event message	HIS historical information
Used Server	SCSddss (*1) or full path to the folder where the cash data is stored	HIS computer name
Type	SCS Events	CENTUM HIS Log

*1: Specify a domain number for dd and a station number for ss in SCSddss.

If the data source is not used, select [Not Used] to avoid a generation of error messages.

Message Source(s)

Specify the type of event messages retrieved from an SCS by a query.
If the [Alarms] check box is selected, diagnostic information messages are the target of collection. If the [Events] check box is selected, SOE event information are the target of collection. Select either the [Alarms] or [Events] check box, or both. Both check boxes are selected by default.

Source Filter tab

If a query is executed with the date range specified in the "Date/Time" tab while one or more filter parameters are specified, the filter is applied to event messages displayed in the message record list. Filter parameters can be specified for each data source. These filter parameters are automatically applied to the current query result. It is not necessary to execute a query anew in SOE Viewer even if filter parameters are changed.

Server Connection

This section displays the server name and the type of data source related to the filter specified in this tab. These fields are grayed out and cannot be changed.

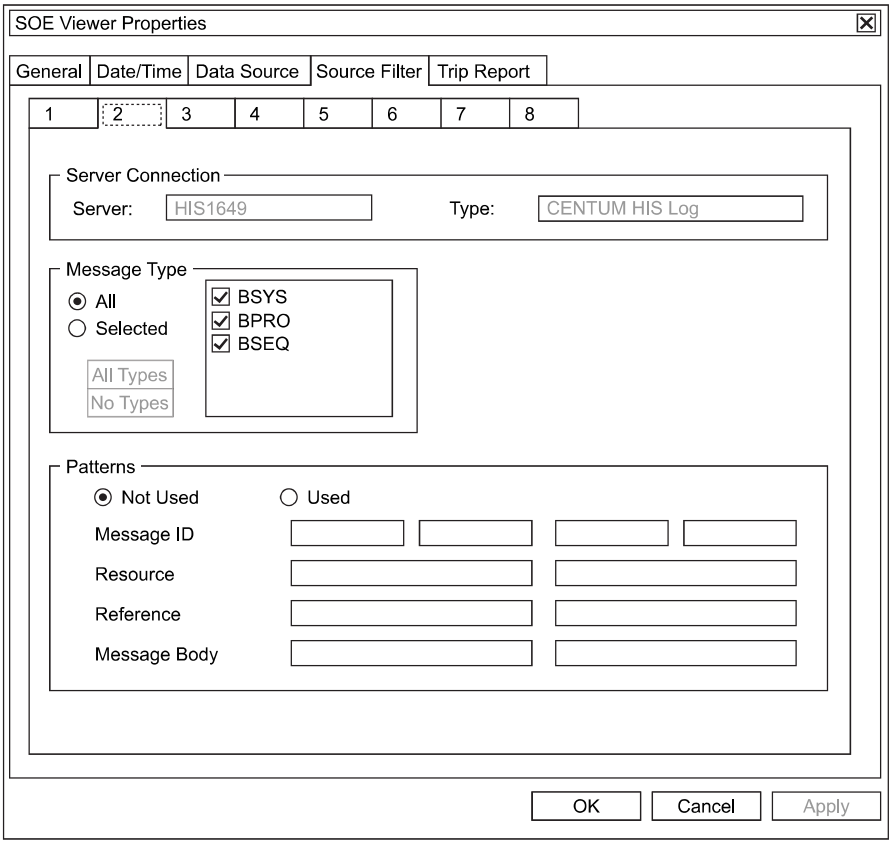


Figure I4.3.2-8 Source Filter tab of SOE Viewer Properties dialog box (example when Server Type is CENTUM HIS log)

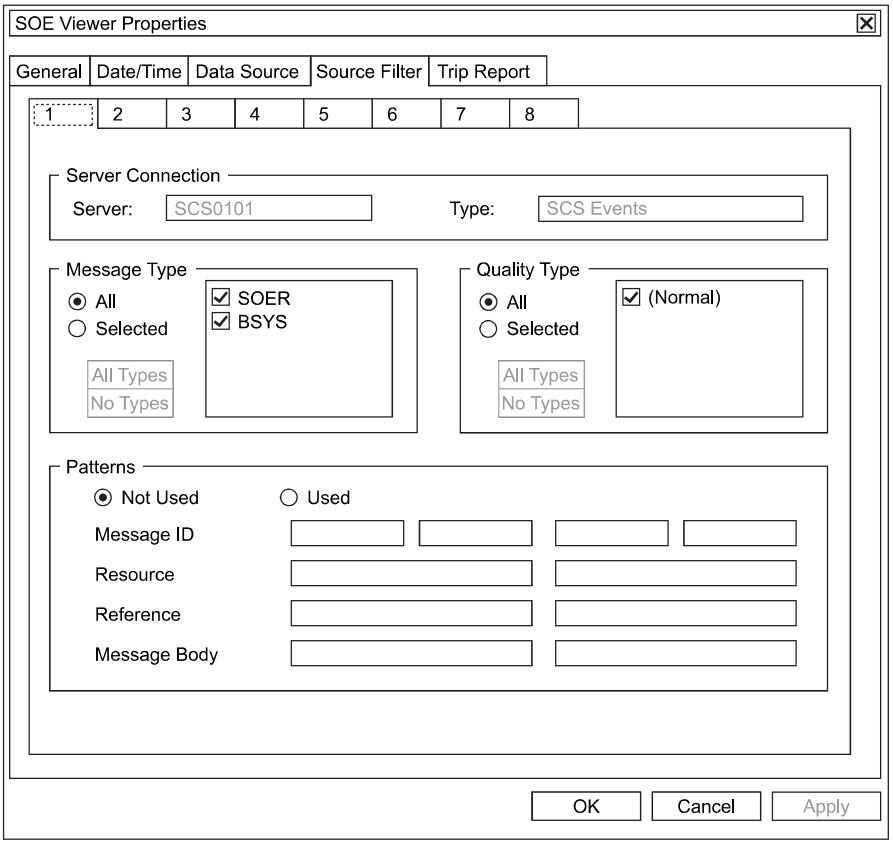


Figure I4.3.2-9 Source Filter tab of SOE Viewer Properties dialog box (example when Server Type is SCS events)

Message Type

It is possible to select the messages displayed in SOE Viewer according to the specific message types. The lists of event messages to which the message type selections are applied are automatically executed from the data source during a query.

- [All]
  Select all message types without restrictions.
- [Selected]
  Restrict the display to only the specified message type. Check the check box of the desired type.

  [All Types]: Select all message types at once.

  [No Types]: Deselect all message types at once.

Quality Type

This filter is only valid when the server type is SCS Events.

It is possible to select the event messages displayed according to the quality of the attached time stamp information.

- [All]
  Select all quality types without restriction.
- [Selected]
  Restrict the display to only the specified quality type. Check the check box of the desired type.

  [All Types]: Select all quality types at once.

  [No Types]: Deselect all quality types at once.

Patterns

It is possible to select the event messages displayed to those including the character string pattern specified in the relevant field.

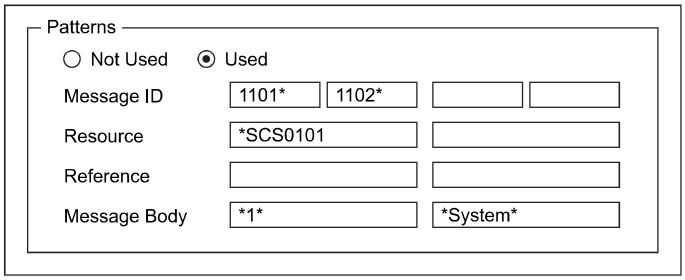


Figure I4.3.2-10 Source Filter tab (Patterns)

- [Not Used]
  No selections related to character string patterns are applied.
- [Used]
  Selections related to character string patterns are applied. Specify the desired patterns to be matched.

It is possible to use wildcards of asterisks (*) and question marks (?) in the character string patterns. "*" placed in front of a character string indicates any number of arbitrary characters before the character string. If an asterisk is placed after a character string, the wildcard indicates any number of characters after the character string. "?" is a wildcard indicating one arbitrary character.

If multiple character string patterns are specified for one pattern type (e.g., multiple character string patterns are specified for Message ID only), the filtering result includes all messages matching any of the specified patterns (patterns are combined using OR condition).

If two or more pattern types are specified (e.g., a character string pattern is specified for Message ID and Resource), the result includes only messages that match all of the specified patterns (patterns are combined using AND condition).

In the pattern example shown in the previous figure, all messages satisfying the following conditions are displayed:

Message(s) "whose message ID starts with 1101 or 1102" and "whose resource name ends with SCS0101" and "whose message text includes ‘1’ or ‘System’ somewhere in the message."

TIP Specified filter patterns are not deleted by selecting [Not Used] in order to avoid re-entering conditions from scratch in case the specified filter patterns may be needed again. If the patterns are needed again, change the option to [Used].

Trip Report tab

The "Trip Report" tab is used to specify the trip source. It is only valid when the server type is SCS Events. To display messages in the trip mode in SOE Viewer, specify the trip source in the "Trip Report" tab and execute a query.

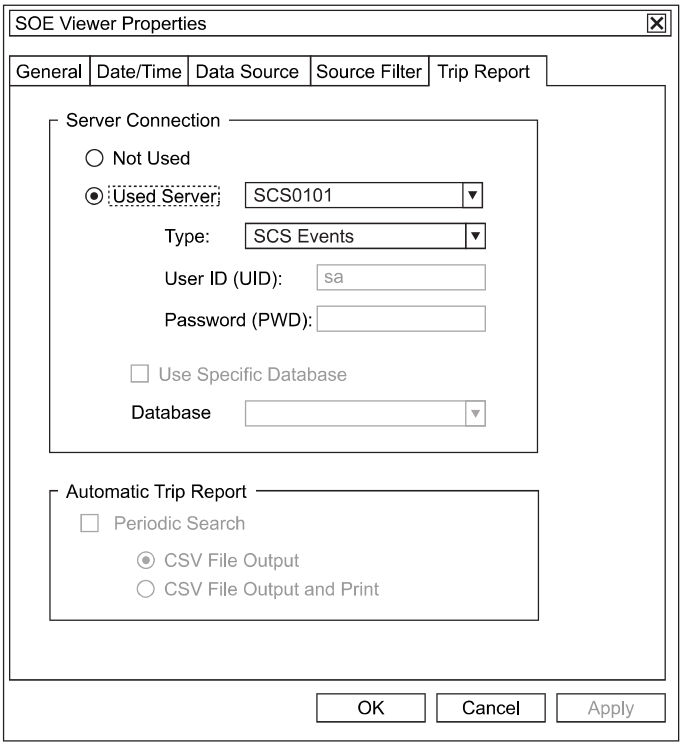


Figure I4.3.2-11 Trip Report tab of the SOE Viewer Properties dialog box

Server Connection

Specify the destination of the trip source. To specify a trip source, select [Used Server]. Specify SCSddss (dd: domain number, ss: station number) for the server name. Select [SCS Events] from the drop-down list of [Type].

Saving settings

Click the [OK] button to save the changes to settings made in the SOE Viewer Properties dialog box and close the dialog box.
Click the [Cancel] button to close the dialog box without saving the changes.

To retain the configured property settings for use in future SOE View sessions, select [Save Configuration] in the [File] menu.

I4.3.3 Event mode operation

In this mode, SOE Viewer displays event messages of an SCS in a list format. This allows analyzing events from relevant information using filtering. This section explains typical operations in the event mode of SOE Viewer.

Activating the Event mode

When you start SOE Viewer, the event mode is automatically activated. When you start up SOE Viewer for the first time, no data source is setup. Specify one or more data sources in the SOE Viewer Properties dialog box.
Properties can be set by reading an SOE Viewer configuration file set and saved in advance. If an SOE Viewer configuration file is read, the name of the file is displayed in the title bar of SOE Viewer.

If it is desired to change the display to the event mode while SOE Viewer is in the trip mode, click [Event Mode] button on the toolbar. Alternatively, select [Event Mode] in the [View] menu. SOE Viewer switches to the event mode.

Data source query

If a query is executed, event messages matching the date/time and the data source parameters specified in the SOE Viewer Properties dialog box are acquired, up to the maximum number of records. The event messages are displayed in the message record list of SOE Viewer. In order to execute a query, click [Execute Query] button on the toolbar. Alternatively, select [Execute Query] in the [Action] menu.

Message filtering

The filtering function is used to select only messages of interest among the displayed messages. Filtering by data source is performed based on the message type, message status and filtering pattern settings in the "Source Filter" tab of the SOE Viewer Properties dialog box. It is possible to set different filtering settings for each data source.
In order to apply filtering, click [Filter data] button on the toolbar. Alternatively, select [Filter Results] in the [Action] menu. The results of the current query are filtered automatically; it is not necessary to execute a query anew.

To view all messages without applying filtering, click [Clear Filter] button on the toolbar. Alternatively, select [No Filter/Remove Filter] in the [Action] menu.

Printing

It is possible to print messages displayed in the message record list. Select [Print] button on the toolbar or [Print] in the [File] menu. The standard Windows print dialog box appears.
The orders of columns and sorting used for the printout match with the display in SOE Viewer. The following example shows a printout from SOE Viewer.

Query at 12/20/08 13:51:42 SOE Viewer Report Page1

Timestamp	Quality	Type	ID	Resource	Reference	Message
12/20/08 14:52:27.740		BSYS	4125-1	SCS0101	SCS0101	SCS0101 IOM Channel Error ...
*12/20/08 14:52:27.740		SOER	EVT_TRUE	SCS0101	Tank-A Level	LLL
*12/20/08 14:52:27.740		SOER	EVT_TRUE	SCS0101	Tank-A Pressure	LLL
12/20/08 14:52:43.244		BSYS	4180-4	SCS0101	SCS0101	SCS0101 Security Level=1 ...
12/20/08 14:52:44.644		BSYS	4173-4	SCS0101	SCS0101	SCS0101 Writing Security Pa ...
12/20/08 14:52:48.744		BSYS	4180-4	SCS0101	SCS0101	SCS0101 Security Level=0 ...

All Messages from [Begin] to [END]

Figure I4.3.3-1 Example of printout

TIP "*" (asterisk) in the Timestamp column indicates a trip trigger event.

A footer is combined from the following character strings according to the messages printed, and then attached to the printed pages.

"All" or "Selected" or "Filtered" + "Messages from" + "StartDate" to "EndDate"

Either one of the "All," "Selected" or "Filtered" is printed out.

- All
  Indicates that all event messages in the printing range are specified.
- Selected
  Indicates that only event messages selected in the printing range are specified.
- Filtered
  Indicates that event messages are filtered.
- StartDate
  Indicates the start date/time of a query request.
  [Begin] means that no specific start date is specified.
- EndDate
  Indicates the end date/time of a query request.
  [End] means that no specific end date is specified.

Exporting

It is possible to export data displayed in the message record list to a CSV format file. It is also possible to specify whether or not to apply filtering when exporting the data.
Select the [Export data] button on the toolbar or [Export List to file] in the [File] menu.

The Export SOE Viewer data dialog box appears. Specify the name and location of a file and click [Save].

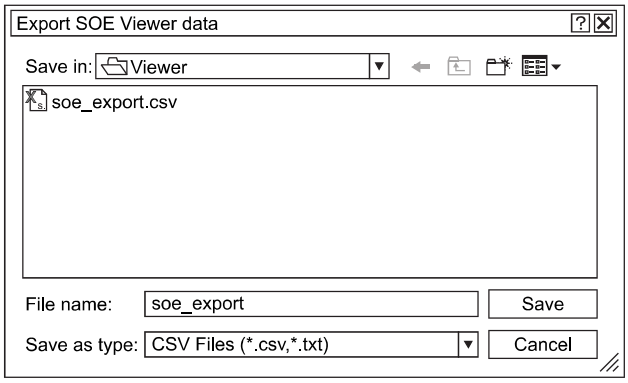


Figure I4.3.3-2 Export SOE Viewer Data dialog box

The first line of a CSV file describes the output column format. The order of columns of an exported file is always the same, even if the column order has been changed in SOE Viewer. The header line is as follows.

Timestamp, Quality, Type, ID, Alarm State, Resource, Reference, Message

```
Timestamp,Quality,Type,ID,Alarm State,Resource,Reference,Message
 *12/05/07    15:02:33.310,,SOER,EVT_TRUE,,SCS0101,Tank-A Level,LLL
 *12/05/07    15:02:33.310,,SOER,EVT_TRUE,,SCS0101,Tank-A Pressure,LLL
  12/05/07    15:02:33.317,,BSYS,4129-2,,SCS0101,SCS0101,SCS0101    GPS Interface Unit Error
  12/05/07    15:02:33.310,,BSYS,0083-2,,SCS0101,SCS0101,SCS0101    IOM Configuration Error FIO NODE 01 SLOT 01
  12/05/07    15:02:33.310,,BSYS,0083-2,,SCS0101,SCS0101,SCS0101    IOM Configuration Error FIO NODE 01 SLOT 03
  12/05/07    15:02:33.310,,BSYS,0083-2,,SCS0101,SCS0101,SCS0101    IOM Configuration Error FIO NODE 01 SLOT 05
  12/05/07    15:02:33.310,,BSYS,0081-1,,SCS0101,SCS0101,SCS0101    IOM Fail FIO NODE 01 SLOT 01 Code = 5103
  12/05/07    15:02:33.310,,BSYS,0081-1,,SCS0101,SCS0101,SCS0101    IOM Fail FIO NODE 01 SLOT 03 Code = 5103
  12/05/07    15:02:33.310,,BSYS,0081-1,,SCS0101,SCS0101,SCS0101    IOM Fail FIO NODE 01 SLOT 05 Code = 5103
  12/05/07    15:02:26.841,,BSYS,0047-2,,SCS0101,SCS0101,SCS0101    LEFT     Battery Alarm
  12/05/07    15:02:16.801,,BSYS,0451-2,,SCS0101,SCS0101,SCS0101    LEFT     Control
  12/05/07    15:02:16.801,,BSYS,0011-2,,SCS0101,SCS0101,SCS0101    LEFT     Fail (V STOP   Code= 0814 0000 0000 0000)
  12/05/07    15:02:16.801,,BSYS,0001-2,,SCS0101,SCS0101,SCS0101    LEFT     Manual Reset Start
  12/05/07    15:01:57.610,,BSYS,4173-4,,SCS0101,SCS0101,SCS0101    Writing Security Password to Flash Memory Succeeded
  12/05/07    15:01:48.510,,BSYS,4173-4,,SCS0101,SCS0101,SCS0101    Writing Security Password to Flash Memory Succeeded
```

Figure I4.3.3-3 Example of CSV file

TIP

"*" (asterisk) in the Timestamp column indicates a trip trigger event.

I4.3.4 Trip mode operation

In this mode, SOE Viewer displays only trip trigger events specified as trip signals in a list format. It also displays detailed information generated near a specified trip trigger event for analysis. This section provides an overview of the trip mode of SOE Viewer and information displayed in the trip detail display.

Activating the Trip mode

Click [Trip Mode] button on the toolbar or select [Trip Mode] in the [View] menu. SOE Viewer switches to the trip mode.
The trip trigger event list is blank until a query is executed. Once a query is executed, trip signals in the specified date range are uploaded from the specified data source and the trip trigger events are displayed in the trip trigger event list. This data is displayed again when the trip mode is activated again.

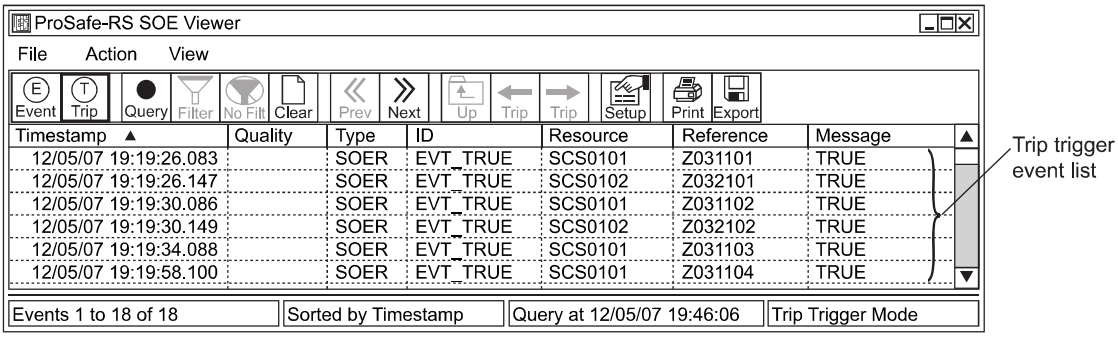


Figure I4.3.4-1 SOE Viewer (Trip mode)

Trip detail display

The Trip Detail Display window displays detailed trip records related to the trip trigger event selected in the trip mode of SOE Viewer. If you double-click a trip trigger event in the trip mode or press the [Enter] key on the keyboard, a query is automatically executed for the specified data source. The time range to be displayed in the Trip Detail Display window is determined based on the selected trip trigger event and approximately 500 events and 1000 events before and after the selected trip trigger event, respectively, and all the events generated in the time range, including other SCS events, are displayed as detailed trip records.

The initial display of the trip detail record list is a page that includes the selected trip trigger event.

The display mode frame of the status bar shows Trip Detail followed by the Reference information related to the current trip trigger event.

In the Trip Detail Display window, the [Up to Trigger List], [Prev Trip Detail] and [Next Trip Detail] buttons are enabled on the toolbar.

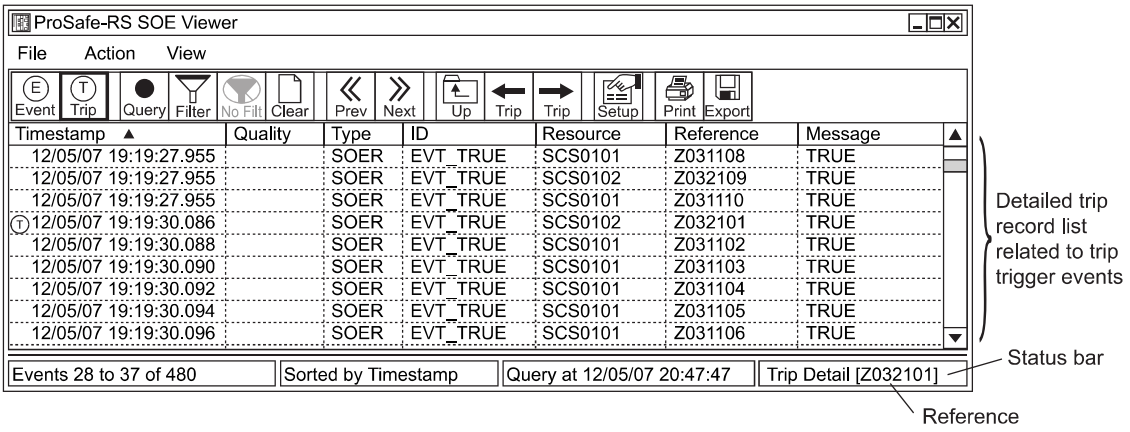


Figure I4.3.4-2 Trip Detail Display window

I4.3.5 Troubleshooting SOE Viewer

SOE Viewer displays warnings and error messages in the Warning/Error Log dialog box. Errors occur in file input/output or database access operations. This section explains how warnings and error messages are displayed and the actions to be taken.

Notification via the Warning/Error Log dialog box

If a warning or error condition occurs during operation of SOE Viewer, an exclamation icon is displayed in the display mode field of the status bar at the bottom of the SOE Viewer window. If you double-click the icon, the Warning/Error Log dialog box appears. This dialog box also appears by selecting [Warning/Error Log] in the [View] menu.

Click a message in the Log column of the Warning/Error Log dialog box to view detailed information about the message in the [Detail] area. Up to 1000 warning/error messages can be displayed. If more than 1000 messages have been recorded, messages are deleted starting from the oldest message.



Figure I4.3.5-1 Exclamation icon

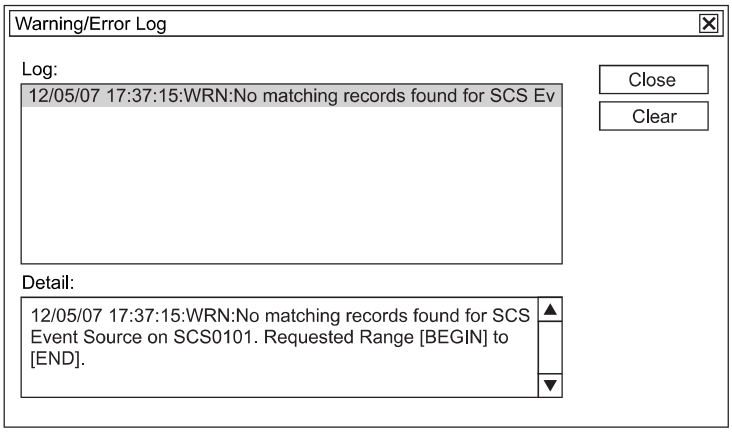


Figure I4.3.5-2 Warning/Error Log dialog box

Click the [Clear] button to delete all messages displayed in the Warning/Error Log dialog box. Click the [Close] button to close the dialog box.

The tables below show error messages and warning messages that may be generated.

Table I4.3.5-1 Error messages

Message	Explanation	Action
Error loading configuration file [Filename]	Uploading the specified SOE Viewer configuration file failed.	Check that the specified file name and path name are correct and perform the upload operation again.
Error on file [Filename] Cause: An attempt was made to access Event past its end.	Uploading the specified SOE Viewer configuration file failed. The file was found but the data or format of the file is illegal.	Upload settings from a normal SOE Viewer configuration file or use the SOE Viewer Properties dialog box to make the settings manually.

Continues on the next page

Table I4.3.5-1 Error messages (Table continued)

Message	Explanation	Action
Unable to connect to HIS server: [ServerName] Error 0x20000116 on HIS OpenLog( )	SOE Viewer failed to make a query for messages from the specified HIS server. An HIS log file cannot be opened.	Check that the specified server name and path name are correct. Check that network communication between the HIS server and SOE Viewer PC is functioning correctly. Check also that there is at least one "Daily Hishist log" file in the HIS corresponding to the requested date range.
Could not obtain Cache Data.	Cache data could not be acquired.	The message cache service is not running and/or in the process of starting up. Wait for a while and try again.
SOE viewer package of ProSafe-RS not installed.	The ProSafe-RS package has not been installed.	The problem may be solved by re-installing the ProSafe-RS package. If the error persists even if the package is re-installed, contact the service department.
Could not obtain V net address. Check [Used Server:].	Network address of the control bus could not be acquired.	Check that the correct server name is entered in the [Used Server] field.
librhhmscache.dll is damaged.	A program file is damaged.	The problem may be solved by re-installing the ProSafe-RS package. If the error persists even if the package is re-installed, contact the service department.

Table I4.3.5-2 Warning messages

Message	Explanation	Action
No matching records found for [SCS/HIS] Event Source on [ServerName]	No record was found in the date range requested in the specified server.	This occurs under normal circumstances as well. Expand the date range of messages on which queries are performed as necessary.
Results from [SCS/HIS] Event Source on [ServerName] exceeded limit.	The number of records in the date range requested for the specified server exceeded the specified limit. Records outside the range are discarded.	Make the requested date range of messages smaller or make the maximum number of records (MaxRecordsPerSource) as large as possible.
Input a correct SCS name into [Used Server:]. (For example, SCS0101) (*1)	The format of the entered SCS name is illegal.	Enter the correct SCS name. The correct SCS name format is SCSddss (dd: domain number, ss: station number).

*1: Warnings are notified via pop-up dialog boxes even if the [Display warnings as popup messages] check box is disabled.

Notification in the Error dialog box and the Warning dialog box

If an error or warning is generated, a pop-up dialog box appears to notify about the error message or warning message at the time of occurrence.

Messages displayed in the Error and Warning dialog boxes can also be viewed in a list in the Warning/Error Log dialog box.

Error message display

Errors generated during operation of SOE Viewer are notified via the Error pop-up dialog box. If an error occurs while executing a query, the user can cancel the query request or retry the query for the next specified data source.



Figure I4.3.5-3 Error dialog box

Click the [Retry] button to retry the query for the next specified data source and click the [Cancel] button to cancel the query request.

Warning message display

Warnings generated while executing a query for a data source are also notified via the Warning pop-up dialog box. The Warning dialog box appears if you select the [Display warnings as popup messages] check box in the "General" tab of the SOE Viewer Properties dialog box.

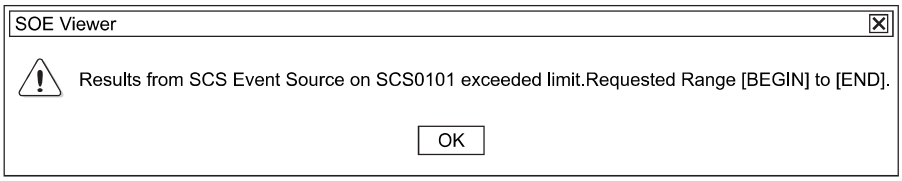


Figure I4.3.5-4 Warning dialog box

Click the [OK] button to close the Warning dialog box.

I4.4 Master database offline download

During master database offline download, the master database stored in the SENG is loaded to an SCS. Since the downloaded SCS database is identical to the master database, it is possible to download the information downloaded previously to the SCS even while changing the work database of an SCS project.

Use this download function to once again download the database that was previously downloaded; in the case, for example, when the CPU module of an SCS is replaced. This download is not required when one of a pair of redundant CPU modules is replaced.

Procedure for master database offline download

What to do before master database offline download

Use the SCS security level operation function to set the SCS security level to Level 0.

Start the master database offline download

1. Select [Controller] from the [Tools] menu of SCS Manager.
   The [Controller] launcher menu appears.
2. From the Controller Launcher menu, select [Reset SCS] > [Master Database Offline Download].
   The master database offline download confirmation dialog box appears.

TIP

- If the SCS security level is Level 1 or Level 2, a message prompting to set the security level to Level 0 is notified and the download ends with an error. Set the security level to Level 0, and start the master database offline download.
- If the I/O Lock window or Inter-SCS Communication Lock window is left open when you start master database offline download, an error message appears and the download processing ends.

3. Click [OK].
4. Set a new password for changing the SCS security level.

I4.5 NIU maintenance port setting tool

The NIU maintenance port setting tool is used in the following cases:

- To disable the NIU maintenance ports of all N-IO nodes on a per station basis in a batch
- To disable the NIU maintenance ports on a per node basis
- To enable the NIU maintenance ports on a per node basis

This section describes how to use the NIU maintenance port setting tool.

Rights to execute the NIU maintenance port setting tool

The NIU maintenance port setting tool can be executed by the logged-in Windows user who belongs to any of the following Windows groups: PSF_MAINTENANCE, PSF_MAINTENANCE_LCL, PSF_ENGINEER and PSF_ENGINEER_LCL.

To disable the NIU maintenance ports of all N-IO nodes on a per station basis in a batch

1. On the Hardware Configuration Tree View of the SCS State Management window, select the station for which the maintenance ports of NIU are to be disabled in a batch.
2. Select [Disable Maintenance port] in the [Operation] menu. Or, click the [Disable Maintenance port] button on the toolbar.
   The NIU Maintenance Port Setting Tool window appears.

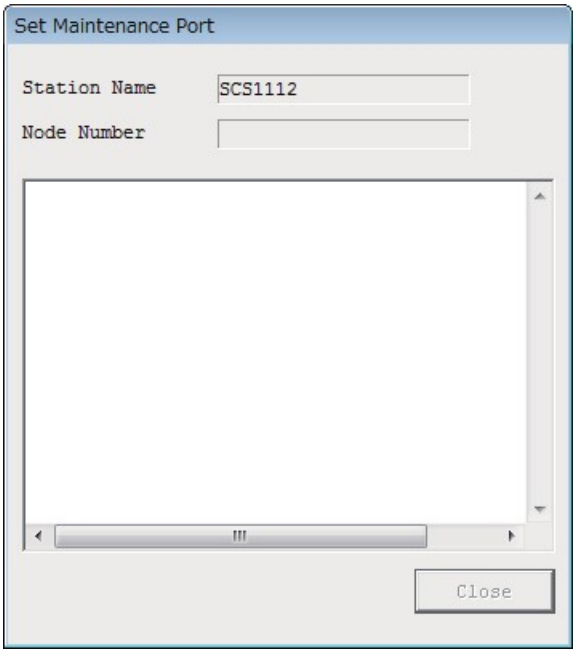


Figure I4.5-1 NIU Maintenance Port Setting Tool window

   The execution result is displayed in the message area once the processing is complete.

3. Click [Close].
   The NIU Maintenance Port Setting Tool window is closed.

To disable the NIU maintenance ports on a per node basis

1. On the Hardware Configuration Tree View of the SCS State Management window, select the N-IO node for which the maintenance port of NIU is to be disabled.

2. Select [Disable Maintenance port] in the [Operation] menu. Or, click the [Disable Maintenance port] button on the toolbar.
   The NIU Maintenance Port Setting Tool window appears.

   The execution result is displayed in the message area once the processing is complete.

3. Click [Close].
   The NIU Maintenance Port Setting Tool window is closed.

To enable the NIU maintenance ports on a per node basis

1. Check that the SCS security level is Level 1 or 0 by using the SCS security level operation function.
2. On the Hardware Configuration Tree View of the SCS State Management window, select the N-IO node for which the maintenance port of NIU is to be enabled.
3. Select [Enable Maintenance port] in the [Operation] menu. Or, click the [Enable Maintenance port] button on the toolbar.
   The NIU Maintenance Port Setting Tool window appears.

   The execution result is displayed in the message area once the processing is complete.

4. Click [Close].
   The NIU Maintenance Port Setting Tool window is closed.

IMPORTANT

Set the security level of the SCS to 1 or 0 to enable the maintenance port of NIU. You cannot enable the maintenance port of NIU when the security level is 2.

Display of execution results

The following execution results are displayed in the message area when the NIU maintenance port setting tool is executed.

Table I4.5-1 Display of execution results

Display	Description
Succeeded	Successfully completed the configuration process of the maintenance port.
Skipped	Skipped the configuration process of the maintenance port.
Failed	Failed in the configuration process of the maintenance port.

When a node is specified (example):

```
Disabling NIU Maintenance Port start 2015/12/11 18:02:00
Station:SCS0101 Node:1 … Succeeded.
Disabling NIU Maintenance Port end 2015/12/11 18:02:01
```

When all nodes are set at a time (example):

```
Disabling NIU Maintenance Port start 2015/12/11 18:03:00
Station:SCS0101 Node:1 … Succeeded.
Station:SCS0101 Node:2 … Skipped.
Station:SCS0101 Node:3 … Skipped.
Disabling NIU Maintenance Port end 2015/12/11 18:02:03
```

When disabling the port for all nodes, the result is displayed only for the nodes that are defined.

The following cases result in Skipped or Failed, and an error message is displayed.

- Specified port is already enabled/disabled
- NIU is in maintenance mode
- Node failure
- N-ESB bus failure

I4.6 IOM Download tool

The IOM Download tool enables you to configure input/output modules by downloading input/output configuration information from the master database of an SCS project to the modules. Use the IOM Download tool in the following cases.

- After replacing failed input/output modules with normal modules.
- When resetting AIO/DIO modules for recovery from errors in the field. This is only applicable with SCS system program release number R3.02 or later.

The correct operation procedure, when to use the IOM Download tool, and precautions are included in the topic of the input/output module maintenance. Use the IOM Download tool according to the instructions of reference documents in this section.

TIP

With SCS system program release number R2.03 or later, you can choose to enable automatic download of configuration information whenever stand by AIO/DIO module in a dual redundant configuration is replaced. This setting is available in the SCS Constants Builder. If the automatic download is executed, you do not have to use the IOM Download tool.

SEE ALSO

For more information about input module recovery procedure, refer to:

G2.2.1, “Actions taken at input module error occurrence and recovery procedure” on page G2-12

For more information about output module recovery procedure, refer to:

G2.2.3, “Actions taken at output module error occurrence and recovery procedure” on page G2-15

For more information about I/O module maintenance procedure, refer to:

“■ Maintenance of I/O modules” on page I1-12

For more information about how to replace the I/O module of the FIO node, refer to:

E4.7, “Replacing FIO I/O modules” in Hardware User's Guide (IM 32P06C10-01EN)

For more information about how to replace the I/O module of the N-IO node, refer to:

E5.3, “Replacing N-IO I/O modules” in Hardware User's Guide (IM 32P06C10-01EN)

■ Configuring Input/Output modules by using the IOM Download tool

The IOM Download tool must be used for modules where the hardware is working properly. Follow these steps to configure an input/output module:

TIP

The input/output configuration information stored in the master database of the SCS project is downloaded by IOM download. So the information previously downloaded to the input/output module is downloaded again even if the SCS project is being changed.

1. In the SCS State Management window, select an input/output module whose status is Fail .
2. On the tool bar, click [IOM Load].
   The IOM Load dialog box appears.
3. Click [OK].
   The input/output configuration information is downloaded to the selected input/output module. The downloaded information is stored in the non-volatile memory of the input/output module. After that, the SCS starts the input/output modules.
4. Check the results of the IOM Download tool execution in the diagnostic information messages.

IMPORTANT

- The channels of the output module are in the Output Disable status after the module starts. To output signals from the module, put the channels to be in the Output Enable status by performing the Output enable operation. After all channels go into the Output Enable status, SCS operating mode is changed from Waiting Mode to Running Mode.
- When the IOM Download tool is executed, the communication program is downloaded to the communication module, and the module restarts. The Output Enable Operation is unnecessary for the communication module because the communication begins automatically.

SEE ALSO For more information about how to view diagnostic information messages, refer to:

H5.1, “Diagnostic Information window” on page H5-2

For more information about Output enable operation, refer to:

C8., “Output enable operation” on page C8-1

Automatic execution of IOM download

After replacing I/O module, you need to perform IOM download in order to set configuration information. However, you can specify automatic execution of IOM download in following conditions.

When automatic execution of IOM download is specified, and if a standby side of a duplexed AIO/DIO module is replaced in the SCS that is running for a purpose such as maintenance, the configuration information is automatically downloaded from the module on the control side to the replaced module. This operation is possible only when specification is done with the SCS Constants Builder. If it is not specified, manual IOM download is required after replacing the module on the standby side. You need to perform manual IOM download when replacing both sides of redundant AIO/DIO modules or AIO/DIO modules of single configuration.

Automatic IOM download is not performed for communication modules.

SEE ALSO For more information about setting procedures using SCS Constants Builder, refer to:

C1.2.6, “SCS Constants Builder” on page C1-21

IOM download automatic execution conditions

If a redundant module on the standby side is replaced, IOM download is automatically executed if the following conditions are met.

- Automatic IOM download is enabled in the SCS Constants Builder.
- The redundant AIO/DIO module on the control side is operating normally.
- The replaced redundant module on the standby side failed due to configuration error (*1)

*1: Except the case where the model names on the control and standby sides are different or the case of hardware failure (the STATUS LED of the module is OFF).

Operations during automatic IOM download

The SCS operates as follows while automatic IOM download is being executed.

- If multiple AIO/DIO modules on the standby side are replaced, the processing of automatic IOM download is executed sequentially on a one-by-one basis.

- Diagnostic information messages (No. 0475 and 0476) are notified at the start and completion of automatic IOM download.
- If an error occurs during automatic execution of IOM download, the diagnostic information message indicating erroneous termination of automatic IOM download (No. 477) is notified and the IOM download processing is aborted.

IMPORTANT

Do not remove and put back the applicable AIO/DIO module while automatic IOM download is being executed. If it is removed and put back, a major failure may occur in the module (the STATUS LED of the module becomes OFF).
Automatic download is completed in approximately 30 seconds after inserting the module on the standby side, and the diagnostic information message indicating completion of IOM download (No. 0476) is output. If you need to remove and put back a module, check the diagnostic information message indicating completion of IOM download in the Diagnostic Information window of the SCS Maintenance Support Tool before doing so.

If a major failure occurs due to erroneous removal and reinsertion, perform IOM download manually to the applicable AIO/DIO module, and then remove and reinsert the module after the completion.

- Automatic IOM download is not executed on AIO/DIO modules to which online change download of input/output parameters or manual IOM download are being executed. However, automatic IOM download to a different module is executed in parallel.
- If it is attempted to execute online change download of input/output parameters or manual IOM download on the applicable AIO/DIO modules for which automatic IOM download is being executed, an error occurs in the manual download.

I4.7 IOM Control Right Switching Tool

The IOM Control Right Switching Tool is used for switching between the control side and the standby side of the pair of AIO/DIO modules placed in redundant configuration. However, this tool can not be used for the redundantly configured communication modules.

This section explains the operation procedures.

Overview of the IOM Control Right Switching Tool

The IOM Control Right Switching Tool is used for switching between the control side and the standby side of the pair of AIO/DIO modules for which redundant configuration is specified. It is possible to perform a switching operation for one AIO/DIO module pair or one node in one operation.

This tool can be used when the SCS security level is 1 or 0.

TIP

The IOM Control Right Switching Tool is not used to display the status of AIO/DIO modules or to perform operations related to the status of AIO/DIO modules.

Precautions at starting the IOM Control Right Switching Tool

The IOM Control Right Switching Tool can be used even if the SCS project is opened in SCS Manager.

Note, however, that if a download operation and an AIO/DIO module control right switching operation are performed at the same time, an error occurs in one of the operations. Moreover, the control right of AIO/DIO modules cannot be switched during checking in/out in Version Control or executing the Master Database Restoring Function.

How to start the IOM Control Right Switching Tool

Double-click the following command in Windows Explorer to start the tool. (ProSafe-RS installation top folder) Specify \ProSafe-RS\YOKOGAWA\scs\tool\RHEToolIOSwitch.exe or, from the [Start] menu of Windows, select [Run...] and specify "RHEToolIOSwitch.exe." The main window of the IOM control right switching tool appears.

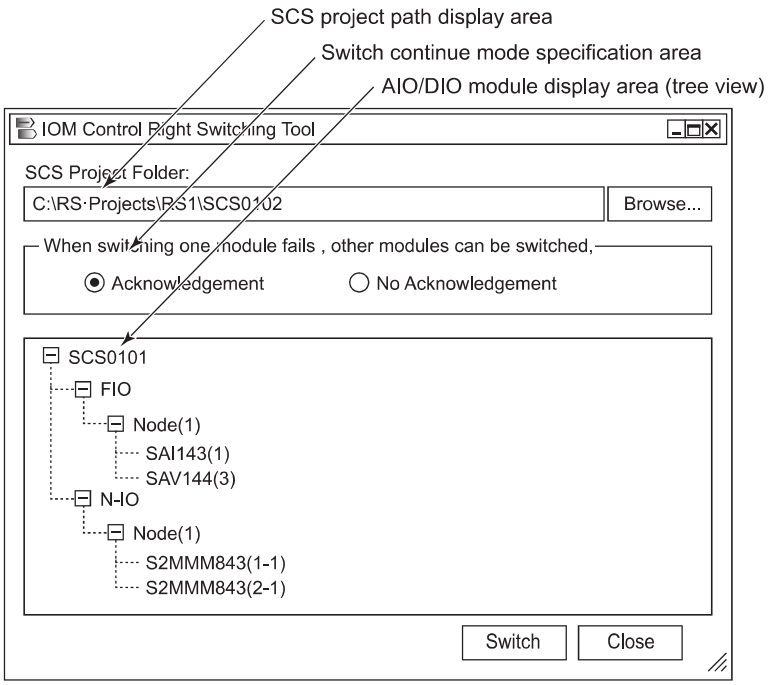


Figure I4.7-1 Main window of the IOM Control Right Switching Tool

Procedure to switch the control right of AIO/DIO modules

1. Specify the top folder of the SCS project in the SCS project path display area. The specified SCS project should be the one downloaded to the SCS. You can also select a folder from the folder selection dialog box that is displayed by clicking [Browse].
2. In the switch continue mode specification area, select [Acknowledgement] or [No Acknowledgement].
   You can select whether to display a confirmation dialog that appears during switching multiple AIO/DIO modules if switching fails for a certain AIO/DIO module, and the next AIO/DIO module is to be switched in continuation.
3. The redundant AIO/DIO modules in the SCS project, which is specified in the SCS project path display area, are displayed in a tree format in the AIO/DIO module display area.
   You can select either the AIO/DIO module or node for which the control rights are to be switched. Only one AIO/DIO module or one node can be selected at a time. You cannot select a station name, FIO or N-IO.
4. Click the [Switch] button. A confirmation dialog box appears.

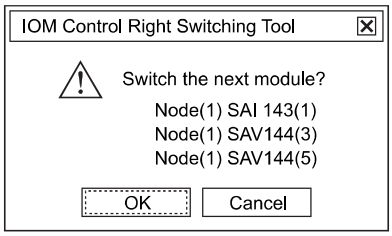


Figure I4.7-2 Confirmation dialog box

5. Click [OK]. The control right switching process of the AIO/DIO module starts, and the Message Display dialog box appears.

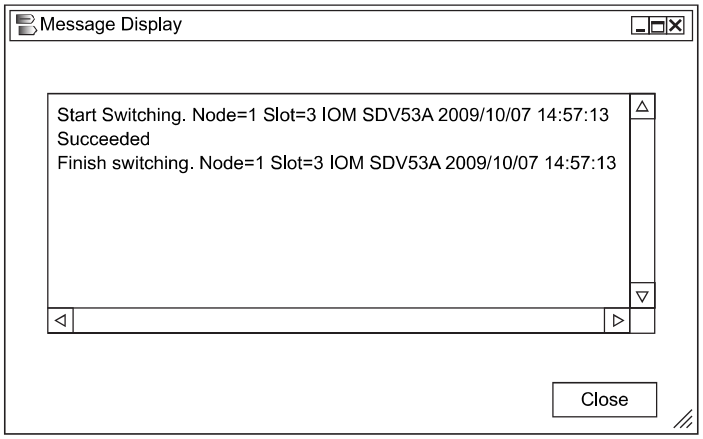


Figure I4.7-3 Message Display dialog box

   The Message Display dialog box shows the AIO/DIO module targeted for switching and the processing results, etc.

TIP

Select [Select All] from the pop-up menu displayed by right-clicking the mouse in order to select data displayed in the Message Display dialog box. Select [Copy] to copy the data.

6. When the switching operation is completed, click the [Close] button in the Message Display dialog box.
7. Click [Close] in the main window to exit the IOM Control Right Switching Tool.

I5. Procedures and precautions for adding a station or domain

This section describes the procedures and precautions that must be followed when you add a station or a domain to a Vnet/IP network in a star topology.

TIP

For information about the procedures and precautions when you add a station or a domain to a Vnet/IP network in a ring topology, contact YOKOGAWA.

SEE ALSO

For more information about the procedures and precautions for adding stations or adding domains in a CI Server integration configuration, refer to:

C5.2, “Procedures and precautions for adding a station or domain” in Integration with CI Server (IM 32P04D20-01EN)

Procedures and precautions for adding a Vnet/IP station

When adding a station to Vnet/IP network, follow the following procedure:

IMPORTANT

- If you add a station to a stand-alone ProSafe-RS system, special operation may be needed before adding it. For detailed procedure, refer to the link included at the end of this section.
- Before you add a station, make sure that there are no duplicate station addresses.
- Turn off the power of the additional station before you connect the cables.

SEE ALSO

For more information about procedure required before adding Vnet/IP station for a stand-alone ProSafe-RS system, refer to:

I6., “Procedures and precautions for adding or replacing Vnet/IP devices” on page I6-1

Case 1: When using existing Layer 2 switches (ports are available on existing Layer 2 switches)

1. In the Network Status Display dialog box on HIS, check that both buses are normal. (*1)
2. Make sure that the additional station is not powered.
3. Connect the Vnet/IP connector for BUS1 of the additional station to the Layer 2 switch for BUS1 with a cable. If the port on the Layer 2 switch is disabled, enable the port.
4. In the Network Status Display dialog box on HIS, check that both buses are normal.(*1)
5. Connect the Vnet/IP connector for BUS2 of the additional station to the Layer 2 switch for BUS2 with a cable. If the port on the Layer 2 switch is disabled, enable the port.
6. In the Network Status Display dialog box on HIS, check that both buses are normal.(*1)
7. Turn on the power of the additional station.
8. In the Network Status Display dialog box on HIS, check that both buses are normal.(*1)

*1: For a stand-alone ProSafe-RS system, use an SCS status display window (either SCS Status Overview or SCS State Management) of SCS Maintenance Support Tool on an SENG to check the bus status. When you call up the SCS status display window, select the project of a running SCS and then call up the window.

TIP Alternatively, you can add a station to Layer 3 switches directly instead of Layer 2 switches.

Case 2: When you need to add Layer 2 switches (no ports are available on existing Layer 2 switches)

Firstly, carry out steps 1 to 11 as shown below to add Layer 2 switches for BUS1 and BUS2. Next, carry out the procedure for "Case 1" above to add a station.

1. In the Network Status Display dialog box on HIS, check that both buses are normal.(*1)
2. Disconnect the cable between any one of the existing stations and a Layer 2 switch for BUS1.
3. Connect the additional Layer 2 switch for BUS1 to the existing Layer 2 switch for BUS1 with a cable.
4. Turn on the power of the Layer 2 switch that you have added.
5. Connect the existing station that you have disconnected at step 2 to the newly added Layer 2 switch for BUS1 with a cable.
6. In the Network Status Display dialog box on HIS, check that both buses are normal.(*1)
7. Disconnect the cable between any one of the existing stations and a Layer 2 switch for BUS2.
8. Connect the additional Layer 2 switch for BUS2 and the existing Layer 2 switch for BUS2 with a cable.
9. Turn on the power of the Layer 2 switch that you have added.
10. Connect the existing station that you have disconnected at step 7 to the newly added Layer 2 switch for BUS2 with a cable.
11. In the Network Status Display dialog box on HIS, check that both buses are normal.(*1)
12. Add a station according to the procedure for "Case 1".

*1: For a stand-alone ProSafe-RS system, use an SCS status display window (either SCS Status Overview or SCS State Management) of SCS Maintenance Support Tool on an SENG to check the bus status. When you call up the SCS status display window, select the project of a running SCS and then call up the window.

Procedures and precautions for adding a Vnet/IP domain

Follow these steps when you want to add a domain to a Vnet/IP network.

IMPORTANT

Make sure that there are no duplicate station addresses (domain number + station number) in the system.

Case 1: When using existing Layer 3 switches (ports are available on existing Layer 3 switches)

Firstly, carry out steps 1 to 5 as shown below to configure Layer 3 switches for BUS1 and BUS2. Next, add stations by following the procedures in "Procedures and precautions for adding a Vnet/IP station."

1. In the Network Status Display dialog box on HIS, check that both buses are normal. (*1)
2. Make the necessary settings on the existing Layer 3 switch for BUS1. If the port on the Layer 3 switch is disabled, enable the port.
3. In the Network Status Display dialog box on HIS, check that both buses are normal. (*1)

4. Make the necessary settings on the existing Layer 3 switch for BUS2. If the port on the Layer 3 switch is disabled, enable the port.
5. In the Network Status Display dialog box on HIS, check that both buses are normal. (*1)
6. Add stations for the new domain by following the procedures in "Procedures and precautions for adding a Vnet/IP station."

*1: For a stand-alone ProSafe-RS system, use an SCS status display window (either SCS Status Overview or SCS State Management) of SCS Maintenance Support Tool on an SENG to check the bus status. When you call up the SCS status display window, select the project of a running SCS and then call up the window.

Case 2: When you need to add Layer 3 switches (no ports are available on existing Layer 3 switches)

Firstly, carry out steps 1 to 7 as shown below to add Layer 3 switches for BUS1 and BUS2. Next, add stations by following the procedures in "Procedures and precautions for adding a Vnet/IP station."

1. In the Network Status Display dialog box on HIS, check that both buses are normal. (*1)
2. Make the necessary settings on the Layer 3 switch for BUS1 that you are going to add.
3. Connect the additional Layer 3 switch for BUS1 to an existing Layer 2 or Layer 3 switch for BUS1 with a cable.
4. In the Network Status Display dialog box on HIS, check that both buses are normal. (*1)
5. Make the necessary settings on the Layer 3 switch for BUS2 that you are going to add.
6. Connect the additional Layer 3 switch for BUS2 to an existing Layer 2 or Layer 3 switch for BUS2 with a cable.
7. In the Network Status Display dialog box on HIS, check that both buses are normal. (*1)
8. Add stations for the new domain by following the procedures in "Procedures and precautions for adding a Vnet/IP station."

*1: For a stand-alone ProSafe-RS system, use an SCS status display window (either SCS Status Overview or SCS State Management) of SCS Maintenance Support Tool on an SENG to check the bus status. When you call up the SCS status display window, select the project of a running SCS and then call up the window.

I6. Procedures and precautions for adding or replacing Vnet/IP devices

This section describes the procedures and precautions that must be followed when you add or replace a Vnet/IP device in a Vnet/IP domain of CENTUM integration system or a stand-alone ProSafe-RS system.

The Vnet/IP device is a generic name of the following devices:

- Processor module of SCS for Vnet/IP and FCS for Vnet/IP
- Vnet/IP interface card (Model: VI702)

TIP

The replacement of a Vnet/IP device includes not only replacement of a Vnet/IP station, but also replacement of a VI702 card and a processor module.

SEE ALSO

For more information about procedure and precaution after adding or replacing Vnet/IP devices in a CI server integration system, refer to:

C5.3, “Procedures and precautions for adding or replacing Vnet/IP devices” in Integration with CI Server (IM 32P04D20-01EN)

Precautions for adding or replacing Vnet/IP devices

The following problems may occur if the necessary procedures are not performed when you add the Vnet/IP device to a Vnet/IP domain or when you replace the Vnet/IP device in a Vnet/IP domain.

- Message issued by SCS cannot be received.
- Inter-SCS safety communication is disabled.

If these problems occur, perform the following operation.

Procedures after adding or replacing Vnet/IP devices of CENTUM integration system

For CENTUM integration system, if you add or replace the Vnet/IP device while all the Vnet/IP stations in the Vnet/IP domain that you want to add or replace the Vnet/IP device are turned off, follow the steps described below after you add or replace the Vnet/IP device.

TIP

If there is a powered-on Vnet/IP station on the Vnet/IP domain, the procedure is not necessary.

1. Start the computer with system builders of CENTUM VP first. If the domain does not contain a computer with system builders, start the computer with system builders in other domain first.
2. Start a station other than the computer with system builders in the domain.
3. Start System View, select a station in the domain, right-click, and select [Domain Properties] on the shortcut menu.
   Domain Properties appears.

TIP

You can select a station other than the one that you started in the step 2.

4. Click [OK].
   A dialog box appears, asking you to download Domain Properties.

5. Click [OK].
   The information of Domain Properties is reflected to the stations that have been started in the domain.
6. Start the stations that have been turned off in the domain.
   The information of Domain Properties is reflected to them.

TIP If you did not start the computer with system builders first, download Domain Properties immediately after you start the computer with system builders.

Procedures before adding or replacing Vnet/IP devices of stand-alone ProSafe-RS system

For stand-alone ProSafe-RS system that is not connected to CENTUM VP or CI Server, in advance of addition or replacement, clear the setting information of the Vnet/IP device that will be joined to the Vnet/IP domain by addition or replacement.

Procedures before adding or replacing VI702

Before adding or replacing SENG, or replacing VI702 of SENG, make sure to clear the setting information of VI702.

SEE ALSO For more information about procedure of clearing the setting information of VI702, refer to:

Appendix 2., “Procedure for Erasing VI702 Internal Settings” in Installation Guide (IM 32P01C50-01EN)

Procedures before adding or replacing processor module

If the SCS or processor module to be added or replaced has ever been used by another system, clear the processor module setting information before adding or replacing SCS or replacing the processor module. If it has never been used by another system, there is no need to clear the setting information.

SEE ALSO For more information about procedure of replacing a processor module that includes the procedure of clearing the setting information, refer to:

E4.2, “Replacing processor module” in Hardware User's Guide (IM 32P06C10-01EN)

Appendix 1. Settings for node, module, and channel

This section explains the settings for node, module, and channel. These settings can be done in the Safety I/O Editor or in IOM Definition Editor; however, this section explains how to do it in each tab of I/O Parameter Builder.

Appendix 1.1 Setting items for nodes

The following are the node settings of the Node tab in I/O Parameter Builder for input/output.

- Node number:
- Component Number
- Node Interface Unit
- Extends node bus
- Extends to
- N-IO Node Connection
- Enable External Alarm Input
- Normal Value
- Comment

Each node setting item is explained in detail as follows.

Node Number

This is the node number for which the module is mounted.

Component Number

This is a comment related to node layout information. Any character string of up to 8 single-byte characters or 4 double-byte characters can be entered.
This setting item is not downloaded to an SCS.

This item can be changed online.

Node Interface Unit: SCSP3, N-IO node

This is the model name of the bus module for node interface unit.

Extends Node Bus: SCSP3, SCSL2, and SCSP2

You can specify whether or not to extend nodes by the optical ESB bus repeater. For the remote node installed via the optical ESB bus repeater, you must select [Yes] and specify the distance in [Extends To]. If you do not make this setting, the data from the nodes and SOE data will not be updated correctly. If [Yes] is set for this item on CPU nodes, a build error will occur.

- Yes: Node extension by an optical ESB bus repeater is applied
- No: Node extension by an optical ESB bus repeater is not applied (default)

This setting item can be changed online.

Extends To: SCSP3, SCSL2, and SCSP2

You can specify the distance from a CPU node to a safety node unit and to an N-IO node. It is only valid if [Yes] is selected in the specification of node extension distance [Extends Node Bus].

- Range: 5 to 50 km (default: 5 km)
- Setting unit: 5 km

This item can be changed online.

Extends Node Bus : SCSP1

You can specify whether or not to extend nodes by the optical ESB bus repeater. To extend a node, select [Yes] and specify the distance in [Extends To]. A build error will occur if you select [Yes] for this item when [Optical ESB Bus Repeater] on the SCS Constants Builder is set to [No]. A build error will also occur if [Yes] is set for this item on CPU nodes.

- Yes: Node extension by an optical ESB bus repeater is applied
- No: Node extension by an optical ESB bus repeater is not applied (default)

This setting item can be changed online.

TIP

In the case of nodes equipped with ALR111, ALR121, or ALE111 for Modbus slaves, if 10 km or longer is specified in [Maximum Extension Distance] on the SCS Constants Builder, select [Yes] and specify the node extension distance in [Extends To].

Extends To: SCSP1

You can specify the distance from a CPU node to a safety node unit. It is only valid if [Yes] is selected in the specification of node extension distance [Extends Node Bus].
A build error will occur if the node extension distance is longer than [Maximum Extension Distance] defined on the SCS Constants Builder.

If default (0) is specified, it is regarded as if the node is at the position specified by [Maximum Extension Distance] defined on the SCS Constants Builder.

- Range: 0 to 50 km (default: 0)
- Setting unit: 5 km

This item can be changed online.

IMPORTANT

Be sure to specify the extension distance according to the actual node extension distance. If no specification is made for SCSP1, load fluctuation of CPU becomes large if input/output modules and/or bus fail.

N-IO Node Connection: SCSP3, FIO node

You can specify whether to connect the N-IO node to the path from the CPU node to FIO node.

- Yes: Connects the N-IO node to the path from the CPU node to FIO node.
- No: Does not connect the N-IO node to the path from the CPU node to FIO node (default).

This setting can be changed online.

Enable External Alarm Input: SCSP3, N-IO node

You can specify whether or not to use alarm input from an external device.

- Yes: Alarm input from an external device is used.
- No: Alarm input from an external device is not used (default).

This setting can be changed online.

Normal Value: SCSP3, N-IO node

You can specify the normal value to 0 or 1 for the alarm input if [Yes] is specified for [Enable External Alarm Input].

- 0: 0 is the normal value.
- 1: 1 is the normal value (default).

This setting can be changed online.

Comment

This is a comment related to the node. Any character string of up to 24 single-byte characters or 12 double-byte characters can be entered.
This setting item is downloaded to an SCS.

This setting item can be changed via online change download.

Appendix 1.2 Settings for modules

The following are the settings in the module tab of I/O Parameter Builder.

Node Number

This item displays the node number in which the I/O module is mounted.

Unit Number: N-IO I/O module

This item displays the unit number in which the I/O module is mounted.

Slot Number

This item displays the slot number in which the I/O module is mounted.

Device

The model name of the I/O module is displayed.

Base Plate: N-IO I/O module

You can select the base plate model for which the I/O module is mounted.

Table Appendix 1.2-1 Available base plate models

I/O module model	Base plate model	Description
S2MMM843, S2MDV843	S2BN1D	Standard base plate (default)
	S2BN_D	Base plate for barrier

TIP

If the base plate model is changed, all the channel items set for the module are initialized.

Dual-Redundant

This item displays whether the input/output module is placed in single configuration or redundant configuration. Input/output modules are placed in redundant configuration using an odd-numbered slot and the adjacent even-numbered slot (the odd number + 1).

Device Index

This is the device index assigned to the I/O module.

Comment

This is a comment related to the input/output module. Any character string of up to 24 single-byte characters or 12 double-byte characters can be entered.
This setting item is not downloaded to an SCS, so changing the definition does not affect input/output processing.

This item can be changed online.

Device Reset Function (per module): SAI143/L1AI143

This item specifies whether or not to use the device reset function.

- Enable: Uses the device reset function.

- Disable: Does not use the device reset function. (Default)

This setting is displayed when using an SCS project newly created with a version of SENG that is R4.03.00 or later.

SEE ALSO For more information about engineering for resetting the Smoke and Heat Detector, refer to:

A3.4.4, “Engineering regarding the device reset function and alarm suppression during device reset” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Command Line: analog output module

TIP Specify the command line using up to 256 single-byte characters. If the command line is not set, the default value will be used for each applicable item. The format is as follows.

Item name = Data value, Item name = Data value, ...

SOOP (Output open detection level setting)

This item specifies an output open (OOP) detection level. An open circuit error is recognized when the readback value of an output falls below the set value. The default is 0.00085 A.

Format

- SOOP=0.001

Parameter

- Output open detection level
  You need to specify an output open detection level in amperes (A).

  SOOP < Output value at fault (fail-safe value)

  If tight-shut output is specified : SOOP < Tight-shut output value

  If tight-shut output is not specified : SOOP < Power-on output value (0.00125 A)

- This item can be changed via online change download. Note, however, that IOM download is also performed at the same time.

Software Filter: digital input module, N-IO I/O module (DI channel only)

The software filter is applied for reducing the influence of noises. An integer between 0 and 10 can be selected as the filter setting value. The default setting is 1.

With this filter, the discrete input chattering signals can be sifted out so as to prevent from error actions.

The filter setting value multiplied by 10 ms (sampling period) is the filter time. The chattering signals occurred within this filter time will be eliminated.

As an example, if the filter setting value is 2, the chattering signals shorter than 20 ms (2x10 ms) will be eliminated.

- If the filter setting value is 0, the noise signals will not be filtered thus PV varies with the noise signals. In general, the filter setting value should not be set to 0.

This item can be changed via online change download. Note, however, that IOM download is also performed at the same time.

Automatically Delete Noisy Events (Automatically delete SOE event): digital input module, N-IO I/O module (DI channel only)

You can specify whether or not to delete events automatically if many events that are targets of SOER occur.
If a channel repeatedly generates too many events, the events from other channels may be lost. This function can be used to restrict events per channel and the above problem can be avoided. If the number of events that have occurred during the time specified in [SOE Deletion Schedule] exceeds the number of events specified in [Number of SOE Events], all subsequent events are discarded. For example, if [SOE Deletion Schedule] is set to 1.0 second and [Number of SOE Events] is set to 3, and if three or more events have occurred within 1 second, then the fourth and subsequent events occurring within 1 second are automatically discarded. However, if the last event is different from the current status of the DI, a pseudo event is generated to indicate the DI status.

- Yes (Delete):
  Automatically delete events if many events occur.
- No (Do not delete):
  Do not delete events even if many events occur (default).

This item can be changed via online change download. Note, however, that IOM download is also performed at the same time.

SOE Deletion Schedule (SOE event period): digital input module, N-IO I/O module (DI channel only)

You can specify the time period setting for [Automatically Delete Noisy Events] in units of seconds. This setting is enabled if [Yes (Delete)] is selected for [Automatically Delete Noisy Events].
Select either 0.5, 1.0, 1.5, 2.0, 2.5, 3.0 or 3.5 seconds. The default value is 1.0 second.

This item can be changed via online change download. Note, however, that IOM download is also performed at the same time.

Number of SOE Events: digital input module, N-IO I/O module (DI channel only)

You can specify the number of events for [Automatically Delete Noisy Events]. This setting is enabled if [Yes (Delete)] is selected for [Automatically Delete Noisy Events].
Select either 3 or 5. The default value is 3 events.

This item can be changed via online change download. Note, however, that IOM download is also performed at the same time.

Appendix 1.3 Settings for channel items

The following are the settings in the channel tab of I/O Parameter Builder.

Appendix 1.3.1 Common display items for channels

The following items are displayed commonly for all AIO/DIO modules with channel parameters in I/O Parameter Builder.

Channel Number

This is the channel number displayed in I/O Wiring View of SCS Manager. It is sequential number starting from 1.

Wiring Position

This is the channel name that is displayed in I/O Wiring View of SCS Manager. It is determined by device index and channel identification number. The channel identification number used for wiring position is sequential number starting from 0. The wiring position of the input modules is prefixed with %IU while the wiring position of the output modules is prefixed with %QU.

Example:

In the case of a 16-channel input module: %IU1.0, %IU1.1, ... %IU1.14, %IU1.15

In the case of a 8-channel output module: %QU3.0, %QU3.1, ... %QU3.6, %QU3.7

I/O Variable Name

This is the name of I/O variables assigned to the channel.

Direction: AIO/DIO module of FIO

This item indicates whether a signal is an input or output signal.

Comment

This is a comment for an I/O variable specified in Dictionary View (*1)of SCS Manager.

*1: The comment for the I/O variable specified in Dictionary View of SCS Manager is displayed as the comment for the wired channel. Up to 64 characters can be specified for the variable comment, but only 32 characters are retained in SCS database; therefore, make sure not to specify more than 32 characters. Channel comments for unused channels (unconnected channels) are not displayed.
Comments for DI/DO variables are the variables used as identifiers of SOE.

TIP

If comments for DI/DO variables are changed in Dictionary View of SCS Manager, discrepancies occur due to the input/output definition changes, and it becomes necessary to perform online change download to the SCS. Since this changes only the definitions in the databases of the SCS (no changes are made to the parameters of the DI/DO modules themselves), the inputs and outputs are not influenced by the online change download.

Signal Type: AIO/DIO module of N-IO

This item specifies type and direction of the I/O signal. Selection of the signal type can be different depending on the classified signal category that is specified.

Table Appendix 1.3.1-1 Signal type

Signal category	Signal type	Description
AI	Current Input	Select this item if HART communication function is not used (default).
	Current Input (HART Communication)	Select this item if HART communication function is used.
AO	Current Output	Select this item if HART communication function is not used (default).
	Current Output (HART Communication)	Select this item if HART communication function is used.
DI	Status Input	Only one DI signal type (default)
DO	Status Output	Use one channel (default).
	1.3A Status Output	Use two consecutive channels. When the settings for one channel (for example channel no. 3) are configured, the same contents are set automatically for the succeeding channel (for example channel no. 4). This item cannot be selected for the module mounted in the base plate for barrier.
	2.0A Status Output	Use three consecutive channels. When the settings for one channel (for example channel no. 3) are configured, the same contents are set automatically for the two succeeding channels (for example channels no. 4, 5). This item cannot be selected for the module mounted in the base plate for barrier.

IMPORTANT

When using S2MMM843 or S2MDV843 in an explosion protection system, refer to the following document without fail because the approved values of the explosion protection parameters are different depending on the signal type.

ProSafe-RS/ProSafe-RS Lite Explosion Protection (TI 32S01J30-01E)

P&ID Tag Name

This is a comment that the user can specify in order to make it easy to identify information drawn on a P&ID drawing with the channel.

For FIO, the comment should be written within 16 single-byte characters or 8 double-byte characters. For N-IO, the comment should be written within 32 single-byte characters or 16 double-byte characters. This setting item can be omitted.

Appendix 1.3.2 Settings for the AI channel

The following are the settings for the AI channel in I/O Parameter Builder.

Table Appendix 1.3.2-1 Settings for the AI channel

Setting items	Online change download (*1)	IOM download (*2)	Remarks
Channel Number (Specify Channel Number)	-	-	-
Wiring Position (Specify Wiring Position)	-	-	-
I/O Variable Name (Specify I/O Variable Name)	-	-	-
Direction (Specify Direction)	-	-	-
Comment (Specify Comment)	-	-	-
Time to Chattering Recovery Notice (s) (Specify Time to Chattering Recovery Notice)	Yes	No	-
Connection Method (Specify Connection Method)	Yes	Yes	-
Device OFF-ON Variable Name (Specify Device OFF-ON Variable Name)	Yes	No	-
Reset Group ID (Specify Reset Group ID)	Yes	No	-
Input Processing at Fault (Specify Input Processing at Fault)	Yes	No	-
Input Value at Fault (Specify Input Value at Fault)	Yes	No	-
Input Processing at Transmitter Fault (Specify Input Processing at Transmitter Fault)	Yes	No	-
Signal Conversion (Specify Signal Conversion)	Yes	No	For SAT145/ L1AT145 and SAR145/L1AR145, the IOM download is run.
Low Limit (Specify Low Limit)	Yes	Yes	-
High Limit (Specify High Limit)	Yes	Yes	-
Unit (Specify Unit)	No	No	-
Detect IOP (High) (Specify Detect IOP (High))	Yes	No	-
Detect IOP (Low) (Specify Detect IOP (Low))	Yes	No	-
Threshold of IOP (High) % (Specify Threshold of IOP (High) %)	Yes	No	-
Threshold of IOP (Low) % (Specify Threshold of IOP (Low) %)	Yes	No	-

Continues on the next page

Table Appendix 1.3.2-1 Settings for the AI channel (Table continued)

Setting items	Online change download (*1)	IOM download (*2)	Remarks
Detect Transmitter Fault (High) (Specify Detect Transmitter Fault (High))	Yes	No	-
Detect Transmitter Fault (Low) (Specify Detect Transmitter Fault (Low))	Yes	No	-
Threshold of Transmitter Fault (High) % (Specify Threshold of Transmitter Fault (High) %)	Yes	No	-
Threshold of Transmitter Fault (Low) % (Specify Threshold of Transmitter Fault (Low) %)	Yes	No	-
Field Power Diagnosis (Specify Field Power Diagnosis)	Yes	Yes	-
Reference Junction Compensation (Specify Reference Junction Compensation)	Yes	Yes	-
Burnout (Specify Burnout)	Yes	Yes	-
P&ID Tag Name (Specify P&ID Tag Name)	Yes	No	-
Command Line (Specify Command Line)	Yes	No	-

*1: Indicates whether the setting can be changed by online change downloading.
Yes: The setting can be changed by online change downloading.
No: Online change downloading is not required.
- : Not a target

*2: Indicates whether the IOM downloading is performed with the online change downloading.
Yes: The IOM downloading is performed together with the online change downloading.
No: The IOM downloading is not performed together with the online change downloading.
- : Not a target

Each of setting items that are not explained as common items is explained as follows.

Time to Chattering Recovery Notice (s) (Time to Chattering Recovery Notice)

This item is used to suppress the chattering alarm.

Set the time by which to delay display of the system alarm for recovery of a channel error of an input module. When an error is recovered during the alarm suppression period, SCS monitors whether the normal status persists for the amount of time set for this item. Alarm suppression is continued if an error occurs during the set time, while an error recovery system alarm is displayed if an error does not occur.

The chattering alarm suppression function is disabled when this time is set to 0.

Setting range: 0 to 120 seconds

Default: 0

IMPORTANT

This item can be used with SCS projects created using version R4.03.00 or later with SENG on which a CENTUM integration configuration license has been reflected.

Connection Method: AIO/DIO module of N-IO

- For the AIO/DIO module that is mounted in the standard base plate

You can set the connection method between field device and AIO/DIO module. The default is 2-Wire.

- For the AIO/DIO module that is mounted in the standard base plate for barrier
  You can set the connection method between barrier and AIO/DIO module. The default is 4-Wire.

Device OFF-ON Variable Name: SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

You can specify a BOOL-type variable to switch OFF/ON of the power supply of the Smoke and Heat Detector. The fault detection status is reset by switching the device off and on. With S2MMM843, you can only set the variable when the connection method is 2-Wire.

When using SAI143 or SAV144, this item is displayed when using an SCS project newly created with a version of SENG that is R4.03.00 or later.

SEE ALSO For more information about engineering for resetting the Smoke and Heat Detector, refer to:

A3.4.4, “Engineering regarding the device reset function and alarm suppression during device reset” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Reset Group ID: SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

An ID used, when multiple Smoke and Heat Detectors are to be reset, to interpret the channels of the Smoke and Heat Detectors being reset at the same time as being in the reset status. SCS manages whether the channels are in the reset status in units of each reset group ID. With S2MMM843, you can only set this ID when the connection method is 2-Wire.

Set the same reset group ID for channels to be interpreted as being in the reset status at the same time. Even in cases when there are no Smoke and Heat Detectors to be reset at the same time, set a reset group ID that is not in use with other channels. However, set this value to 0 if you will not be using the alarm suppression function during device reset nor the function block HSDTR.

This setting is displayed when using an SCS project newly created with a version of SENG that is R4.03.00 or later.

- Setting range: 0 to 1000 (default: 0)

SEE ALSO For more information about engineering for resetting the Smoke and Heat Detector, refer to:

A3.4.4, “Engineering regarding the device reset function and alarm suppression during device reset” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Input Processing at Fault

This item specifies an input processing to be used when an input fault is detected or when [Input Processing at Fault] is selected in [Input Processing at Transmitter Fault].
You can specify [Hold] or [Fixed Value].

The input faults that can be detected include the following: Errors on both sides of the path from the CPU to an analog input module, errors in analog input modules, channel errors, IOP and field wiring errors (transmitter errors are not included).

- Hold:
  The value before the fault was detected is retained.
- Fixed Value (specified input value):
  The input value specified in [Input Value at Fault] is set (default).

Input value at fault (%)

This is the value set as an input value instead of process value if [Fixed Value] is selected in [Input Processing at Fault] (the value is used as an input value at error occurrence).

For SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

You can specify the input value at error occurrence (%) in the range from -25.0 to 125.0. The default value is 0.0 %.

Even if the [Signal Conversion] is set to [SQRT], this setting value is used as the input value at error occurs. (The value set here will not be square-rooted when used as the input value.)

For SAT145/L1AT145 and SAR145/L1AR145

You can specify the input value at error occurrence (%) in the range from -1000.0 to 1000.0. The default is 100.0%.

Input Processing at Transmitter Fault: SAI143/L1AI143, SAV144/ L1AV144, and S2MMM843

This is the value set as the input value if a transmitter error is detected (a value used as an input value at error). This item is only enabled for current inputs.

- Input Processing at Fault:
  Follow the setting of [Input Processing at Fault] if a transmitter error occurs (default).
- Raw Data:
  The raw data from the input module is set as the input value.

Signal Conversion

You can specify the conversion method of the input signal.

For SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

- LINEAR (No Conversion):
  The physical range specified by the "Low Limit" and "High Limit" (mA or V) is converted to 0 to 100 (%) data (default).
- SQRT:
  After LINEAR conversion, input range checks are performed (against the IOP high limit/low limit and transmitter fault high limit/low limit). Then, the square root is calculated and the result is converted to a data value of 0 to 100 (%).

  The square-root conversion is illustrated as follows:

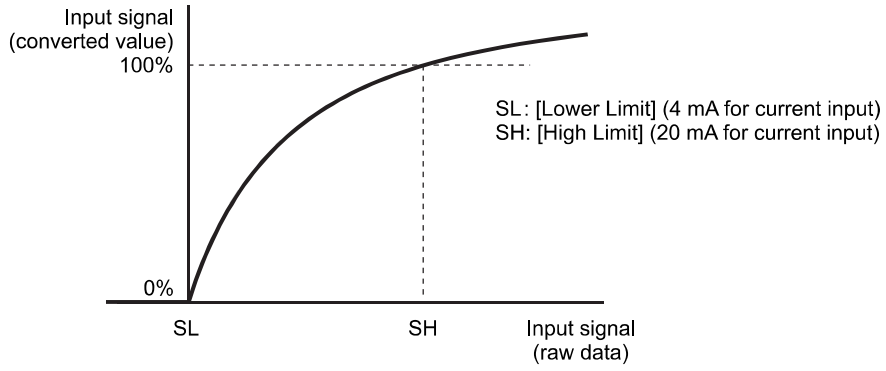


Figure Appendix 1.3.2-1 SQRT

For SAT145/L1AT145 and SAR145/L1AR145

Table Appendix 1.3.2-2 Input signal conversion for the thermocouple/mV input module (SAT145/ L1AT145)

Selection	Explanation of signal conversion
Type K	Temperature conversion Type K (default)
Type E	Temperature conversion Type E
Type T	Temperature conversion Type T
Type J	Temperature conversion Type J
Type R	Temperature conversion Type R
Type S	Temperature conversion Type S
Type B	Temperature conversion Type B
Type N	Temperature conversion Type N
mV Input -20 to 80 mV (%)	No temperature conversion. However, the physical range (mV) set in "High Limit" and "Low Limit" is converted to 0 to 100% data.
mV Input -100 to 150 mV (%)	
mV Input -5 to 25 mV (%)	
TC Input -20 to 80 mV (V)	No temperature conversion. Voltage value entries are directly applied to input valuables.
TC Input -100 to 150 mV (V)	
TC Input -5 to 25 mV (V)	

Table Appendix 1.3.2-3 Input signal conversion for the resistance temperature detector input module (SAR145/L1AR145)

Selection	Explanation of signal conversion
PT100	Temperature conversion Type PT100 (default)
JPT100	Temperature conversion Type JPT100
PT50	Temperature conversion Type PT50
PT200	Temperature conversion Type PT200
PT500	Temperature conversion Type PT500
PT1000	Temperature conversion Type PT1000
Ni100 (DIN)	Temperature conversion Type Ni100 (DIN)
Ni120 (MINCO)	Temperature conversion Type Ni120 (MINCO)
RTD Input 0 to 800 ohm (%)	No temperature conversion. However, the physical range (ohm) set in "High Limit" and "Low Limit" is converted to 0 to 100% data.
RTD Input 0 to 4000 ohm (%)	
RTD Input 0 to 800 ohm (ohm)	No temperature conversion. Resistor value entries are directly applied to input valuables.
RTD Input 0 to 4000 ohm (ohm)	

High Limit/Low Limit

These are the upper limit values and lower limit values of the measured range in the terminal.

For SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

Values between 0 and 100% are assigned to the specified measurement range. The measurement range can only be changed for voltage input modules.

Table Appendix 1.3.2-4 High Limit value/Low Limit value

Input type	Module model	Low limit value of range	High limit value of range
Current input	SAI143/L1AI143	4	20
	S2MMM843	4	20
Voltage input	SAV144/L1AV144	1.000 to 10.000 (default is 1)	1.000 to 10.000 (default is 5)

For SAT145/L1AT145 and SAR145/L1AR145

The upper and lower limits are determined based on the combination of the signal conversion type and the engineering unit symbol. They are shown according to the module type and engineering unit symbol.

Table Appendix 1.3.2-5 Range upper and lower limits for the thermocouple/mV input module (SAT145/L1AT145) (engineering unit symbol C)

Signal conversion	Low limit value of range	High limit value of range
Type K	-200	1200
Type E	-200	900
Type T	-200	350
Type J	-40	750
Type R	0	1600
Type S	0	1600
Type B	600	1700
Type N	-200	1200

Table Appendix 1.3.2-6 Range upper and lower limits for the thermocouple/mV input module (SAT145/L1AT145) (engineering unit symbol F)

Signal conversion	Low limit value of range	High limit value of range
Type K	-300	2200
Type E	-300	1700
Type T	-300	650
Type J	-40	1400
Type R	0	2900
Type S	0	2900
Type B	1100	3100
Type N	-300	2200

Table Appendix 1.3.2-7 Range upper and lower limits for the thermocouple/mV input module (SAT145/L1AT145) (engineering unit symbol K)

Signal conversion	Low limit value of range	High limit value of range
Type K	100	1500
Type E	100	1200
Type T	100	600

Continues on the next page

Table Appendix 1.3.2-7 Range upper and lower limits for the thermocouple/mV input module (SAT145/ L1AT145) (engineering unit symbol K) (Table continued)

Signal conversion	Low limit value of range	High limit value of range
Type J	200	1000
Type R	250	1900
Type S	250	1900
Type B	900	2000
Type N	100	1500

Table Appendix 1.3.2-8 Range upper and lower limits for the thermocouple/mV input module (SAT145/ L1AT145) (engineering unit symbol mV)

Signal conversion	Low limit value of range	High limit value of range
mV Input -20 to 80 mV (%)	-20 (default) to 80	-20 to 80 (default)
mV Input -100 to 150 mV (%)	-100 (default) to 150	-100 to 150 (default)
mV Input -5 to 25 mV (%)	-5 (default) to 25	-5 to 25 (default)
TC Input -20 to 80 mV (V)	-20 (default) to 80	-20 to 80 (default)
TC Input -100 to 150 mV (V)	-100 (default) to 150	-100 to 150 (default)
TC Input -5 to 25 mV (V)	-5 (default) to 25	-5 to 25 (default)

Table Appendix 1.3.2-9 Range upper and lower limits for the resistance temperature detector input module (SAR145/L1AR145) (engineering unit symbol C)

Signal conversion	Low limit value of range	High limit value of range
PT100	-200	850
JPT100	-200	500
PT50	-200	850
PT200	-200	850
PT500	-200	850
PT1000	-200	850
Ni100 (DIN)	-60	250
Ni120 (MINCO)	-80	320

Table Appendix 1.3.2-10 Range upper and lower limits for the resistance temperature detector input module (SAR145/L1AR145) (engineering unit symbol F)

Signal conversion	Low limit value of range	High limit value of range
PT100	-300	1500
JPT100	-300	900
PT50	-300	1500
PT200	-300	1500
PT500	-300	1500
PT1000	-300	1500
Ni100 (DIN)	-50	450
Ni120 (MINCO)	-100	600

Table Appendix 1.3.2-11 Range upper and lower limits for the resistance temperature detector input module (SAR145/L1AR145) (engineering unit symbol K)

Signal conversion	Low limit value of range	High limit value of range
PT100	100	1100
JPT100	100	750
PT50	100	1100
PT200	100	1100
PT500	100	1100
PT1000	100	1100
Ni100 (DIN)	250	500
Ni120 (MINCO)	200	550

Table Appendix 1.3.2-12 Range upper and lower limits for the resistance temperature detector input module (SAR145/L1AR145) (engineering unit symbol ohm)

Signal conversion	Low limit value of range	High limit value of range
RTD Input 0 to 800 ohm (%)	0 (default) to 800	0 to 800 (default)
RTD Input 0 to 4000 ohm (%)	0 (default) to 4000	0 to 4000 (default)
RTD Input 0 to 800 ohm (ohm)	0 (default) to 800	0 to 800 (default)
RTD Input 0 to 4000 ohm (ohm)	0 (default) to 4000	0 to 4000 (default)

Unit

This is the unit for input signal.

For SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

This is determined by the type of input module.

For SAT145/L1AT145 and SAR145/L1AR145

The available types depend on symbol conversion.

- Thermocouple/mV input module (SAT145/L1AT145)

Table Appendix 1.3.2-13 Engineering unit symbols for the thermocouple/mV input module (SAT145/L1AT145)

Engineering unit symbol	Description	Symbol conversion
C	Celsius (default)	Type K, Type E, Type T, Type J, Type R, Type S, Type B, Type N
F	Fahrenheit	
K	Kelvin	
mV	Millivolt	mV input (%), TC input (V)

- Resistance temperature detector input module (SAR145/L1AR145)

Table Appendix 1.3.2-14 Engineering unit symbols for the resistance temperature detector input module (SAT145/L1AT145)

Engineering unit symbol	Description	Symbol conversion
C	Celsius (default)	PT100, JPT100, PT50, PT200, PT500, PT1000, Ni100 (DIN), Ni120 (MINCO)
F	Fahrenheit	
K	Kelvin	
ohm	Ohm	RTD input (%), RTD input (Ω)

Detect IOP (High)

This item specifies whether to detect an input open status when the process value (the value after the input signal was converted (0 to 100%)) exceeds the threshold. When the signal conversion setting is [SQRT], the value prior to the square-root calculation is used as the process value (hereinafter referred to as "process value"). The input value at fault is the value specified by the setting item "Input Processing at Fault".

- No:
  An input open circuit error is not detected.
- Yes:
  If a process value exceeds the threshold value, an input open circuit error is detected and the data status of the input variable connected to the applicable channel becomes BAD (default). The threshold value is specified with [Threshold of IOP (High) %].

Detect IOP (Low)

This item specifies whether or not to detect an input open circuit error if a process value falls below the threshold value. The input value at fault is the value specified by the setting item "Input Processing at Fault."

- No:
  An input open circuit error is not detected.
- Yes:
  If a process value falls below the threshold value, an input open circuit error is detected and the data status of the input variable connected to the applicable channel becomes BAD (default). The threshold value is specified with [Threshold of IOP (Low) %].

Threshold of IOP (High) %

This item specifies the upper limit level at which an input open circuit is detected. This item can only be enabled when [Yes] is specified for [Detect IOP (High)]. The process value exceeding the Detect IOP (High) level means input open.

For SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

The default value is 112.5% (for current input) and 106.3% (for voltage input).

Note that the following checks are performed even if [No] is specified for [Detect IOP (High)]:

- An error occurs if a value is entered such that the value of [Threshold of IOP (High) %] becomes equal to or smaller than the value of [Threshold of Transmitter Fault (High) %].
- An error occurs if a value outside the setting range of the analog input module is entered.
  «Setting range»

  Current input: -18.75% to 118.75% (1 to 23 mA)

  However, in the case of SAI143-H style S3 or later, L1AI143-H, or S2MMM843, -23.75% to 118.75% (0.2 to 23 mA)

  Voltage input: Varies depending on the range specification (0.1 to 11 V).
  - If the range is set to 1 to 10 V: -10% to 111.1% (0.1 to 11 V)
  - If the range is set to 1 to 5 V: -22.5% to 125% (0.1 to 6 V)

In addition to the above checks, the following inputs are checked:

- Number of characters: Up to 7 single-byte characters
- Number of decimal places: Within 2 digits

For SAT145/L1AT145 and SAR145/L1AR145

The default value is 106.3%.

Note that the following checks are performed even if [No] is specified for [Detect IOP (High)]:

- If you input a value outside of the -1000.0% to 1000.0% range, an error occurs.
- If you input a value outside of the -25.0% to 125% range, a warning is displayed when saving.

In addition to the above checks, the following input checks are performed:

- Number of characters: Up to 7 single-byte characters
- Number of decimal places: Within 2 digits

Threshold of IOP (Low) %

This item specifies the lower limit level at which an input open circuit is detected. This item can only be enabled when [Yes] is specified for [Detect IOP (Low)]. The process value less than the Detect IOP (Low) level means input open.

For SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

Specify a value between -25.0% to 125.0%. The default value is -6.3%.

Note that the following checks are performed even if [No] is specified for [Detect IOP (Low)].

- An error occurs if a value is entered such that the value of [Threshold of IOP (Low) %] level becomes equal to or greater than the value of [Threshold of Transmitter Fault (Low) %].
- An error occurs if a value outside the setting range of the analog input module is entered.
  «Setting range»

  Current input: -18.75% to 118.75% (1 to 23 mA)

  However, in the case of SAI143-H style S3 or later, L1AI143-H, or S2MMM843, -23.75% to 118.75% (0.2 to 23 mA)

  Voltage input: Varies depending on the range specification (0.1 to 11 V).
  - If the range is set to 1 to 10 V: -10% to 111.1% (0.1 to 11 V)
  - If the range is set to 1 to 5 V: -22.5% to 125% (0.1 to 6 V)

In addition to the above checks, the following inputs are checked:

- Number of characters: Up to 7 single-byte characters
- Number of decimal places: Within 2 digits

For SAT145/L1AT145 and SAR145/L1AR145

Specify a value between -1000.0% to 1000.0%. The default value is 0.0% for resistance temperature detector input and -6.3% for thermocouple input.

Note that the following checks are performed even if [No] is specified for [Detect IOP (Low)].

- If you input a value outside of the -1000.0% to 1000.0% range, an error occurs.
- If you input a value outside of the -25.0% to 125% range, a warning is displayed when saving.

In addition to the above checks, the following input checks are performed:

- Number of characters: Up to 7 single-byte characters

- Number of decimal places: Within 2 digits

Detect Transmitter Fault (High): SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

This item specifies whether or not to detect a transmitter error if a process value exceeds the threshold value. This item is only enabled for current inputs. The input value at fault is the value specified by the setting item "Input Processing at Transmitter Fault".

- No:
  A transmitter error is not detected.
- Yes:
  If the process value exceeds the threshold value, a transmitter error is detected and the data status of the input variable connected to the applicable channel becomes BAD (default). The threshold value is specified with [Threshold of Transmitter Fault (High) %].

Detect Transmitter Fault (Low): SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

This item specifies whether or not to detect a transmitter error if a process value falls below the threshold value. This item is only enabled for current inputs. The input value at fault is the value specified by the setting item "Input Processing at Transmitter Fault".

- No:
  A transmitter error is not detected.
- Yes:
  If the process value falls below the threshold value, a transmitter error is detected and the data status of the input variable connected to the applicable channel becomes BAD (default). The threshold value is specified with [Threshold of Transmitter Fault (Low) %].

Threshold of Transmitter Fault (High) %: SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

This item specifies the upper limit level at which a transmitter error is detected. This item is enabled only when [Yes] is specified for [Detect Transmitter Fault (High)]. This item is only enabled for current inputs. It is judged that a transmitter error has occurred if the process value exceeds this setting.
The default value is 106.3%.

Note that the following checks are performed even if [No] is specified for [Detect Transmitter Fault (High)]:

- An error occurs if a value is entered such that the value of [Threshold of IOP (High) %] becomes equal to or smaller than the value of [Threshold of Transmitter Fault (High) %].
- An error occurs if a value outside the setting range of the analog input module is entered.
  «Setting range»

  Current input: -18.75% to 118.75% (1 to 23 mA)

  However, in the case of SAI143-H style S3 or later, L1AI143-H, or S2MMM843, -23.75% to 118.75% (0.2 to 23 mA)

Threshold of Transmitter Fault (Low) %: SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

This item specifies the lower limit level at which a transmitter error is detected. This item is enabled only when [Yes] is specified for [Detect Transmitter Fault (Low)]. This item is only

enabled for current inputs. It is judged that a transmitter error has occurred if the process value falls below this setting.
The default value is -1.25%.

Note that the following checks are performed even if [No] is specified for [Detect Transmitter Fault (Low)]:

- An error occurs if a value is entered such that the value of [Threshold of IOP (Low) %] level becomes equal to or greater than the value of [Threshold of Transmitter Fault (Low) %].
- An error occurs if a value outside the setting range of the analog input module is entered. «Setting range»

  Current input: -18.75% to 118.75% (1 to 23 mA)

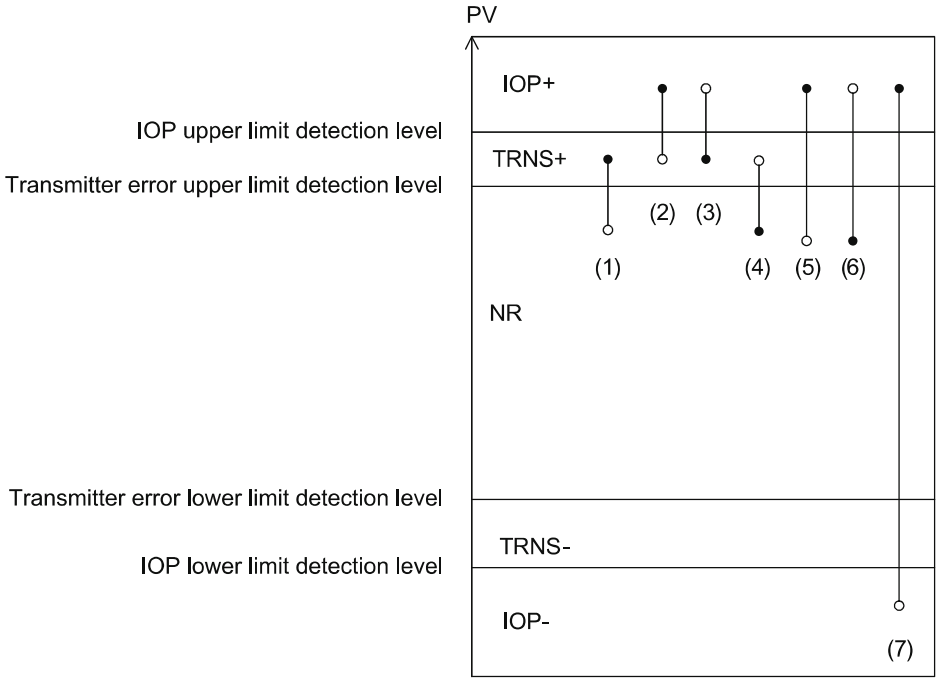
  However, in the case of SAI143-H style S3 or later, L1AI143-H, or S2MMM843, -23.75% to 118.75% (0.2 to 23 mA)

TIP

If it is specified to detect input open (IOP+, IOP-) and transmitter errors (TRNS+, TRNS-), diagnostic information messages indicating the occurrence of an alarm and the recovery are notified as follows:

- If the PV value changes, causing the alarm status to change, a diagnostic information message corresponding to the status after change is notified.
- The diagnostic information message indicating recovery from the generated alarm is notified only when the alarm status recovers to NR (normal). Messages indicating recovery from individual alarms, IOP+/IOP-/TRNS+/TRNS-, are not notified.

Following (1) to (7) are the Diagnostic information messages that are notified at the change of the PV value:



○ PV value before change
● PV value after change

(1) Occurrence of TRNS+
(2) Occurrence of IOP+ (No messages indicating recovery from TRNS+ are generated.)
(3) Occurrence of TRNS+ (No messages indicating recovery from IOP+ are generated.)
(4) Recovery from channel error
(5) Occurrence of IOP+ (No messages indicating occurrence of/recovery from TRNS+ are generated.)
(6) Recovery from channel error
(7) Occurrence of IOP+ (No messages indicating recovery from IOP- are generated.
No messages indicating occurrence of/recovery from TRNS- are generated.
No messages indicating occurrence of/recovery from TRNS+ are generated.)

Figure Appendix 1.3.2-2 Generation of diagnostic information messages

Field Power Diagnosis: SAI143/L1AI143 and SAV144/L1AV144

You need to specify the wiring type. It is used to determine the method of power supply diagnosis of the FIO input modules. Based on this setting, current input modules perform self-diagnosis on whether or not the power is supplied correctly to the field. This item is only enabled for current inputs.

IMPORTANT

Make sure that this setting matches with the 2-wire/4-wire setting that is made by using the setting pins in the analog input module. If the settings are different from those of the hardware, a channel error occurs in the case of single input for FIO module, or the control shifts to the standby module in the case of a dual-redundant input module configuration.

- None: Do not perform field power supply diagnosis.
- 2 wire:
  2-wire (Default: Diagnose that the power is supplied to the field. Diagnosis indicates normal if the power is supplied to the field device.) The input value at fault is the value specified by the setting item "Input Processing at Fault".
- 4 wire:
  4-wire (Diagnose that no power is supplied to the field. Diagnosis indicates normal if no power is supplied to the field device.) The input value at fault is the value specified by the setting item "Input Processing at Fault."

Reference Junction Compensation: SAT145/L1AT145 and SAR145/L1AR145

Specify whether or not to perform reference junction compensation. This item is only available in the thermocouple input module. However, it is not available when [mV Input], [TC Input], or [Type B] is specified for signal conversions.

- No:
  Reference junction compensation is not performed.
- Yes:
  Reference junction compensation is performed (default).

Burnout: SAT145/L1AT145 and SAR145/L1AR145

Specify the input operation when there is a disconnection. When detection of input open circuit errors is enabled and an input open circuit error is detected, the value specified in Input Processing at Fault is set as the input variable.

- Burnout upscale:
  Clamps the input to the upper limit specified by the module when there is a disconnection (default).
- Burnout downscale:
  Clamps the input to the lower limit specified by the module when there is a disconnection.
- No:
  Disables the burnout operation.

Command Line: AIO/DIO module of N-IO

TIP

Specify the command line with no more than 250 single-byte characters. If the command line is not set, the default value is used for each applicable item. The format is as follows:

Item name = Data value, Item name = Data value, ...

HARTPRI (HART communication master priority order setting)

You can specify whether to consider AIO/DIO module of N-IO as the primary master or the secondary master.

- Format
  HARTPRI=Yes
- Parameter
  Yes: The module is set as the primary master. (Default)

  No: The module is set as the secondary master.

For example, you can set the handy terminal as the secondary master when the module is set as the primary master.

HARTEVENT (notification setting for the changed status of HART device)

You can specify whether or not to notify the changed status of HART device. If No is set, the changed status that is received by N-IO I/O module is not notified to the SCS. If Current Input (HART Communication) or Current Output (HART Communication) is selected as signal type, the default is Yes. If other signal type is selected, the default is No.

- Format
  HARTEVENT=No
- Parameter
  Yes: The changed status of HART device is notified.

  No: The changed status of HART device is not notified.

HARTPERIOD (setting of detection period by I/O module for the changed status of HART device)

This item sets the period in which the AIO/DIO module of N-IO detects detailed information of HART device by using Command #48. This can be set only when HARTEVENT=Yes.

- Format
  HARTPERIOD=30
- Parameter
  Select either 15, 30, 45, or 60 seconds. The default is 30 seconds.

Appendix 1.3.3 Settings for the AO channel

The following are the settings for the AO channel in I/O Parameter Builder.

Table Appendix 1.3.3-1 Items set for each channel of analog output module

Setting items	Online change download (*1)	IOM download (*2)	Remarks
Channel Number (Specify Channel Number)	-	-	-
Wiring Position (Specify Wiring Position)	-	-	-
I/O Variable Name (Specify I/O Variable Name)	-	-	-
Direction (Specify Direction)	-	-	-
Comment (Specify Comment)	-	-	-
I/O Shutoff Switch (Specify I/O Shutoff Switch)	Yes	Yes	-
Output Shutoff Switch (Specify Output Shutoff Switch)	Yes	Yes	-
Output Processing at Fault (Specify Output processing at fault)	Yes	Yes	-
Output Value at Fault (Specify Output value at fault)	Yes	Yes	-
Tight-shut/Full-open (Specify Tight-shut/Full-open)	Yes	Yes(*3)	-
Tight-shut Value (Specify Tight-shut Value)	Yes	Yes	-
Full-open Value (Specify Full-open Value)	Yes	No	-
Detect Short Circuit (Specify Detect Short Circuit)	Yes	Yes	-
Detect Disconnection (Specify Detect Disconnection)	Yes	Yes	-
P&ID Tag Name (Specify P&ID Tag Name)	Yes	No	-
Command Line (Specify Command Line)	Yes	Yes	For the AIO/DIO module of N-IO, the IOM download does not take place.

*1: Indicates whether the setting can be changed by online change downloading.
Yes: The setting can be changed by online change downloading.
No: Online change downloading is not possible
- : Not a target

*2: Indicates whether the IOM downloading is performed with the online change downloading.
Yes: The IOM downloading is performed together with the online change downloading.
No: The IOM downloading is not performed together with the online change downloading.
- : Not a target

*3: IOM downloading may be performed according to the modified contents.

The setting items that are not explained above as common items are explained below.

I/O Shutoff Switch: AIO/DIO module of N-IO

Specifies whether or not to activate the I/O shutoff switch when a critical malfunction that can prevent normal output has occurred. If the I/O shutoff switch is activated, all channels of the corresponding module other than the AI channel (4-wire) are shut off.

- Enable:
  Activates the I/O shutoff switch when a critical malfunction such as an overcurrent occurs (default).
- Disable:
  Does not activate the I/O shutoff switch even when a critical malfunction occurs.

Output Shutoff Switch: analog output module of FIO

The output shutoff switch can be used to shutoff all the outputs of the module when the module encounters a critical malfunction for properly outputting signals, and the whole module becomes failure mode (Module HRDY OFF). Enable or disable this switch needs to be specified.

- Enable:
  Activate the Output Shutoff switch if a dangerous failure occurs (default).
- Disable:
  Do not activate the Output Shutoff switch even if a dangerous failure occurs.

Output Processing at Fault

This item needs to be specified so that when an error occurs in CPU module (both CPU modules in redundant configuration) or in the path from CPU to output module, the output module can act the specified processing for the output from the output channel to the field device.

- Hold:
  Hold the outputs upon detection of an error.
- Fixed Value:
  Change each output value to the value specified in [Output Value at Fault] upon detection of an error (default).

Output Value at Fault

This value is used as a fail-safe value (i.e., output value at fault) when [Output Processing at Fault] is set to [Fixed Value].

- Specify the value to be output upon error, in a range of -17.19 to 117.19 (%). The default value is -17.19 %. This setting is effective only when [Output Processing at Fault] is set to [Fixed Value].

The following input checks are performed.

- Range: -17.19 to 117.19 (%)
- Permitted characters: Single-byte numbers, decimal point, negative sign (-)
- Number of characters: Up to 6 single-byte characters
- Number of decimal places: Within 2 digits

Tight-shut/Full-open

Tight-shut/full-open is a function that reduces the actual output value to 0% or below when the manipulated output value is 0%, or increases the actual output value to 100% or above when the manipulated output value is 100%, in order to fully close or open the control valve firmly. Specify whether or not to enable this function.
If PRM (Plant Resource Manager) is used, set "Tight-shut/Full-open" to "Yes" and determine an appropriate tight-shut value for the connected device.

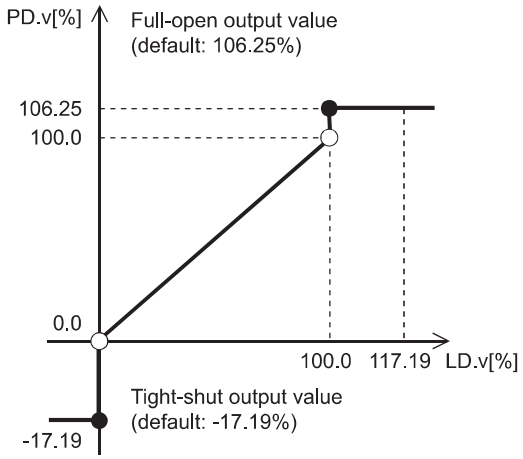
- Yes:
  Enable the tight-shut/full-open function (default). Specify a tight-shut value in [Tight-shut Value], and a full-open value in [Full-open Value].

The initial output value of the module (i.e., default initial value upon power-on) will be the same value of the tight-shut output.

- No:
  Disable the tight-shut/full-open function. The initial output value of the module (default initial value upon power-on) is fixed to -17.19% (1.25 mA).

The following graphs show the relationships of logical data (LD) and physical data (PD) when the data is normal, output is enabled, and output variable is not locked.

<Relationship of LD and PD with tight-shut specification>



<Relationship of LD and PD without tight-shut specification>

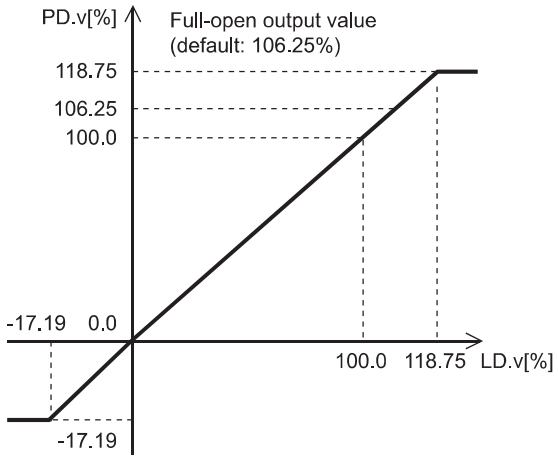


Figure Appendix 1.3.3-1 The following graphs show the relationships of logical data (LD) and physical data (PD) when the data is normal, output is enabled, and output variable is not locked.

Tight-shut Value

This item specifies in a range of -17.19 to 0 (%) the actual value to be output when the tight-shut/full-open function is specified and the output value is 0 %. The default is -17.19 % (1.25 mA). This setting is possible only when [Tight-shut/Full-open] is set to [Yes].
The following input checks are performed.

- Range: -17.19 to 0 (%)
- Permitted characters: Single-byte numbers, decimal point, negative sign (-)
- Number of characters: Up to 6 single-byte characters
- Number of decimal places: Within 2 digits

Full-open Value

This item specifies in a range of 100 to 117.19 (%) the actual value to be output when the tight-shut/full-open function is specified and the output value is 100%. The default is 106.25% (21 mA). This setting is possible only when [Tight-shut/Full-open] is set to [Yes]. To implement "reverse output", create the necessary application using the application logic.
The following input checks are performed.

- Range: 100 to 117.19 (%)
- Permitted characters: Single-byte numbers, decimal point
- Number of characters: Up to 6 single-byte characters
- Number of decimal places: Within 2 digits

Detect Short Circuit

This item specifies whether or not to detect short circuit. If a base plate for the barrier is used, it is fixed to No.

- Yes: Detect short circuit (default).
- No: Do not detect short circuit.

Detect Disconnection

This item specifies whether or not to detect open circuit.

- Yes: Detect disconnection (default).
- No: Do not detect disconnection.

Command Line

TIP

For the analog output module of FIO, specify the command with no more than 256 single-byte characters. For the AIO/DIO module of N-IO, specify the command with no more than 250 single-byte characters. If the command line is not set, the default value is used for each applicable item. The format is as follows:

Item name = Data value, Item name = Data value, ...

SCREG (short circuit detection level)

This item specifies a short circuit detection level. A short circuit is detected when the wiring resistance falls below the set value. By specifying a value greater than the wiring resistance as the short circuit detection level, a short circuit on a device terminal can be detected. The default value is 70 Ω.

- Format
  SCREG=100
- Parameter
  Specify an integer value for SCREG. The unit is ohms (Ω) and the specifiable range is 60 to 750 Ω. SCREG must satisfy the following condition:
  SCREG (short circuit detection level setting) > Wiring resistance (*1)

  *1: Add the resistance of KS cables, etc. to the wiring resistance.

IMPORTANT

If the current output value falls below -6.25 % (3 mA) due to the settings in [Output Value at Fault] and [Tight-shut Value], the short circuit detection operation becomes unstable in the range of SCREG setting ±20 Ω.

Therefore, considering the above characteristic and the actual wiring resistance, you need to set an appropriate SCREG value that allows the short circuit detection to be performed without fail.

If the default SCREG setting (SCREG=70) is used without setting the command line, a short circuit is not detected if the wiring resistance reaches or exceeds 90 Ω. However, a short circuit is detected without fail when the wiring resistance is 50 Ω or below.

Example:

When a device is connected by using a KS cable and SCREG is set to 70 Ω

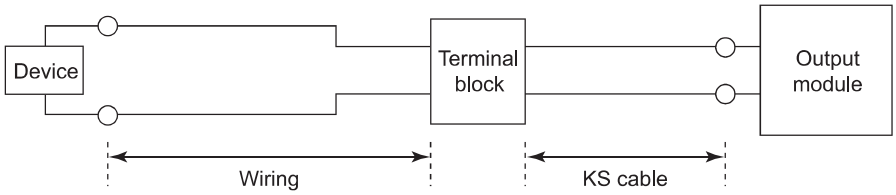


Figure Appendix 1.3.3-2 Example of a device connection by using a KS cable

- Add the resistance of a KS cable to the wiring resistance.
- If SCREG is set to 70 Ω, the following operations are performed according to the output current value:
  - 3 mA (-6.25%) or above
    There is an error of ±10 Ω. A short circuit is always detected if the wiring resistance is 60 Ω or below. A short circuit is not detected if the wiring resistance is 80 Ω or above.
  - 1 mA (-18.75%) or above, but below 3 mA
    There is an error of ±20 Ω. A short circuit is always detected if the wiring resistance is 50 Ω or below. A short circuit is not detected if the wiring resistance is 90 Ω or above.
  - Below 1 mA
    A short circuit is not detected.

TIP

The resistance value of a KS cable is 230 Ω/km while the resistance value of a standard cable (such as AWG20) is 23 to 50 Ω/km.

SOOP (Output open detection level): AIO/DIO module of N-IO

This item specifies an output open (OOP) detection level. An open circuit error is recognized when the readback value of an output falls below the set value. The default is 0.00085 A.

Format

- SOOP=0.001

Parameter

- Output open detection level
  You need to specify an output open detection level in amperes (A).

  SOOP < Output value at fault (fail-safe value)

  If tight-shut output is specified : SOOP < Tight-shut output value

  If tight-shut output is not specified : SOOP < Power-on output value (0.00125 A)
- This item can be changed via online change download. Note, however, that IOM download is also performed at the same time.

HARTPRI (HART communication master priority order settings): AIO/DIO module of N-IO

You can specify whether to consider AIO/DIO module of N-IO as the primary master or the secondary master.

- Format
  HARTPRI=Yes
- Parameter
  Yes: The module is set as the primary master. (Default)

  No: The module is set as the secondary master.

For example, you can set the handy terminal as the secondary master when the module is set as the primary master.

HARTEVENT (notification settings for the changed status of HART device): AIO/DIO module of N-IO

You can specify whether or not to notify the changed status of HART device. If No is set, the changed status that is received by N-IO I/O module is not notified to the SCS. If Current Input (HART Communication) or Current Output (HART Communication) is selected as signal type, the default is Yes. If other signal type is selected, the default is No.

- Format
  HARTEVENT=No
- Parameter
  Yes: The changed status of HART device is notified.

  No: The changed status of HART device is not notified.

HARTPERIOD (setting of detection period by I/O module for the changed status of HART device): AIO/DIO module of N-IO

This item sets the period in which the AIO/DIO module of N-IO detects detailed information of HART device by using Command #48. This can be set only when HARTEVENT=Yes.

- Format
  HARTPERIOD=30
- Parameter
  Select either 15, 30, 45, or 60 seconds. The default is 30 seconds.

Appendix 1.3.4 Settings for the DI channel

The following are the settings for the DI channel in I/O Parameter Builder.

Table Appendix 1.3.4-1 Items set for each channel of a digital input module

Setting items	Online change Download (*1)	IOM Download (*2)	Remarks
Channel Number (Specify Channel Number)	-	-	-
Wiring Position (Specify Wiring Position)	-	-	-
I/O Variable Name (Specify I/O Variable Name)	-	-	-
Direction (Specify Direction)	-	-	-
Comment (Specify Comment)	-	-	-
Input Processing at Fault (Specify Input Processing at Fault)	Yes	No	-
Detect Disconnection (Specify Detect Disconnection)	Yes	Yes	-
Detect Short Circuit (Specify Detect Short Circuit)	Yes	Yes	-
Detect LFD (Specify Detect LFD)	Yes	Yes	-
Pulse Test (Specify Pulse Test)	Yes	Yes	-
SOER (Setting for SOER) (Specify Trip Signal)	Yes	Yes	-
Trip Signal (Setting for SOER) (Specify Trip Signal)	Yes	No	-
P&ID Tag Name (Specify P&ID Tag Name)	Yes	No	-

*1: Indicates whether the setting can be changed by online change downloading.
Yes: The setting can be changed by online change downloading.
No: Online change downloading is not required.
- : Not a target

*2: Indicates whether the IOM downloading is performed with the online change downloading.
Yes: The IOM downloading is performed together with the online change downloading.
No: The IOM downloading is not performed together with the online change downloading.
- : Not a target

Each of setting items that are not explained as common items is explained as follows.

Input Processing at Fault

This item specifies a value that will be passed to the application logic instead of the input from the field if an error is detected in the input of the channel, including channel errors, DI module errors and errors in the path from the CPU to the DI module.

- 0: The input value is set to 0 at error detection (default).
- 1: The input value is set to 1 at error detection.
- Hold: The value immediately before the error was detected is retained when an error is detected.

Detect Disconnection (Open Circuit)

This item specifies whether to detect disconnection (open circuit). If a base plate for the barrier is used, it is fixed to [No].

- Yes: Detect disconnection.
- No: Do not detect disconnection (default). When the disconnection occurs, input value is 0 and the status is GOOD.

IMPORTANT

If [Yes] is set for [Detect Disconnection], disconnection errors can be detected. Make sure, however, to connect a wiring check adapter (SCB100) on the channel if you specify [Yes]. If you specify [Yes] without connecting the adapter, the SCS erroneously detects a disconnection error whenever the input value is OFF.

Detect Short Circuit

This item specifies whether or not to detect a short circuit in the wiring. If a base plate for the barrier is used, it is fixed to [No].

- Yes: Detect short circuit (default).
- No: Do not detect short circuit. When the short-circuit error occurs, input value is 1 and the status is GOOD.

IMPORTANT

If [Yes] is set for Detect Short Circuit, short-circuit errors can be detected (assuming short circuit with the power supply line). However, if you specify [Yes] , ensure to install a wiring check adapter (SCB110) in the channel. If you specify [Yes] without connecting the adapter, the SCS erroneously detects a short-circuit error whenever the input value is ON.

Detect LFD: AIO/DIO module of N-IO

This item specifies whether or not to detect line fault in the barrier.

- Type A, Type B: Line fault is detected.
- No: Line fault is not detected.

Pulse Test: digital input module of FIO

This item specifies whether or not to perform a pulse test (wiring check between the input channels using pulse output).

- Yes: Perform a pulse test (default)
- No: Do not perform the pulse test

IMPORTANT

If [Yes] is set for [Pulse Test], wiring short-circuit errors between input channels can be detected. Make sure, however, to connect a wiring check adapter (SCB110) to the channel if you specify [Yes] for a channel which receives NC input signals.. If you specify [Yes] without connecting the adapter, the SCS cannot detect inter-channel short circuit when the input value is ON.

SOER (setting for SOER)

This item specifies whether or not to accumulate events for SOER when a signal changes.

- Yes: Accumulate SOE events when a signal changes (default).
- No: Do not accumulate SOE events.

Trip Signal (setting for SOER)

This item specifies whether or not to regard an event as a trip occurrence. This setting is only enabled if [Yes] is set for [SOER].

- No (0):
  Changes are not regarded as a trip signal (default).
- OFF TRIP (1):
  A change to OFF is regarded as a trip signal and SOE data before and after a trip is stored in an SCS.
- ON TRIP (2):
  A change to ON is regarded as a trip signal and SOE data before and after a trip is stored in an SCS.

Appendix 1.3.5 Settings for the DO channel

The following are the settings for the DO channel in I/O Parameter Builder.

Table Appendix 1.3.5-1 Items set for each channel of a digital output module

Setting items	Online change download (*1)	IOM download (*2)	Remarks
Channel Number (Specify Channel Number)	-	-	-
Wiring Position (Specify Wiring Position)	-	-	-
I/O Variable Name (Specify I/O Variable Name)	-	-	-
Direction (Specify Direction)	-	-	-
Comment (Specify Comment)	-	-	-
Output Shutoff Switch (Specify Output Shutoff Switch)	Yes	Yes	-
DO Shutoff Switch (Specify DO Shutoff Switch)	Yes	Yes	-
Output Value in Detecting Error/Output Processing at Fault (*3) (Specify Output processing at fault)	Yes	Yes	-
Detect Disconnection (Specify Detect Disconnection)	Yes	Yes	-
Detect LFD (Specify Detect LFD)	Yes	Yes	-
Pulse Test (OFF) (Specify Pulse Test (OFF))	Yes	Yes	-
Pulse Test (ON) (Specify Pulse Test (ON))	Yes	Yes	-
Low Voltage Pulse Test (On) (Specify Low Voltage Pulse Test (On))	Yes	Yes	-
SOER (Setting for SOER) (Specify Trip Signal)	Yes	No	-
Trip Signal (Setting for SOER) (Specify Trip Signal)	Yes	No	-
P&ID Tag Name (Specify P&ID Tag Name)	Yes	No	-
Command Line (Specify Command Line)	No	No	This item does not need to be entered.

*1: Indicates whether the setting can be changed by online change downloading.
Yes: The setting can be changed by online change downloading.
No: Online change downloading is not required.
- : Not a target

*2: Indicates whether the IOM downloading is performed with the online change downloading.
Yes: The IOM downloading is performed together with the online change downloading.
No: The IOM downloading is not performed together with the online change downloading.
- : Not a target

*3: For FIO, Output Value in Detecting Error, and for N-IO, Output Processing at Fault

Each of setting items that are not explained as common items is explained as follows.

Output Shutoff Switch: digital output module of FIO

The output shutoff switch can be used to shutoff all the outputs of the module when the module encounters a critical malfunction such as the output is clutched to ON status, and the whole module becomes failure mode (Module HRDY OFF). If the Output Shutoff switch is activated, the output of all DO channels of the relevant module is set to OFF. This setting is not affected in the event of short circuit. For SDV526/L1DV526, this setting cannot be changed. It is fixed at Disable.

- Enable:
  Activate the Output Shutoff switch if a dangerous failure such as the output getting stuck in the ON status occurs (default).
- Disable:
  Do not activate the Output Shutoff switch even if a dangerous failure occurs.

DO Shutoff Switch: AIO/DIO module of N-IO

You can specify whether or not to activate the DO shutoff switch if a critical malfunction that can prevent normal output has occurred to the module. If the DO shutoff switch is activated, all DO channels of the corresponding modules are shut off.

- Enable:
  Activate the DO shutoff switch if a critical malfunction such as output stuck occurs (default).
- Disable:
  Do not activate the DO shutoff switch even if a critical malfunction occurs.

Output Value in Detecting Error/Output Processing at Fault

This item specifies a value output from the channel to the field if an error occurs on the CPU module (both CPU modules in redundant configuration) or in the path from CPU to output module. This definition is used as the fail-safe value set for the output variables. For SDV526/L1DV526, this setting cannot be changed. It is fixed at the default value.

- 0: Output 0 to the field at error detection (default).
- 1: Output 1 to the field at error detection.
- Hold: The value immediately before the error was detected is maintained.

TIP

For FIO, the name of this item is Output Value in Detecting Error, and for N-IO, it is Output Processing at Fault.

In AD Suite, however, specify a value in Output Processing at Fault even if it is FIO. The value is reflected in this item when you run Reflection.

Detect Disconnection (Open Circuit detection)

This item specifies whether to detect disconnection (open circuit). If a base plate for the barrier is used, it is fixed to No. To detect disconnection for AIO/DIO modules of N-IO, also set Low Voltage Pulse Test (On) to Yes.

- Yes: Detect disconnection (default)
- No: Do not detect disconnection

Detect LFD: AIO/DIO module of N-IO

This item specifies whether or not to detect line fault in the barrier.

- Type A, Type B: Line fault is detected.
- No: Line fault is not detected.

Pulse Test (OFF)

This item specifies whether to implement the off-edge pulse test. This item enables the use of the off-edge pulse output to test the wiring of the channel that may be clutched to ON status. For SDV526/L1DV526, this setting is fixed to No. For digital output modules other than SDV526/L1DV526, faults that can be detected are clutched-to-ON faults and short circuits between channels. Only clutched-to-ON faults can be detected for S2MMM843 and S2MDV843.

- Yes: Perform the off-edge pulse test (default)
- No: Do not perform the pulse test

Pulse Test (ON)

This item specifies whether to implement the on-edge pulse test. This item enables the use of the on-edge pulse output to test the wiring of the channel that may be clutched to OFF status. For SDV526/L1DV526, this setting is fixed to No. For digital output modules other than SDV526/L1DV526, faults that can be detected are clutched-to-OFF faults, short circuits between channels, and short circuits while an OFF signal is being output. Only clutched-to-OFF faults can be detected for S2MMM843 and S2MDV843.

- Yes: Perform the on-edge pulse test
- No: Do not perform the pulse test (default)

Low Voltage Pulse Test (On): AIO/DIO module of N-IO

This item specifies whether to implement low voltage pulse test (on). This item enables the use of the on-edge pulse output (5V) to test the wiring in order to detect open circuit and short circuit while an OFF signal is being output. To detect disconnection, set Detect Disconnection to Yes.

- Yes: Conduct the low voltage pulse test (on) (default)
- No: Do not conduct the low voltage pulse test

SOER (setting for SOER)

This item specifies whether or not to accumulate events for SOER when a signal changes.

- Yes: Accumulate SOE events when a signal changes.
- No: Do not accumulate SOE events (default).

Trip signal (setting for SOER)

This item specifies whether or not to regard an event as a trip occurrence. This setting is only enabled if [Yes] is set for [SOER].

- No (0):
  Changes are not regarded as a trip signal (default).
- OFF TRIP (1):
  A change to OFF is regarded as a trip signal and SOE data before and after a trip is stored in an SCS.
- ON TRIP (2):

A change to ON is regarded as a trip signal and SOE data before and after a trip is stored in an SCS.

Command Line

This item does not need to be entered.

Appendix 2. RS original engineering

RS original engineering is applied to SCS projects for which I/O list engineering is not performed. This section describes the engineering methods that are unique to RS original engineering. If you select the RS original engineering method, you cannot engineer using iDefine.

TIP

RS projects that include SCS projects that were created before introducing AD Suite can also be registered in AD Server.
The history management function of AD Server can be used on SCS projects that have been registered in AD Server.

SEE ALSO

For more information about history management function, refer to:

C2., “History management” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects to AD Server, refer to:

C1.2.3, “Registering RS projects in the AD project” on page C1-13

Appendix 2.1 Operations on SCS projects that are not registered in the AD project

In principle, RS projects, including SCS projects, must be registered in AD projects. However, in some cases, RS projects cannot be registered in AD projects because the timing of the modification does not fit or for other reasons. The actions to take in such a case are described as follows:

- Starting SCS Manager
- Backing up SCS Projects

Starting SCS Manager

Select [YOKOGAWA ProSafe] > [Workbench]. SCS Manager starts up.

TIP

- With Windows 10, select [ProSafe] > [Workbench].
- It is not possible to open SCS Manager and Version Control Tool, or to open SCS Manager and Master Database Restoring Function at the same time.
- For SCS projects that are engineered in RS original engineering and are registered in an AD project, you can start SCS Manager from AD Organizer. In System Structure Navigator, select the SCS and click the button for calling SCS Manager.

Backing up RS projects

When you back up all the folders under an RS project folder, all the SCS projects containing the implementation data of an application are also backed up.

The RS project backup shall be saved in external media, by saving folders below the RS project folder using Windows Explorer.

IMPORTANT

The RS project backup operation must be performed when the engineering function and SCS Maintenance Support Tool are not used.

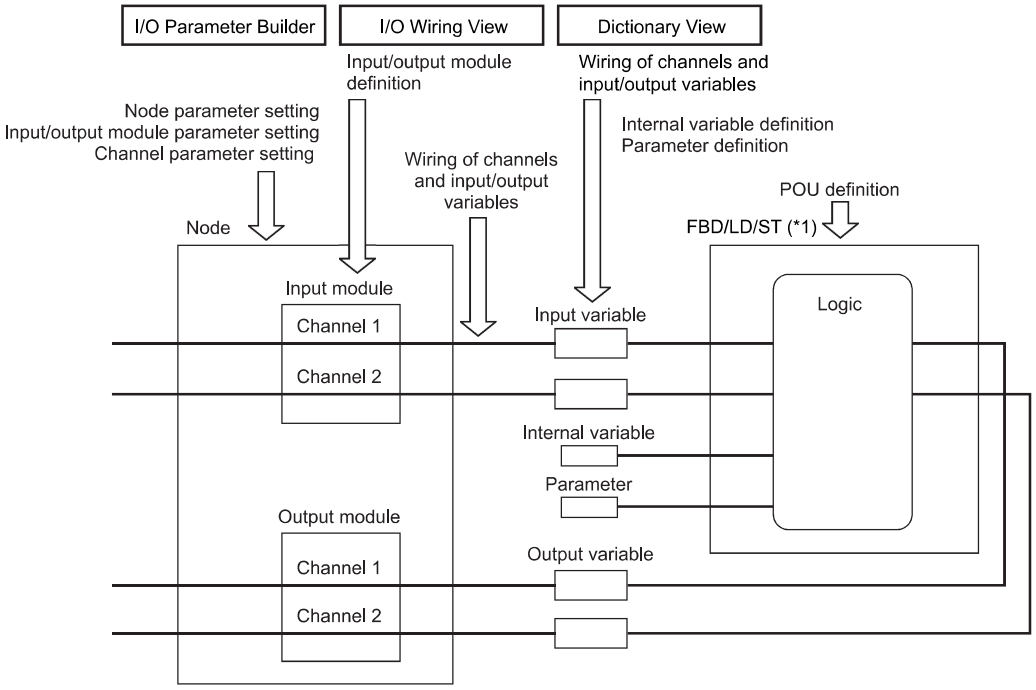
When you choose the standard model of IT security, you need to logon to the PC with a user account that is authorized to access the ProSafe-RS related folders so as to perform backups.

Appendix 2.2 Definitions of inputs/outputs

When defining inputs and outputs, use Dictionary View, I/O Wiring View and I/O Parameter Builder to set the following items.

Table Appendix 2.2-1 Definitions of inputs and outputs

Definition	Description	Tool used
Input/output variable definition	Define input/output variables.	Dictionary View
Input/output module definition	Define the configuration of input/output modules. Specify the model and mounting position (node number and slot number) of a module, as well as redundancy.	I/O Wiring View
Wiring of channels and input/output variables	Assign input/output variables to channels.	
Node parameter setting	Set parameters for nodes.	I/O Parameter Builder
Input/output module parameter setting	Set parameters for input/output modules.	
Channel parameter setting	Set parameters for channels.	



*1: ST can be used for user-defined FB/FU only.

Figure Appendix 2.2-1 Definitions of inputs/outputs

SEE ALSO For more information about Dictionary View details, refer to:

"Dictionary View" in "Workbench" in the Workbench User's Guide

Input/Output definition operations

Input/output definitions are made using Dictionary View, I/O Wiring View and I/O Parameter Builder.

IMPORTANT

If you changed I/O definitions and saved them in I/O Wiring View, make sure to save them also in I/O Parameter Builder.

Make input/output definitions according to the following procedure.

1. Input/output variable definition
   Define input/output variables using Dictionary View.
2. Definitions of I/O modules
   You need to define I/O modules by using I/O Wiring View, and set the mounting positions of I/O modules (node number and slot number, or unit number) and whether to make them redundant or not.
3. Wiring of channels and input/output variables
   Use I/O Wiring View to associate the channels of the input/output module with the input/output variables.
4. Parameter settings

   Use I/O Parameter Builder to set parameters for nodes, input/output modules and channels.

TIP

Steps “1. Definitions of I/O variables” and “2. Definitions of I/O modules” can be performed independently; however, both steps must be performed before “3. Wiring of channels and I/O variables."

Steps “3. Wiring of channels and I/O variables” and “4. Parameter settings” can be performed independently in FIO I/O modules; however, steps must be performed in a sequence in universal type I/O modules. This is because the signal category is determined by wiring the channel and I/O variable in the universal type I/O module. You cannot set the parameter when the signal category is not determined because the parameter settings vary depending on the signal category.

Appendix 2.2.1 I/O Wiring View

I/O Wiring View is used to define input/output modules.

Make the following definitions in I/O Wiring View.

- Creation and deletion of input/output modules
- Specification of mounting positions of input/output modules
- Selection of redundant and single input/output module configurations
- Wiring of variables and channels

IMPORTANT

- When editing definitions in I/O Wiring View, close I/O Parameter Builder first.
- If you changed I/O definitions and saved them in I/O Wiring View, make sure to save them also in I/O Parameter Builder.

How to display I/O Wiring View

Select [I/O Wiring] from the [Project] menu of SCS Manager; I/O Wiring View appears.

I/O Wiring View window structure

I/O Wiring View consists of I/O Wiring Tree View that lists input/output modules and I/O Wiring Grid View that lists input/output variables that can be wired to channels.

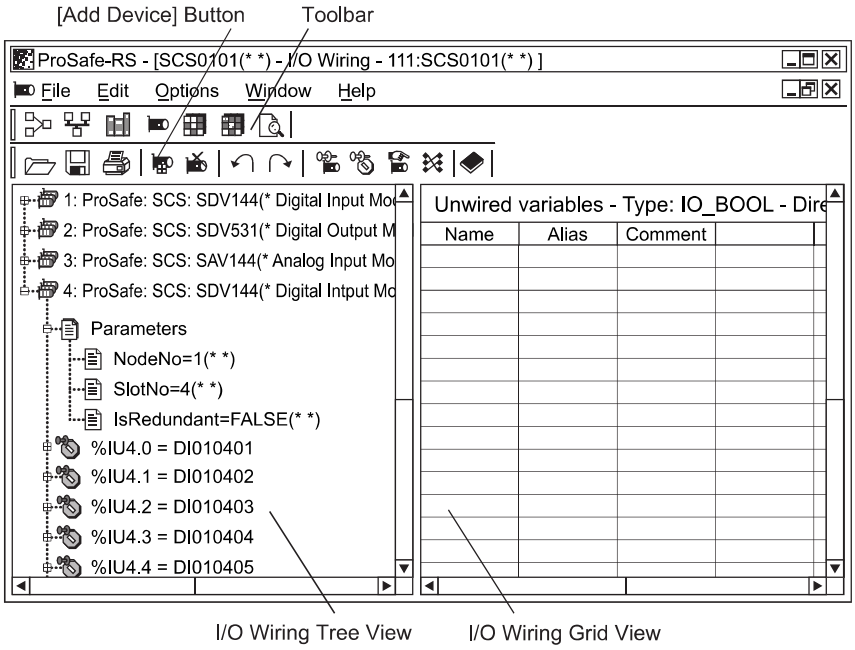


Figure Appendix 2.2.1-1 I/O Wiring View

SEE ALSO For more information about Dictionary View details, refer to:

"I/O Wiring View" in "Workbench" in the Workbench User's Guide

Setting items in I/O Wiring View

You need to set the following items in I/O Wiring View:

- Model of input/output module
- Device index
- Node number
- Unit number (for N-IO I/O module)
- Slot number
- Specification of redundancy
- Wiring of channels and input/output variables

However, to change the model of input/output module or device index, you need to first delete the model and then add the new setting.

Creation of Input/Output modules

To add input/output modules, click "Add Device" button in the toolbar. The Device Selection dialog box appears.

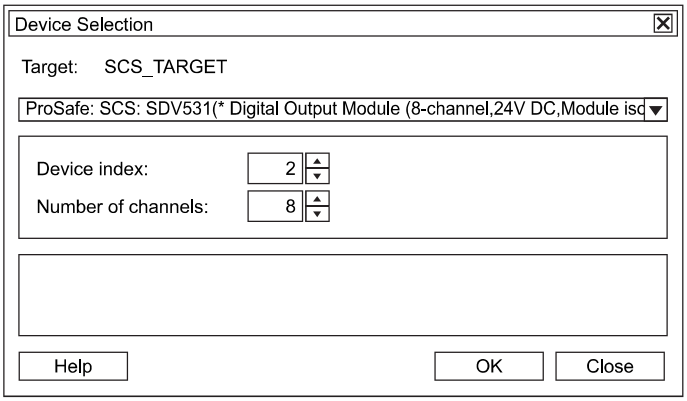


Figure Appendix 2.2.1-2 Device Selection dialog box

Adding AIO/DIO modules or communication modules

When adding an AIO/DIO module or communication module, specify the model of the module in I/O Wiring View.

AIO/DIO modules for SCS supporting SIL 3 that can be specified are as follows.

Table Appendix 2.2.1-1 AIO/DIO modules for SCS supporting SIL 3 that can be specified

AIO/DIO module model	Description
SAI143	Analog input module (4 to 20 mA, 16-channel, module isolation)
SAI143H	Analog input module (4 to 20 mA, 16-channel, module isolation, with HART communication)
SAV144	Analog input module (1 to 5 V/1 to 10 V, 16-channel, module isolation)
SAT145	Analog input module (thermocouple/mV, 16-channel, isolated channels)
SAR145	Analog input module (RTD, 16-channel, isolated channels)
SAI533H	Analog output module (4 to 20 mA, 8-channel output, module isolation, with HART communication)

Continues on the next page

Table Appendix 2.2.1-1 AIO/DIO modules for SCS supporting SIL 3 that can be specified (Table continued)

AIO/DIO module model	Description
SDV144	Digital input module (24 V DC, 16-channel, module isolation)
SDV521	Digital output module (24 V DC, 4-channel, module isolation)
SDV526	Digital output module (100 to 120 V AC, 4-channel, module isolation)
SDV531	Digital output module (24 V DC, 8-channel, module isolation)
SDV531L	Digital output module (24 V DC, 8-channel, module isolation, long distance type)
SDV53A	Digital output module (48 V DC, 8-channel, module isolation)
SDV541	Digital output module (24 V DC, 16-channel, module isolation)
S2MMM843	Analog digital I/O modules (16-channel, module isolation)
S2MDV843	Digital I/O modules (16-channel, module isolation)
SEC402/SEC401 (*1)	ESB bus coupler module
S2EN402/S2EN404 (*1)	N-ESB bus coupler module

*1: Set SEC402/SEC401 and S2EN402/S2EN404 to connect the CPU node and the node by using ESB bus or N-ESB bus. These are not AIO/DIO modules; however, they are described in the same table.

AIO/DIO modules for SCS supporting SIL 2 that can be specified are as follows:

Table Appendix 2.2.1-2 AIO/DIO modules for SCS supporting SIL 2 that can be specified

AIO/DIO module model	Description
L1AI143	Analog input module (4 to 20 mA, 16-channel, module isolation)
L1AI143H	Analog input module (4 to 20 mA, 16-channel, module isolation, with HART communication)
L1AV144	Analog input module (1 to 5 V/1 to 10 V, 16-channel, module isolation)
L1AT145	Analog input module (thermocouple/mV, 16-channel, isolated channels)
L1AR145	Analog input module (RTD, 16-channel, isolated channels)
L1AI533H	Analog output module (4 to 20 mA, 8-channel output, module isolation, with HART communication)
L1DV144	Digital input module (24 V DC, 16-channel, module isolation)
L1DV521	Digital output module (24 V DC, 4-channel, module isolation)
L1DV526	Digital output module (100 to 120 V AC, 4-channel, module isolation)
L1DV531L	Digital output module (24 V DC, 8-channel, module isolation, long distance type)
L1DV53A	Digital output module (48 V DC, 8-channel, module isolation)
L1DV541	Digital output module (24 V DC, 16-channel, module isolation)
L1EC402/L1EC401 (*1)	ESB bus coupler module

*1: Set L1EC402/L1EC401 to connect the CPU node and the node by using ESB bus. These are not AIO/DIO modules; however, they are described in the same table.

Communication modules that can be specified are as follows. The communication modules that can be specified differ depending on the communication type.

Table Appendix 2.2.1-3 Communication modules that can be specified

Communication module	Description	Communication modules that can be specified	
		For Modbus slave communication	For subsystem communication (*1)
ALR111	RS-232C communication module (2-Port)	ALR111	ALR111M

Continues on the next page

Table Appendix 2.2.1-3 Communication modules that can be specified (Table continued)

Communication module	Description	Communication modules that can be specified	
		For Modbus slave communication	For subsystem communication (*1)
ALR121	RS-422/RS-485 communication module (2-Port)	ALR121	ALR121M
ALE111 (*2)	Ethernet communication module (10BASE-T, 1-Port)	ALE111	ALE111M

*1: In I/O Wiring View and I/O Parameter Builder, names are displayed in this way. However, in other SENG windows and the HIS status display view, the final "M" is not displayed.
*2: When the CPU node of SCS is SSC10D or SSC10S, do not define ALE111.

TIP

- You can use SSB401, S2EN501, SNT401, SNT411, SNT501, and SNT511, without setting it in the I/O Wiring View.
- You can use L1SB401, L1NT401, L1NT411, L1NT501, and L1NT511, without setting it in the I/O Wiring View.

Device index

This is an identifier that is attached to I/O modules. Set a unique numeric value in the range of 0 to 65535. Mounting position of the I/O modules is independent; however, it is recommend to specify the relevant number for the indexes.

IMPORTANT

The index cannot be changed after creating I/O modules.

Number of channels

The number of channels in the defined input/output module is displayed.

Mounting position of Input/Output module and setting of redundancy

In I/O wiring tree view of I/O Wiring View, double-click [Parameters] of an I/O module. The I/O Parameters dialog box appears.
Set the mounting position (node number, unit number, and slot number) and whether or not to use a redundant configuration. You cannot set a redundant configuration for ALR121 that is used in ProSafe-SLS communication function.

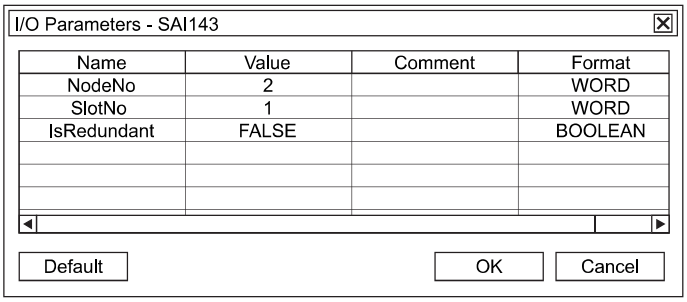


Figure Appendix 2.2.1-3 I/O Parameters dialog box

IMPORTANT

The I/O Parameters dialog box is used to specify the mounting position and redundancy. Parameters of input/output modules are specified in I/O Parameter Builder.

● Node number (NodeNo), unit number (UnitNo), and slot number (SlotNo)

You need to set the mounting position of the I/O module. The allowed range of the node number, unit number, and slot number is as follows.

Table Appendix 2.2.1-4 Allowed range of the node number, unit number, and slot number

Setting item	Allowed range		
	N-IO I/O module	FIO I/O module	
	SCSP3	SCSP3/SCSL2/SCSP2	SCSV1/SCSP1
Node number	1 to 32	1 to 14	1 to 10
Unit number	1 to 6	-	-
Slot number	1 to 2 (*1)	1 to 8	1 to 8

*1: For single configuration, only one module can be defined in a unit. Either of the slot numbers can be used.

To connect the FIO node in SCSP3/SCSP2/SCSP1/SCSV1, or connect the N-IO node by using optical ESB bus in SCSP3, set the ESB bus coupler module (SEC402/SEC401) in slot number 7 of node number 1. To connect the FIO node in SCSL2, set the ESB bus coupler module (L1EC402/L1EC401) in slot number 7 of node number 1. Because a redundant configuration is configured by two ESB bus coupler modules, an I/O module cannot be set in slot number 8.

To connect the N-IO node by using N-ESB bus in SCSP3, set the N-ESB bus coupler module (S2EN402/S2EN404) in an odd slot number of node number 1. Because a redundant configuration is configured by two N-ESB bus coupler modules, an I/O module cannot be set in the adjacent slot number (odd slot number + 1).

● Is Redundant (switching between redundant and single Input/Output module configurations)

You can specify whether or not to make the I/O module redundant. You need to specify TRUE for redundant configuration and FALSE for single configuration. Redundancy can be specified only for I/O modules that are set in odd slot numbers. Note that the adjacent slot number (the odd slot number + 1) must be left unspecified as it is used by the other I/O module in the redundant configuration.

IMPORTANT

- Start I/O Parameter Builder and check that redundant and single configurations are set correctly for the input/output module and then save the definitions. When switching between redundant and single configurations, the change is reflected in the SCS after performing offline download or online change download.
- Set the mounting positions in accordance with node numbers, unit numbers, slot numbers, and redundancy specifications so that they do not overlap. Overlaps of mounting position cause errors when building SCS projects.

■ Wiring of channels and input/output variables

Wiring is an operation where channels are associated with input/output variables. Assign one input variable or output variable to one channel.

IMPORTANT

Make sure to use input/output variables in order to access channel data from the application logic.

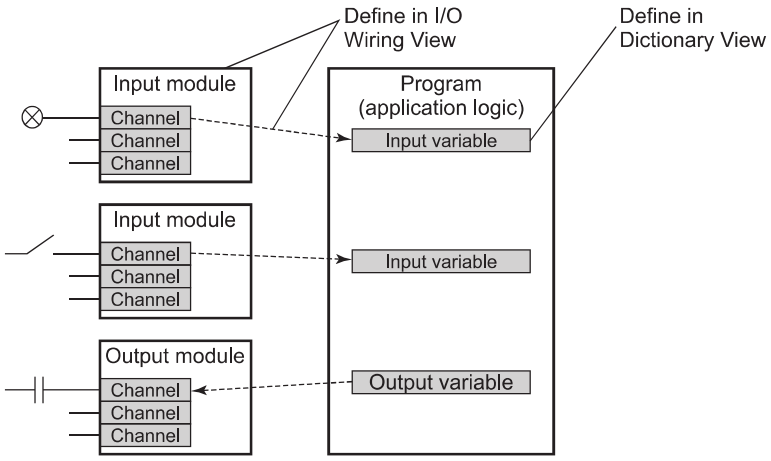


Figure Appendix 2.2.1-4 Wiring of channels and input/output variables

When you select a channel in I/O wiring tree view, a list of I/O variables that can be wired to the channel is displayed in I/O wiring grid view. Double-click the I/O variable for which you want to set the wiring, and set the wiring of channels. To assign the AO channel to S2MMM843, do not specify more than eight channels in a module.

The result of wiring is displayed in I/O Wiring Tree View. It is also displayed in the parameter setting view of each channel in I/O Parameter Builder and Dictionary View.

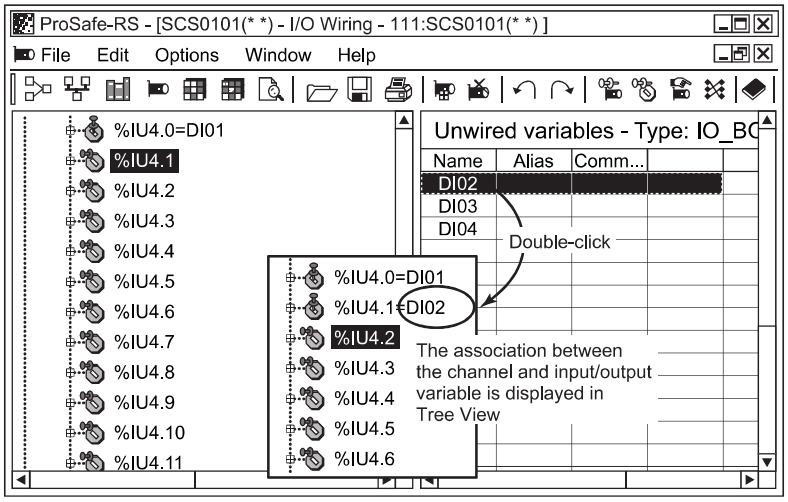


Figure Appendix 2.2.1-5 Example of wiring between a channel and input/output variable

TIP Deletion of wiring is also performed in I/O Wiring View.

In the AIO/DIO module of FIO, the signal category of the channel is determined based on the module that is used.

In the universal type I/O module, if you wire the channel and the I/O variable, the signal category of the channel is determined. If the signal category changes after re-wiring, all setting items will be initialized. If the signal category does not change even after re-wiring, the earlier setting items are retained.

Relationship between the channel and I/O variable is as follows.

Table Appendix 2.2.1-5 Relationship between the channel and I/O variable

Signal category of the channel	Type of input/output variable	Signal type (For universal type I/O modules)
AI	Type: IO_REAL Direction: Input Attribute: Read	Current input Current input (HART communication)
AO	Type: IO_REAL Direction: Output Attribute: Write or Free	Current output Current output (HART communication)
DI	Type: IO_BOOL Direction: Input Attribute: Read	Status input
DO	Type: IO_BOOL Direction: Output Attribute: Write or Free	Status output 1.3 A status output (*1) 2.0A status output (*1)

*1: You cannot select the modules mounted on the base plate for barrier.

Settings prohibited in I/O Wiring View

The following settings are not allowed in I/O Wiring View. Even if you make these settings, the operations of an SCS do not change.

- Channel filtering
  Filtering should be set as a channel parameter using I/O Parameter Builder.
- Channel mapping
  The functions provided in the Channels Map dialog box cannot be used. Even if you specify the mapping in I/O Wiring View, the setting is ignored in the SCS.
- Virtual device
  It is not allowed to switch to virtual device. If you specify a device as a virtual device in I/O Wiring View, an error occurs at building.

Appendix 2.2.2 I/O Parameter Builder

I/O Parameter Builder is used to specify parameters for input/output modules defined in I/O Wiring View.

Make the following settings in I/O Parameter Builder.

- Node parameters
- Input/output module parameters
- Channel parameters

IMPORTANT

When editing settings in I/O Parameter Builder, close I/O Wiring View first.

How to display I/O Parameter Builder

1. Select the [Engineering] launcher from the [Tools] menu of SCS Manager.
   The Engineering launcher menu appears.
2. In the Engineering launcher menu, select [I/O Parameter Builder].
   I/O Parameter Builder appears.

I/O Parameter Builder window structure

In I/O Parameter Builder, you need to set parameters for nodes or I/O modules that are selected on the I/O structure display panel. The tab sheet configuration of the workspace changes depending on the I/O module model.

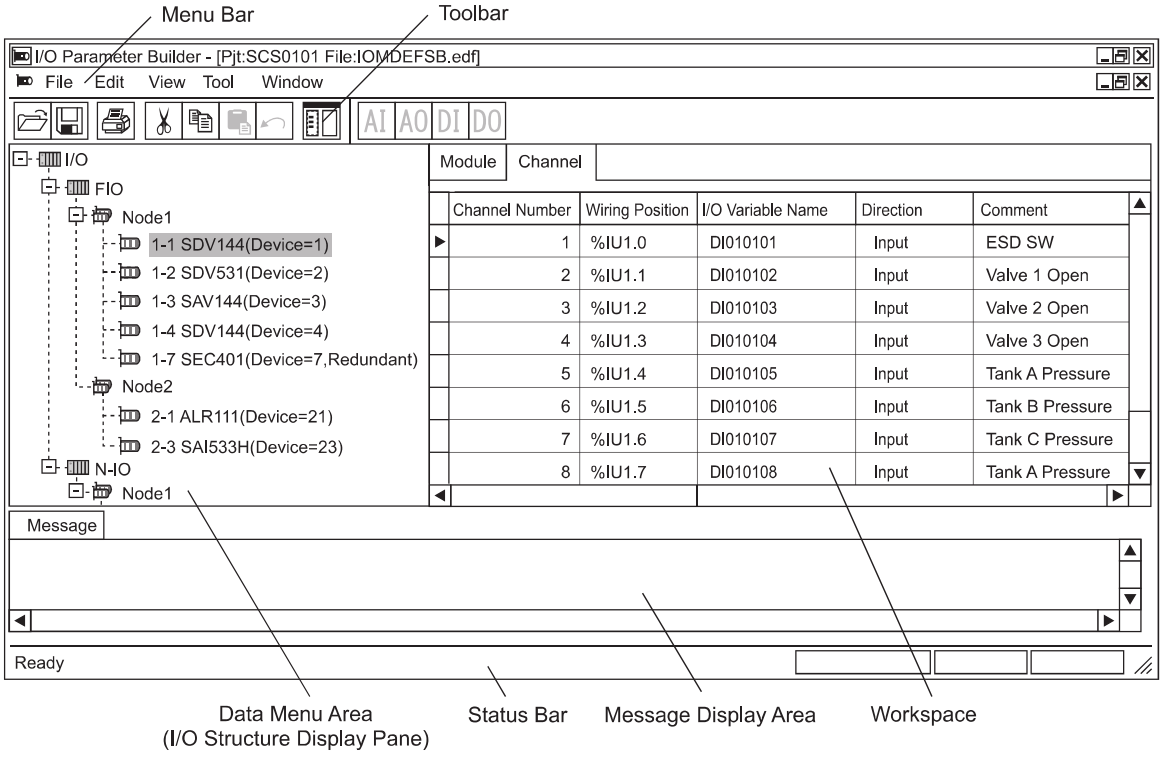


Figure Appendix 2.2.2-1 I/O Parameter Builder

Display channel switching commands in layer (indicating CPU nodes in the View menu on the menu bar)

In I/O Parameter Builder, the following menu items are displayed on the View menu of the menu bar. This is enabled only when the channel tab is selected on the workspace after selecting the universal type I/O module on the I/O structure display panel.

Table Appendix 2.2.2-1 Display channel switching commands in the View menu

Menu item	Description
AI Setting Items	Displays AI channels
AO Setting Items	Displays AO channels
DI Setting Items	Displays DI channels
DO Setting Items	Displays DO channels

AI/AO/DI/DO buttons on the toolbar

In I/O Parameter Builder, the following buttons appear on the toolbar. This is enabled only when the channel tab is selected on the workspace after selecting the universal type I/O module on the I/O structure display panel.

Table Appendix 2.2.2-2 AI/AO/DI/DO buttons on the toolbar

Button	Assigned function
AI	Same as AI Setting items of the View menu
AO	Same as AO Setting items of the View menu
DI	Same as DI Setting items of the View menu
DO	Same as DO Setting items of the View menu

Data Menu Area (I/O Structure Display panel)

The I/O structure display panel displays the I/O structure specified in I/O Wiring View. Select one target (node or input/output module) for which you want to specify a parameter from this panel. Once you select the target, the corresponding tab appears in the workspace.

The hierarchical structure of the I/O structure display panel is shown below.

Table Appendix 2.2.2-3 Hierarchy of the I/O Structure Display Panel

Layer	Description
I/O	Displayed as the top layer under which all inputs and outputs are arranged.
Type	Layer indicating types of nodes and I/O modules. FIO and N-IO are displayed. They are displayed only in SCSP3.
Node	Layer indicating the CPU node, safety node units, and N-IO nodes. Node numbers are displayed.
Module	Layer indicating I/O modules. Mounting position, I/O module models, device index, and classification of redundant and single configurations are displayed.

Workspace

In the workspace, items that can be specified for the node or I/O module selected on the I/O structure display panel are classified into separate tabs and displayed.

Table Appendix 2.2.2-4 Items displayed in the workspace

Setting target	Types of the tabs displayed	Description
Node	Node tab	Parameter setting for the node
Analog input module	Module tab	Setting of module parameters for the analog input module
	Channel tab	Setting of channel parameters for the analog input module
Analog output module	Module tab	Setting of module parameters for the analog output module
	Channel tab	Setting of channel parameters for the analog output module
Digital input module	Module tab	Setting of module parameters for the digital input module
	Channel tab	Setting of channel parameters for the digital input module
Digital output module	Module tab	Setting of module parameters for the digital output module
	Channel tab	Setting of channel parameters for the digital output module
Universal type I/O module	Module tab	Setting of module parameters for the universal type I/O modules
	Channel tab	Setting of channel parameters for the universal type I/O modules
Serial communication modules	Module tab	Settings for common parameters of serial communication modules
	Port1 tab	Settings for parameters of Port 1 of serial communication modules
	Port2 tab	Settings for parameters of Port 2 of serial communication modules
Ethernet communication module	Module tab	Settings for parameters of the Ethernet communication module
Fire and gas communication modules	Module tab	Display of parameters for fire and gas communication modules. The content set with Safety Communication I/O Editor is shown. You cannot configure the settings.

TIP

No information is displayed in the workspace even if SEC402/SEC401, L1EC402/L1EC401, or S2EN402/S2EN404 is selected on the I/O structure display panel.

Appendix 3. Precautions related to main specification additions and modifications

This section describes about the cautions and overview of important items for engineering and maintaining of specification changes and additions that were implemented in the past.

In the SCS, the operation differs with the release number. The operation is determined by the following conditions:

- The release number of the SENG software where SCS projects are newly created
- The release number of the SCS system program that is downloaded to the SCS. The SCS system program can be changed by offline downloading to the SCS.

The release number of the SENG software, where SCS projects are newly created, can be found in the SCS Project Properties dialog box. The release number of the SCS system program that is downloaded to the SCS can be found in the SCS State Management window.

Appendix 3.1 The major changes in R1

The following table shows the important contents as a compatibility information after the specification changes and additions have been implemented in R1.

Table Appendix 3.1-1 The important specification changes in R1

Release number	Revised content
R1.02	After R1.02, Variable DB is downloaded to the SCS via online change download only when variable definitions are modified. Therefore, the time and CRC of Variable DB in the work database are reflected to the master database and SCS only when variable definitions are modified.
R1.03	The item Originally Created in SCS Project Properties does not display the revision number of project data that is created by SENG with a software version prior to R1.03.
R1.03	The SCS Constants Builder displays PV Status of S_ANLG_S in SCS projects that are newly created with a software version R1.03 or later. The setting is configured to No in SCS projects that are created with a software version prior to R1.03 or earlier. The setting is configured to Yes if this SCS project is imported to the software with a version R1.03 or later.

Appendix 3.2 The major changes in R2

This section describes the important contents as a compatibility information after the specification changes and additions have been implemented in R2.

List of the important specification changes in R2

The following table shows the important contents as a compatibility information after the specification changes and additions have been implemented in R2. Detailed description is provided in the separate section, as necessary.

Table Appendix 3.2-1 The important specification changes in R2

Release number	Revised content
R2.01	Security models can be selected with the IT Security Configuration Tool.
R2.01	In the case of SCS with system program R2.01 or earlier, the operation of AIO/DIO modules stops when changes are made to I/O parameters that require IOM download. When you perform online change download after modifying such parameter settings, the output may become 0 depending on the changes made. In order to avoid shutdown in case when output is 0, measures are required at field side.
R2.02	In the case of SCS with system program R2.02 or later, the operation of AIO/DIO modules continues even if changes are made to I/O parameters that require IOM download.
R2.02	In SCS with system program before R2.02, the operation of CASE statement of ST was incorrect. When using SCS projects that are newly created by SENG before R2.02, there are precautions on when you first perform online change download after upgrading SENG.
R2.02	The checking operation in Integrity Analyzer has been changed. When using SCS projects that are newly created by SENG before R2.02, there are precautions on when you first use Integrity Analyzer after upgrading SENG.
R2.02	The self document operation has been changed. Engineering can be performed for compatibility with versions before R2.02.
R2.03	In the SCS with SCS system program R2.03 or later, the measured value for scan cycle is displayed in the SCS State Management window and SCS State Display View of CENTUM HIS. For SCS with system program R2.02 or earlier, the set scan period is displayed.
R2.03	In SCS with SCS system program R2.03 or later, the scan period for application logic execution function can be modified by online change download.
R2.03	In SCS with SCS system program R2.03 or later, the addition and deletion of I/O modules can be performed by online change download. Other items that can be modified by online change download have also been added.
R2.03	In the SCS with SCS system program R2.03 or later, you can execute automatic IOM download.
R2.03	In the SCS with SCS system program R2.03 or later, you can use the automatic scan period extension function. When using this function, use SYS_SCANEXT FB to notify the state that the scan period is extended by using the automatic scan period extension function. If the SCS projects are created by SENG R2.03 or later, you can define SYS_SCANEXT.
R2.03	In the SCS with SCS system program R2.03 or later, you can specify the SCS behavior at abnormal calculation. When using this function, use SYS_CERR FB to notify the occurrence of abnormal calculation and detect that the SCS is continuing the operation even if the abnormalities have occurred in calculation. If the SCS projects are created in SENG R2.03 or later, you can define SYS_CERR.
R2.03	With R2.03 or later, the system checks to see if there is possibility that the online change variables area in the database has been used before executing the offline download.
R2.03.59	The behaviors of inter-SCS safety communication have been changed. R2.03.59 is the official version of operations modified at R2.03.51.

Notes on online change download after upgrading SENG

In R2.02, the problem that the FB for which you have specified a minus value for a label in a CASE statement does not run properly (*1) has been fixed. Because of this, the behavior of online change downloading after you have upgraded the SENG to R2.02 will be as follows.

After you have upgraded the SENG to R2.02, if you perform a build for a project created in a version before R2.02 and execute online change downloading, all the FBs containing any CASE statement in the ST language will be downloaded (*2) even if no changes have been made to the logic. Once you rebuild a project of a version earlier than R2.02 on a R2.02 system and execute online change downloading, FBs with no logic change will not be downloaded in the subsequent online change downloading.

You can use the Database Validity Check Tool, as necessary, to find out which FBs will be downloaded before you execute online change downloading.

In a revision before R2.02, FBs containing any CASE statement in which a minus value is specified for a label do not run correctly, so they can be spotted and removed in the system test. Therefore, no such FBs should exist in a project. However, if such FBs do exist, the FBs may start to run normally after downloading.

To avoid such unexpected change in behavior, you should check the project to see if there are any FBs containing a CASE statement in which a minus value is specified for a label.

- If any FBs using a minus value for a label of CASE statement are found, make sure that the change in behavior does not cause any adverse effects on the system. (*3)(*4)
- If FBs using a minus value for a label of CASE statement are not found, all the FBs using CASE statements will be downloaded but the system behavior remains the same; so you do not need to perform tests again.

*1: If you specify a minus value for a label in a CASE statement in ST, an incorrect database which causes unexpected behavior may be generated. In the following example, if variable1 is neither “1” nor “2”, “3” is always assigned to aaa.

```
CASE variable1 OF
1: aaa := 1;
2: aaa := 2;
-1: aaa := 3; (* When the variable1 is neither 1 nor 2, this line is always executed.*)
-2: aaa := 4;
ELSE aaa := 5;
END_CASE;
```

*2: In this case, Cross Reference Analyzer does not detect the difference of the FBs using CASE statements.
*3: In this case, Cross Reference Analyzer does not detect the difference of the FBs using a minus value for a label of CASE statement.
*4: To find the locations where CASE statements are used, open multiple STs in Multi-Language Editor and search for “CASE”.

Behavior of AIO/DIO modules at online change download

If you perform online change download after using I/O Parameter Builder to modify setting items that require IOM download, AIO/DIO modules continue to operate in SCS system program R2.02 or later. However, it stops operation with versions earlier than R2.02.

IMPORTANT

If AIO/DIO module stops operation, a message appears notifying the possible occurrence of IOM Fail before starting the online download.

You can confirm the system program release number of SCS in the SCS State Management Window of the SCS maintenance support tool.

This section explains the behaviors of AIO/DIO modules when the SCS system program revision is earlier than R2.02.

Behavior of Input modules

- At the time of online change, the data status of all channels of the target module become BAD, and the diagnostic information message “IOM Fail” appears. The input signals of all channels of the module are processed according to the [Input Processing at Fault] settings.
- If on-demand HART communication with PRM is performed, the HART communication is discontinued during the “IOM Fail” status.
- On completion of online change download, the channels’ data automatically return to the values input to the channels and all data statuses become GOOD.
- A diagnostic information message indicating that the input module has recovered to normal is output.
- For dual-redundantly configured I/O modules, the odd-numbered module takes the control right.

TIP

If any setting items that require IOM download and the setting of [Input Processing at Fault] or [Input Value at Fault] are changed online simultaneously, the input value will conform to the changed settings of [Input Processing at Fault] and [Input Value at Fault].

Behavior of Output modules

- At the time of online change, the data status of all channels of the target module become BAD, and the diagnostic information message “IOM Fail” appears. The output values on all channels change to 0 if the target module is a digital output module, and change to the tight-shut output values (*1)if the target module is an analog output module.
- If on-demand HART communication with PRM is performed, the HART communication is discontinued during the “IOM Fail” status.
- On completion of online change download, the data status of all channels become GOOD, while the output values still remain 0 with a digital output module or tight-shut output values with an analog output module.
- A diagnostic information message indicating that the output module has recovered to normal is output.
- For dual-redundantly configured output modules, the odd-numbered module takes the control right.
- If the user performs the output enable operation, outputs of the application logic are output from the output module.

*1: A tight-shut output value can be set for each channel using the I/O Parameter Builder.

Possibilities of online change download

The online change downloadable information for the SCS with a system program before R2.03 is as follows:

POU information that is changeable online

There are changes that enables you to execute online change download or offline download according to each POU type.

Table Appendix 3.2-2 POU information

Modification	Online Change (*1)		
	Program	User-Defined FB	User-Defined FU
Adding/deleting variables	Yes	Yes (*2)	Yes (*3)
Adding a variable to be named the same as that of a deleted variable	No	No	No
Changing attributes of variables	No	No	No
Adding/deleting I/O variables	Yes	-	-
Adding/deleting FU	Yes	Yes	Yes
Adding/deleting user-defined FU (*4)	Yes	Yes	Yes
Adding/deleting FB instances	Yes	No	-
Adding/deleting the user-defined FB instances (*4)	Yes	No	-
Adding a FB to be named the same Instance as that of a deleted FB	No	-	-
Changing logic	Yes	Yes (*2)	Yes (*2)
Creating/deleting programs Changing program names	No (*5)		
Creating/deleting user-defined Function Blocks Changing user-defined Function Block names	No (*5)		
Creating/deleting user-defined Functions Changing user-defined Function names	No (*5)		

*1: Yes: Changeable by online change download.
No: Offline download is required.
*2: It is not allowed to increase/decrease parameter values or change attributes. They cause an error when the database is downloaded.
*3: An error occurs during downloading.
*4: When user-defined FU/FB are added, they need to be tested. Pre-validated user-defined FU/FB do not need to be tested.
*5: Online change is only possible for local variables.

I/O module information that is changeable online

The following table shows whether each item of I/O module related information can be changed by online change downloading.

Table Appendix 3.2-3 I/O module information

Modification	Online Change (*1)
Adding nodes	No
Deleting nodes	No
Changing parameters of nodes	Yes
Adding I/O modules	No
Deleting I/O modules	No
Changing redundant I/O modules	No
Changing parameters of I/O modules	Yes
Changing parameters of channels	Yes
Changing subsystem communication definitions	Yes
Defining link between a variable and an idle channel	Yes
Deleting link between a channel and a variable	Yes
Changing link between a channel and a variable	Yes

Continues on the next page

Table Appendix 3.2-3 I/O module information (Table continued)

Modification	Online Change (*1)
Adding, changing or deleting subsystem communication definitions	Yes
Changing wiring of communication input/output FBs	Yes

*1: Yes: Changeable by online change download.
No: Offline download is required.

Constants and network information that are changeable online

The following table shows whether the setting can be changed by online change downloading in the constant and network related items.

Table Appendix 3.2-4 Constants and Network

Classification	Modification	Online Change (*1)
Configuration	Name	No
	Password	No (*2)
Resource	Name	No
	Resource Number	No
	Scan period	No
	Number of variables permitted for online	No
	Size of temporary variables and constants area	No
Network	IP address	No
	Station address	No
	Inter-SCS safety Communication (Binding)	No
Optional ESB BUS Repeater	Optional ESB BUS Repeater	No
	Max. extension distance	No

*1: No: Offline download is required.
*2: Setting and changing passwords is ignored.

Builder definitions that are changeable online

The following table shows whether online change downloading is possible after you have changed definitions using builders.

Table Appendix 3.2-5 Online change download

Builders	Online Change (*1)
SCS Constants Builder	No
I/O Parameter Builder	Yes
Communication I/O Builder	Yes
SCS Link Transmission Builder	Yes
Modbus Address Builder	Yes
Tag Name Builder	Yes
Alarm Priority Builder	No
Alarm Processing Table Builder	No

*1: Yes: Changeable by online change download.
No: Offline download is required.

Behaviors at abnormal calculation in application logic

If abnormal calculation occurs in the application logic of an SCS with a system program before R2.03, the SCS stops.

About behaviors of SCS at abnormal calculation

- If an overflow or division by zero occurs in operations with REAL-type variables, or division by zero in operations with integer-type variables, SCS stops.
- When floating-point data is converted to a DINT number by the ANY_TO_DINT function, if the resultant number exceeds the maximum or falls below the minimum integer values (i.e. overflow occurs), the SCS stops.
- For the input to ANY_TO_TIME, use a DINT type value in the range from 0 to 86400000. If a value beyond this range is used, it cannot return a proper time. Note that when a real number value greater than 4294967295 (the maximum number of the unsigned 32-bit integer) or smaller than -2147483648 (the minimum number of the unsigned 32-bit integer) is used, the SCS stops.
- If access to the outside of an array occurs, the SCS stops.

Enhanced checking by Integrity Analyzer

Checking for multiple writing to the same variable

Multiple writing to the same variable can reduce the program readability and end up downloading of programs that cause unintended behavior. Integrity Analyzer in R2.02 detects multiple writing to the same variable and displays a warning message.

This warning message is not output with the revisions before R2.02, but it will be displayed after you have upgraded to R2.02 when the program contains any multiple writing to the same variable. If this warning message is displayed, examine the program to find out if you can eliminate the multiple writing.

If you find that the multiple writing is necessary, acknowledge the results of analysis in Integrity Analyzer and you can download the program to SCS without change. In this case, the program can be used as a function allowed for safety application after verifying its validity in user tests.

Checking for multiple calls to the same FB instance

Multiple calls to the same function block (FB) instance can lead to an unexpected state in the system and the program may not behave as intended. Integrity Analyzer in R2.02 detects multiple calls to the same FB instance and displays a warning message.

This warning message is not output with the revisions before R2.02, but it will be displayed after you have upgraded to R2.02 when the program contains multiple calls to the same FB instance. If this warning message is displayed, examine the program to find out if you can eliminate the multiple calls. If you find that the multiple calls are necessary, acknowledge the results of analysis in Integrity Analyzer and you can download the program to SCS without change. In this case, the program can be used as a function allowed for safety application after verifying its validity in user tests.

Checking for writing to output variable status

I/O variable statuses (.status) are the data that reflect the actual statuses (normal/abnormal) of I/O channels. Therefore, they should not be changed by user logic. Integrity Analyzer in R2.02 detects writing to output variable statuses and raises an error.

In revisions before R2.02, no such error is raised. But this error will be raised after you have upgraded to R2.02 when there is any program that writes to any output variable status. If an

error message is displayed, change the program to eliminate the writing to output variable statuses.

Specification changes made in SCS system program (Release number R2.03.51)

Overview of specification changes

After the SCS system program release number R2.03.51, information on system time is no longer used to diagnose delay in inter-SCS safety communication and SCS link transmission safety communication. Specifically, there is no need to consider the gap in the system times of related SCSs when determining the DLYT value.

IMPORTANT

In order to operate inter-SCS safety communication and SCS link transmission safety communication with the specification of R2.03.51 or later, upgrade the revision of all SCS system programs that communicate each other to R2.03.51 or later. If either the revision of the transmission or reception side has not been upgraded, the system operates with the method before the change, which uses the system time for diagnosis of delay. If the communication is performed with the method before the change, take the gap in the system times among involved SCSs as the DLYT value as in the past.

Calculation method of DLYT in Inter- SCS safety communication

How to calculate DLYT in inter-SCS safety communication in case of revisions earlier than R2.03.51 is explained below.

Reception interval timeout value (OUTT) and inter-FB transmission delay timeout value (DLYT) are used to set the timeout monitoring time of inter-SCS safety communication.

Temporary transmission delay errors can be detected by monitoring the communication with OUTT. In addition, you can set DLYT to detect constant transmission delay errors.

DLYT detects not only transmission delay but also time gap among SCSs. For this reason, determine the set value of DLYT taking generation of erroneous trips due to time gap into consideration as well.

- Reception interval timeout value (OUTT)
  An FB for communication on the consumer side (CONS_*) checks the interval of data reception. If the data reception interval exceeds the reception interval timeout value (OUTT), a communication error occurs and a failsafe value (VAL) is output.
- Transmission delay timeout value (DLYT)
  DLYT checks the time from the time an FB for communication on the producer side (PROD_*) transmits data to the time an FB for communication on the consumer side (CONS_*) receives the data. This time interval is called inter-FB transmission delay time. If the status where this interval exceeds the inter-FB transmission delay timeout value (DLYT) of CONS_* continues for the time indicated by OUTT, a communication error occurs and a failsafe value (VAL) is output.

The guidelines of timeout value settings are given in the following.

- Setting of Reception Interval Timeout Value (OUTT)

  OUTT=(select the longer scan period of either the producer or the consumer) x 8 + (Additional Delay)

  Additional Delay

  V net Delay

  No BCV/CGW used: 0 s
  Via BCV/CGW: the number of BCV used x 1 s +
  the number of pairs of CGWs used x 2 s

  Vnet/IP Delay

  Within a Vnet/IP domain: 0 s

  Between Vnet/IP domains (No wide area network):
  0 s (Regardless of the number of L3SWes)

  Between Vnet/IP domains (Wide area network):
  1 s (Regardless of the number of L3SWes)

  Vnet/IP – V net: V net delay + Vnet/IP delay + V net router delay (1 s)

  V net(1) –Vnet/IP –V net(2): V net(1) delay +Vnet/IP delay + V net(2) delay +
  Two V net routers' delay (2 s)

  Set 3 seconds to OUTT when the calculated OUTT is shorter than 3 seconds.

- Setting of the Transmission Delay Timeout Value (DLYT)

  1. In cases of Inter-SCS safety communications between:
     - SCSs in the same domain
     - SCSs synchronized with GPS time
     - SCSPs synchronized with a Vnet/IP network time
     - An SCSP synchronized with SNTP server and an SCSV synchronized with GPS time:

     DLYT= (scan period of the producer) + (scan period of the consumer) + (Additional Delay)
     Additional Delay

     V net Delay

     No BCV/CGW used: 300 ms
     Via BCV/CGW: the number of BCV used x 1.3 s +
     the number of pairs of CGWs used x 2.3 s

     Vnet/IP Delay
     Within a Vnet/IP domain: 300 ms
     Between Vnet/IP domains (No wide area network):
     300 ms (Regardless of the number of L3SWes)
     Between Vnet/IP domains (Wide area network):
     1.3 s (Regardless of the number of L3SWes)
     Vnet/IP – V net: V net delay + Vnet/IP delay + V net router delay (1.3 s)
     V net(1) – Vnet/IP – V net(2): V net(1) delay + Vnet/IP delay + V net(2) delay +
     Two V net routers' delay (2.6 s)

     Set 3 seconds to DLYT when the calculated DLYT is shorter than 3 seconds.

  2. In case of Inter-SCS safety communications between SCSs synchronized with V net time in SCS in different domains:
     DLYT= (the number of BCV used) x 5 s

  3. If there are V net routers between SCSs synchronized with V net time in the Inter-SCS safety communications,
     DLYT= (BCV/number of V net router layers) x 5 s

IMPORTANT

If you set 0 seconds to DLYT and bypass inter-FB transmission check, it is not possible to use reception data of the given inter-SCS safety communication for the safety purpose.

- In both cases, set the value of OUTT as the DLYT value if OUTT is smaller than DLYT.
- The timeout value is used for calculating system reaction time.

Precautions when setting DLYT for Inter- SCS safety communication

Precautions to be followed when setting DLYT for inter-SCS safety communication in software versions R2.03.51 or earlier are given below.

- If IRIG-B time synchronization method is selected, be sure to take the time gap due to failure of GPS and IRIG-B interface into consideration.
- In the case of SCSs connected to Vnet/IP, time gap due to the SNTP server must be taken into consideration.
- Unify the time synchronization method among SCSs that perform inter- SCS safety communication and determine the setting value such that erroneous trips do not occur due to time gap among SCSs.

  If you set DLYT among SCSs over multiple domains, the following points must also be taken into consideration.
- If V net time synchronization method is selected, delay of up to 5 seconds in the first level of BCV-V and 10 seconds in the second level may occur. It is recommended to select IRIG-B time synchronization if it is found that the gap is outside the allowable range.
- If domains are connected via a gateway for broadband connection, it is recommended to synchronize V net time of each domain within the allowable range or select IRIG-B time synchronization.

Precautions when setting DLYT for SCS link transmission safety communication

How to calculate DLYT of SCS link transmission safety communication for revisions R2.03.51 or earlier is explained below.

Reception interval timeout value (reception timeout, hereinafter referred to as OUTT) and inter-SCS transmission delay timeout value (transmission timeout, hereinafter refer red to as DLYT) are used to set the timeout monitoring time of SCS link transmission safety communication.

Temporary transmission delay errors can be detected by monitoring the communication with OUTT. In addition, you can set DLYT to detect constant transmission delay errors.

DLYT detects not only transmission delay but also time gap among SCSs. For this reason, determine the set value of DLYT taking generation of erroneous trips due to time gap into consideration as well.

- Reception interval timeout value (OUTT)
  It is valid only when the station on the transmission side is an SCS.

  The reception interval refers to the time interval of receiving data by an SCS. Specify the reception interval timeout value (OUTT) for each communication target. If normal data cannot be received within the reception interval timeout value (OUTT), a communication error occurs and a failsafe value is output.
- Inter-SCS transmission delay timeout value (DLYT)
  It is valid only when the station on the transmission side is an SCS.

Inter-SCS transmission delay time is the time duration from the time an SCS on the transmission side sends data to the time an SCS on the reception side receives the data. If the inter-SCS transmission delay timeout value exceeds the DLYT timeout value and the status continue for the time specified by OUTT or longer, a communication error occurs and a failsafe value is output.

The guidelines of timeout value settings are given in the following.

- Setting of reception interval timeout value (OUTT)
  OUTT = (Scan frequency on the transmission or reception side, whichever longer) X~ 8

  If OUTT is 3 seconds or less, set 3 seconds.

- Guidelines of setting value of transmission delay timeout value (DLYT)
  If the time synchronization method employed is V net time synchronization or Vnet/IP time synchronization, set 3 seconds for DLYT.

  In the case of IRIG-B time synchronization, determine DLYT as follows:

  DLYT = (Scan frequency on transmission side) + (Scan frequency on the reception side) + (Delay addition) + (Time gap addition)

  Delay addition: 100 ms

  Time gap addition: Determine the setting value so that erroneous trips do not occur due to time gap.

  If DLYT is 3 seconds or less, set 3 seconds.

  If 0 seconds are set for DLYT, checking of transmission delay by DLYT is bypassed.

Appendix 3.3 The major changes in R3

This section describes the important contents as a compatibility information after the specification changes and additions have been implemented in R3. Detailed description is provided, as necessary.

List of the important specification changes in R3

The following table shows the important contents as a compatibility information after the specification changes and additions have been implemented in R3. Detailed description is provided in the separate section, as necessary.

Table Appendix 3.3-1 The important specification changes in R3

Release number	Revised content
R3.01	The specifications for the operation of the ANLG1OO2D, ANLGVOTER, ANLG_S, ANLGI, and VEL functions blocks have been modified.
R3.02	In the SCS with SCS system program R3.02 or later, you can use the IOM reset function. To use the IOM reset function, execute IOM download from the IOM download tool.
R3.02	IT security is strengthened in SOE OPC server R3.02 or later.
R3.02	When using ALE111 in order to perform Modbus slave communication via Modbus TCP protocol, you must use the style S1 module with unit revision U:2 or later.
R3.02	For SCS projects created by SENG before R3.02.00, the POU related online change download may be enabled when Clean project is performed.
R3.02.10	In SCS Constants Builder, the definition item name Writing to a Single Holding Register has been changed to 16-bit Modbus master support mode.

Function Block parameters

The function block operation specifications have been changed in the SCS system program release number R3.01.

Support for Analog Input modules for Thermocouple/RTD

In revisions earlier than R3.01, the following function blocks were able to handle normalization data from 0 to 100% only with their parameters.

Table Appendix 3.3-2 Function Blocks whose parameters were changed in R3.01

Function block	Parameter
ANLG1OO2D	IN1, IN2, DEL, VAL, OUT
ANLGVOTER	IN1, IN2, IN3, DEL, VAL, OUT
ANLG_S	IN, HYS
ANLGI	IN, HYS
VEL	IN, VL, HYS

ANLG1OO2D

Due to the specification changes of ANLG1OO2D parameters, the operations of VAL on SCS are changed as shown in the following table.

Table Appendix 3.3-3 Specification of VAL

Earlier than R3.01	R3.01 or later
-25 to 125%. If you specify a value smaller than -25.0%, it is processed as -25.0%. If you specify a value greater than 125%, it is processed as 125 %.	Specify as % or engineering units. (No restrictions on range in VAL.)

ANLGVOTER

Due to the specification changes of ANLGVOTER parameters, the operations of VAL on SCS are changed as shown in the following table.

Table Appendix 3.3-4 Specification of VAL

Earlier than R3.01	R3.01 or later
-25 to 125%. If you specify a value smaller than -25.0%, it is processed as -25.0%. If you specify a value greater than 125%, it is processed as 125 %.	Specify as % or engineering units. (No restrictions on range in VAL.)

Specification of SCS constant "Writing to a Single Holding Register" has been changed in R3.02.10

"Writing to a Single Holding Register" is a setting item of SCS Constants Builder that was added in R3.02.00. In R3.02.10, the specification of this setting item has been changed as follows:

- The item name has been changed from "Writing to a Single Holding Register" to "16-bit Modbus master support mode".
- When "16-bit Modbus master support mode" is set to Disable, there is no difference in the behavior between R3.02.00 and R3.02.10.
- The following table describes the behaviors when the SCS system program release number is R3.02.00 and when the SCS system program release number is R3.02.10 with "16-bit Modbus master support mode" set to Enable. There is no difference in writing to a Preset Single Register between R3.02.00 and R3.02.10.

Table Appendix 3.3-5 SCS system program release number and the behavior when "16-bit Modbus master support mode" is set to "Enable"

SCS system program release number	Behavior when "16-bit Modbus master support mode" is set to "Enable"
R3.02.00 (*1)	• Preset Single Register (function code 06) is available. • If a multiple-register read/write command (function code 03, 04, or 16) is used specifying an even number for the beginning reference number or an odd number for the size of data, the error code 10 or 11 (hex.) is returned.
R3.02.10	• Preset Single Register (function code 06) is available. • Data access is possible by using multiple-register read/write commands (function codes 03, 04, and 16) specifying an even number for the beginning reference number and/or an odd number for the size of data. Error code 10 or 11 (hex.) is not returned even if an even number is specified for the beginning reference number or an odd number is specified for the size of data.

*1: This means the case when the version of SENG is R3.02.00 and the case when SENG is upgraded to R3.02.10 but offline downloading to SCS is not yet performed.

Appendix 3.4 Major changes in R4

This section describes important contents as compatibility information after the specification changes and additions implemented for R4. Detailed descriptions are provided as necessary.

List of important specification changes in R4

The following table shows important contents as compatibility information after the specification changes and additions implemented for R4. Detailed descriptions are provided in separate sections as necessary.

Table Appendix 3.4-1 Important specification changes in R4

Release number	Revised content
R4.01	Engineering using AD Suite has been enabled.
R4.02	Engineering using iDefine when selecting I/O list engineering has been enabled.
R4.03.10	With SCS projects for which I/O list engineering has been selected, engineering for communication I/O has been modified to be implemented with Safety Communication I/O Editor instead of with Communication I/O Builder.
R4.05	The values available for the "SW" data item are changed to 0, 1, and 2 in each MOA, MOB_11, MOB_21 FB mapping block. As compatibility information, the previous specifications before the system is upgraded to R4.05 are described as follows: • The values available for the SW are 0 and 1. • The value of the FB's SW parameter is reflected as is to the data item SW.
R4.06	Settings to check-in and check-out automatically have been added to the Safety I/O Editor, etc., of AD Organizer.
	The specifications of the iDefine-config file has been changed. To engineer by using iDefine, upgrade the SCS project to the latest version and use it with the recommended version number of iDefine.
R4.07	The classification of POWE/LOGE functions has been changed. POWE/LOGE is a safety function for new SCS projects that are created in SENG in R4.07.00 or later. It can be used as an input to safety loops. It remains as an interference-free function for new SCS projects that are created in SENG in revisions earlier than R4.07.00. It cannot be used as an input to safety loops.
R4.08	The range of reference numbers of Modbus devices is expanded. The range of reference numbers of Modbus devices is expanded for new SCS projects that are created in SENG in R4.08.00 or later. The applicable SCSs are SCSP1/SCSU1/SCSP3/SCSL2. The range of reference numbers of Modbus devices is not expanded for new SCS projects that are created in SENG in revisions earlier than R4.08.00. As compatibility information, the specifications for revisions earlier than R4.08.00 are described. • Coil: 00001 to 01000 • Input relay: 10001 to 14000 • Input registers: 30001 to 34000 • Holding registers: 40001 to 41000
R4.09	The specifications of online change download of POU has changed. For SCS projects newly created with SENG R4.09.00 or later, online change download is available when newly creating, deleting, or renaming all program, user-defined function, and user-defined function block POUs. For SCS projects newly created with SENG earlier than R4.09.00, among all POUs, online change download is available for changes of program name only.
	ProSafe-RS R4.09 or later does not support iDefine. You can use iDefine if you use ProSafe-RS R4.02 to R4.08.
R4.10	The following diagnostic information notification system function blocks have been added: SYS_CPUDSP, SYS_NODEPSU, SYS_N_NODEPSU

Communication I/O List Output Tool

Communication I/O List Output Tool is a tool for creating a safety communication I/O list based on the information of %W included in an SCS project created upon selecting I/O list engineering with a version between R4.01 through R4.03.00. %W is defined as information on communication I/O definitions and communication I/O wiring by using Communication I/O Builder.

When this tool creates a safety communication I/O list, the information of Dictionary View and I/O Wiring View is referenced as well.

The following packages are required to run this tool:

- RS4E5100 safety system engineering and maintenance function
- RS4E5210 I/O list engineering package

Also note that this tool can only be used by users that belong to the PSF_MAINTENANCE group.

Using Communication I/O List Output Tool

In R4.03.10 or later, when performing communication I/O related engineering with an SCS project for which I/O list engineering has been selected, use Safety Communication I/O Editor started from AD Organizer. Communication I/O Builder will be used as read-only.

When you change the communication I/O-related engineering data of an SCS project that was created with a software version from R4.01 through R4.03.00, create a safety communication I/O list by using this tool and load it into Safety Communication I/O Editor.

IMPORTANT

When the engineering is performed by using iDefine, follow these steps after upgrading the software:

1. Create a safety communication I/O list by using this tool, and import it to an empty safety communication I/O list.
2. Among the data defined in the Client I/O table of iDefine, enter the data to be mapped to the user-defined columns of Safety Communication I/O Editor to the the user-defined columns of Safety Communication I/O Editor.
   If you import the ProSafe-RS I/O file to iDefine without performing this task, the corresponding data in the Client I/O table of iDefine will be lost.

   This is because, in the safety communication I/O list created with this tool, user-defined columns are empty.
3. Run Export to iDefine.
4. Import the ProSafe-RS I/O file to iDefine.

Creating a safety communication I/O list

A list cannot be created if the SCS project for which the safety communication I/O list is being created is in use. Close SCS Manager of the applicable SCS project.

1. Click `(ProSafe-RS installation folder)\YOKOGAWA\eng\Tool\RHECIOOutput4310.exe`. The following dialog box appears.

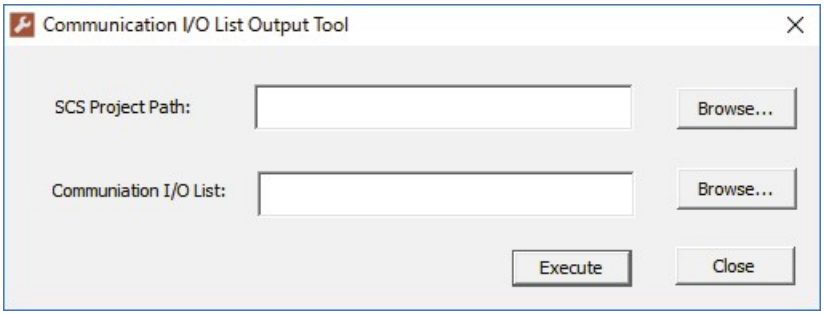


Figure Appendix 3.4-1 Communication I/O List Output Tool screen

2. In the text box for SCS Project Path, specify the path of the SCS project for which the safety communication I/O list is being created. You can also select the path of the SCS project by clicking [Browse].
3. In the text box for Communication I/O List, specify the file name of the safety communication I/O list in the xlsx format of Microsoft Excel. Specify the path where the safety communication I/O list is to be generated by clicking [Browse].
4. Click [Execute].
   The safety communication I/O list is generated in the specified folder.

● Format of data included in the safety communication I/O list

When the safety communication I/O list is generated, the SCS project name is added to the beginning of the P&ID Tag, Program Group, and Communication Group.

Example) If the SCS project name is SCS0101 and the Communication Group is C001, the Communication Group in the list becomes SCS0101_C001.

For this reason, the safety communication I/O lists of multiple SCS projects included in the same AD project can be loaded in order in Safety Communication I/O Editor of the same AD project.

■ Online change of POU information

The availability of online change download to SCS for an SCS project created with SENG earlier than R4.09.00 or when clean project is not executed for an SCS project earlier than R4.09.00 is as follows.

● Changing POU

The following table shows whether POU can be changed online: for operations on POU, online change download can be used for changes of Program name only. If you try to perform online download change on the item that No is described in the table, an error is notified at the time of online change download.

Table Appendix 3.4-2 Whether or not online change can be used for POU operations

Type of POU	Changing a name	Creating, deleting
Program	Yes	No
User-defined FU	No	No
User-defined FB	No	No

Since a new program can not be created online, we recommend that you create dummy programs in advance and change the name of the program online as you need.

Changing a library

When a library is added to or deleted from SCS project, offline download is needed. A warning is displayed at the build operation, and an error occurs at online change download operations.

A project that is created with the revision earlier than R3.02.00 will be in the same condition as R3.02.00 when clean project is executed. Therefore, you cannot perform online change download when the library is added or deleted.

Appendix 4. Maintenance of sales discontinued products

This section describes information that is essential for maintenance of "sales discontinued products".

Appendix 4.1 Time synchronization of SCSV1

SCSV1 is connected on V net. This section describes the specifications and precautions related to the time synchronization of SCSV1.

Time synchronization methods for SCSs connected to V net

There are the following two time synchronization methods, from which the user can select the more appropriate one for the given application.

Table Appendix 4.1-1 Time synchronization method

Method	Description	Setting method
Synchronization with V net time (standard)	Uses the mechanism for synchronizing time of each station connected to V net.	Select "V net" as the time synchronization method in SCS Constants Builder. (*1)
IRIG-B time synchronization (optional)	Uses the GPS unit as the standard time server. If this output (IRIG-B) is connected to each SCS, the standard time (date, hour, minute, second) and the synchronization timing are distributed. Each SCS is synchronized with this timing. Since GPS is used, it is possible to acquire events with high time accuracy.	Connect a commercially available GPS unit and a connector on the CPU node with IRIG-B. Select "IRIG-B" as the time synchronization method in SCS Constants Builder.

*1: The standard time is specified by the user using SCS Maintenance Support Tool of the SENG or the Adjust Time dialog box of an HIS.

Synchronization with V net time

When synchronization with V net time is applied, the user can set the time using SCS Maintenance Support Tool of the SENG or the Adjust Time dialog box of an HIS.

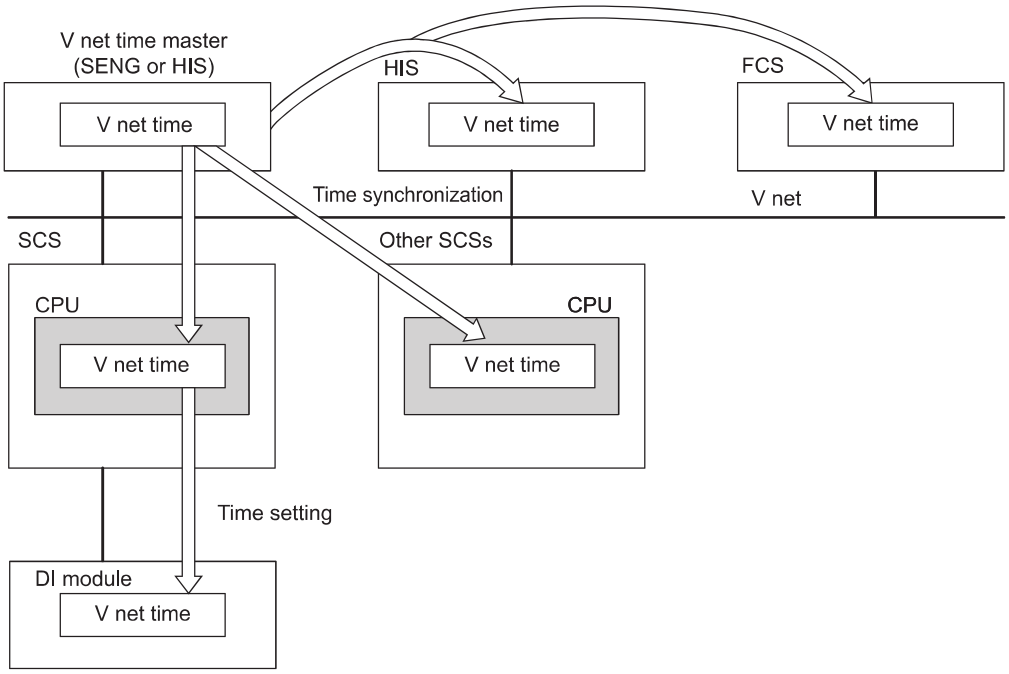


Figure Appendix 4.1-1 Synchronization with V net time

TIP

If the diagnostic information message, "GPS Interface Unit Error" is notified when synchronization with V net time, the CPU module need not be replaced if the following conditions are met. Since this message does not present any problem in practical operations or on safety, you can continue to operate the system.

- If the message is generated only on the control-side CPU module in the redundant configuration immediately after completion of APC:
  If the recovery message, "GPS Interface Unit Recover" is displayed for the control-side CPU module immediately thereafter, the module is not faulty.
- If the V net configuration is unstable:
  In a condition where the V net is not connected correctly, such as at startup, a bus configuration error may occur. In this case, the V net controller in CPU module cannot read time information and this message will be notified as a result. Reconnect the bus correctly and start the SCS. If the message no longer appears, the module is recovered.

IRIG-B time synchronization

In IRIG-B time synchronization, the time is acquired from the standard time receiver. The IRIG-B time is used for time stamps of events and alarms set in the CPU. This method produces more accurate timing for events among SCSs, compared to synchronization with V net time. The time of the CPU module and DI modules are synchronized to the IRIG-B time.

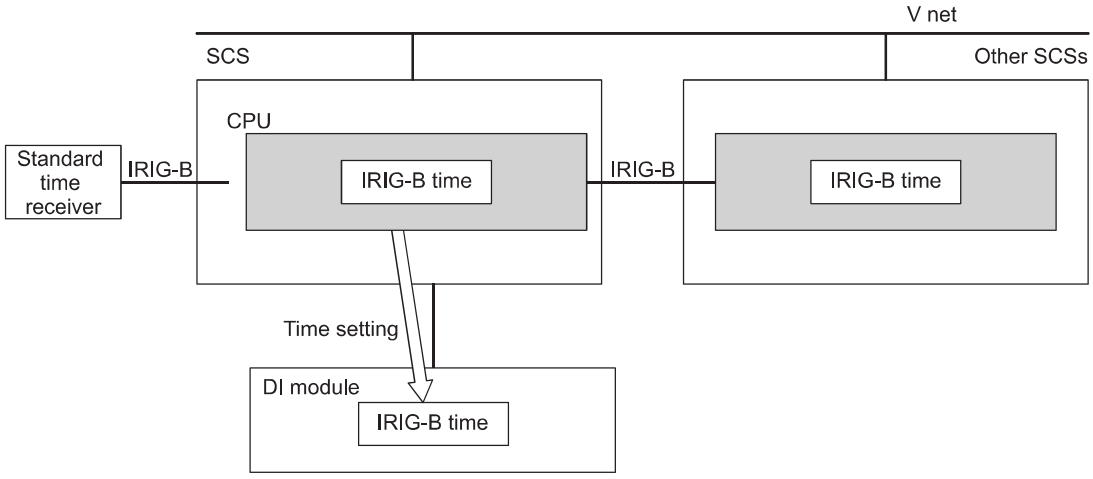


Figure Appendix 4.1-2 IRIG-B time synchronization

Precautions for time synchronization

Precautions regarding time synchronization of SCSs that are connected on V net are described as follows:

When the V net time synchronization is selected

Changing the V net time may cause the SOE generation order to be reversed. Be sure to take the timing to set the time and the difference of the time into consideration when setting the V net time.

When the IRIG-B time synchronization is selected

- It is necessary to synchronize V net clock with IRIG-B clock.
- If the input of the IRIG-B signal fails, SCS updates the time based on the IRIG-B time immediately before the failure. (No synchronization with V net time)
- When the input of the IRIG-B signal recovers, the displayed time may be set back to synchronize with the IRIG-B time again. In this is case, if you want to check the messages and events raised before the recovery, do not sort the messages and events until you finish your check.

If a Vnet/IP domain and a V net domain are connected via a V net router

The following precautions apply in a situation where a V net domain and a Vnet/IP domain are connected via a V net router and the V net time synchronization and the Vnet/IP time synchronization are selected as their respective time synchronization methods.

- If you are using a V net router of style S3 and above and have enabled the Transfer system time ([Transfer higher] or [Transfer lower]) in the V net router property of System View for CENTUM VP R5.01 or later, it is not possible to change the time from a SENG in the domain to which the time is transferred.
- If you are using a V net router of a style below S3 and have enabled the [Transfer lower] of Transfer system time ([Transfer System Time - Transfer lower] for CENTUM VP earlier than R5.01), it is not possible to change the time from a SENG in the V net domain that constitutes a lower domain.

Time discrepancy when multiple domains are connected

You need to consider the following points when connecting multiple domains:

- The time discrepancy that occurs between each connected domain depends on the number of connected BCV-V units. The discrepancy is a maximum of 5 seconds for the first level BCV-V and a maximum of 10 seconds for the second level. Estimate these deviations and if they are not acceptable, consider applying IRIG-B time synchronization.
- If a domain is connected through the wide area network gateway units (CGW), you need to take the measure to keep the differences of the V net time among the domains within an allowable range. Alternatively, consider applying IRIG-B time synchronization.

Actions taken at error occurrence in IRIG-B time synchronization

The IRIG-B time synchronization status can be checked in the SCS State Management Window of the SCS Maintenance Support Tool on the SENG, or in the SCS Status Display view on the HIS.

Reasons for time synchronization error

A time synchronization error occurs for the following reasons.

- Disconnected IRIG-B cable connector
- IRIG-B interface unit failure in the SCS
- No time notification due to GPS receiver failure

TIP

Examples of GPS receiver failure are listed below.

- Failure in the communication route from the GPS antenna to the GPS receiver
- Antenna failure or receiving problem

What happens when the GPS receiver fails is determined by the specification of the selected GPS receiver. The following is an example of what might happen when the GPS receiver fails.

- Since GPS signals are no longer received, the GPS receiver operates based on its clock.
- If reception problem continues more than a specified period, the GPS receiver stops operating on its clock and also stops notifying time information to the connected devices.

Once time notification is stopped, the SCS outputs a diagnostic information message notifying an IRIG-B error.

Notification of time synchronization error

- If the IRIG-B time synchronization state has become abnormal when the IRIG-B time synchronization is selected, the SYNC LED on the SCS's CPU module turns off and a diag-

nostic information message indicating an error is notified. If the SCS adopts a redundant CPU module configuration, diagnostic information messages regarding both modules are notified.

- Once the IRIG-B time synchronization state returns to normal, a diagnostic information message indicating a recovery is notified.

SCS actions taken upon time synchronization error

If time synchronization with IRIG-B stops, the SCS does not synchronize with the V net time. Instead, the SCS's CPU module updates the time based on the time information input immediately before the error. This condition is called "non-synchronized state." The time is updated continuously by the CPU module, but time accuracy still drops. Therefore, it is necessary to recover the IRIG-B error to normal as soon as possible.

While the "not-synchronized state" continues, the SCS takes actions as follows.

- In the not-synchronized state, the difference from the standard time and the time discrepancy among SCSs gradually becomes larger as the time elapses. The difference from the standard time can reach up to ± 4.32 seconds/day and the time discrepancy among SCSs can reach up to 8.64 seconds/day. When debugging applications that require high time precision, it is recommended to connect a GPS simulator to prevent the system from entering the not-synchronized state.
- If the IRIG-B is not connected at the start of the SCS that uses the IRIG-B time synchronization, the SCS enters a not-synchronized state where the CPU module updates the time based on the V net time that was input when the SCS was started.
- If the IRIG-B is not connected at the start of the SCS that uses the IRIG-B time synchronization, a diagnostic information message notifying the cause of the last CPU shutdown and a diagnostic information message regarding the switching of the CPU control right, both of which are normally output when the SCS is started, will not be output.
  Once the SCS has been started or CPU control right switched, however, subsequent messages will be output correctly.
- You can connect normal IRIG-B signals to recover from the error state while the SCS is in a not-synchronized state. Once the signals are connected, the SCS will operate based on the correct time information input from the IRIG-B.

IMPORTANT

If the IRIG-B time synchronization is selected, connect the GPS unit via the IRIG-B first, and then start the SCS.

Time discrepancy caused by GPS failure

With stations connected to the V net where time synchronization among SCSs is performed by the IRIG-B time synchronization, a time discrepancy will occur if the GPS or IRIG-B interface fails because time synchronization by V net will not be carried out, either.

Table Appendix 4.1-2 Abnormality and time discrepancy

Abnormality	Phenomenon	Predicted Discrepancy
Antenna	When antenna error occurs, the standard time receiver will count the time based on its own clock. If the antenna error prolonged, the discrepancy may increase. If multiple SCSs are using the same receiver for time synchronization, the discrepancy will not occur for the SCSs. However, if they use different receivers for time synchronization, the time discrepancy among the SCSs may occur.	Discrepancy varies with the model of standard time receiver. It is necessary to query the vendor of the recover.
The Standard Time Receiver IRIG-B Cable IRIG-B Interface	When abnormality occurs, each SCS will count the time based on its own clock. If abnormality is prolonged, the discrepancy from the standard time and the discrepancy among SCSs may increase.	The time discrepancy among SCSs may occur. The maximum discrepancy is 8.64 sec/day.

Appendix 4.2 Inter-SCS safety communication in a V net domain

Inter-SCS safety communication is supported from SCS system program revision number R1.01.30 or later.

It is possible to perform Inter-SCS Safety Communication between SCS stations in the same V net domain or different V net domains to a range of up to 2 BCV or CGW hops.

If Inter-SCS safety communication is executed between the SCSs whose system program release number is prior to R1.02 in the different V net domains, the communication path cannot include Vnet/IP domains.

Appendix 4.3 Precautions when engineering CENTUM systems for using BCV and CGW

BCV and CGW engineering are performed by CENTUM ENG. In this case, follow the precautions below.

TCP/IP communication relay processing

In the CENTUM Integration Configuration, enable the “Transfer TCP/IP to FCS” in the setting items of BCV or CGW (one of the settings of the CENTUM system builder function), to allow the BCV or CGW to relay TCP/IP broadcast frames in both directions. This function allows the TCP/IP communication between the SENG and SCS to be performed across domains.

Time-related function

BCV and CGW have the function of transferring the time setting when time is set in the Adjust Time dialog on HIS or SENG.

SEE ALSO For more information about TCP/IP communication relay processing and time-related functions, refer to:

- Communication Devices Reference (IM 33J20B10-01EN)
- Communication Devices Reference (IM 33K03M10-50E)

Time discrepancy between domains

A maximum time discrepancy of 5 seconds occurs between two domains connected via a BCV. Times are not synchronized automatically when the time discrepancy increases between two domains connected via CGWs. One way to reduce the time discrepancy in either case is to synchronize each domain with an external absolute time. In this case, ensure that you do not transfer the time by BCV or receive the system time via CGW.

Appendix 4.4 System expansion with V net router connection

It is possible for SENG and/or SCS in a Vnet/IP domain to access an SCS in a V net domain. It is also possible to access an SCS in a V net domain from a CENTUM system and/or Exaopc client in a Vnet/IP domain via a V net router. The V net router is engineered by using the system builders of CENTUM.

When connecting a V net router, make sure to check that the load on the V net router caused by communication passing through the V net router will not become excessive.

TIP

V net routers (AVR10D) are classified into two types of behavioral specification, based on their hardware style and system software revisions. In this document, the two types are defined as "V net router of style S3 or above" and "V net router of a style below S3" as follows.

- V net router of style S3 or above
  When the style of AVR10D is S3 or above and the "operating mode" of V net router is set to [Standard Mode] in the System View of CENTUM VP R5.01 or later. Or, when the “operation mode” of V net router is set to [Extended Mode] in the System View of CENTUM VP R6.07 or later.
- V net router of a style below S3
  For all cases other than the condition described in "V net router of style S3 or later"

If no style is mentioned in explanations about the operation of the V net router in this document, the operation is common to all AVR10D styles and ProSafe-RS/CENTUM VP software revisions.

The following functions are implemented in the V net router connection configuration.

- Perform engineering and maintenance of SCS in a V net domain from SENG in a Vnet/IP domain
- Perform engineering and maintenance of SCS in a Vnet/IP domain from SENG in a V net domain
- Perform safety communication between SCS in a Vnet/IP domain and SCS in a V net domain
- Perform operation and monitoring of SCS in a V net domain from an HIS in a Vnet/IP domain
- Perform operation and monitoring of SCS in a Vnet/IP domain from an HIS in a V net domain
- Refer to data in an SCS in a V net domain and write data to an external communication FB from an FCS in a Vnet/IP domain
- Refer to data in an SCS in a Vnet/IP domain and write data to an external communication FB from an FCS in a V net domain
- Collect and display SOE and diagnostic information of an SCS in a V net domain from the CENTUM Sequence of Events Manager or ProSafe-RS SOE Viewer installed on an HIS in a Vnet/IP domain
- Install the ProSafe-RS SOE OPC Interface package on a PC in a Vnet/IP domain or V net domain and use the HIS or SENG as an OPC server to display SCS events on an OPC client (e.g., Exaquantum) in a Vnet/IP domain.
- Set up an Exaopc server in a Vnet/IP domain or V net domain and access data on the SCS from an OPC client (e.g., Exapilot) in a Vnet/IP domain.
- V net router of style S3 or above: Connect multiple Vnet/IP domains on a single V net domain
- V net router of style S3 or above: Execute SCS global switch communication (link transmission between FCS and SCS stations) between a V net domain and a Vnet/IP domain connected to a V net router.

- V net router of style S3 or above: Effect a time transfer from a V net domain to a Vnet/IP domain with the V net domain as the clock master, or vice versa
- The following specifications are applied when using a V net router of a style below S3
  The V net domain cannot be made the clock master, which means that you cannot change the time on the Vnet/IP domain even if you set the time from a SENG or HIS on the V net domain

Precautions when engineering CENTUM systems for using V net routers

V net routers are engineered using CENTUM ENG. Take the following precautions when engineering the routers.

TCP/IP communication relay processing

When the system consists of V net domains and Vnet/IP domains, enable [Transfer TCP/IP to FCS] in the setting items of the V net router (one of the settings of the CENTUM system builder function) to allow the V net router to relay the TCP/IP broadcast frames in both directions. This function allows the TCP/IP communication between the SENG and SCS to be performed across domains.

Transferring system time

- If you are using a V net router style S3 or above, open the "V net router" property from System View in CENTUM VP R5.01 or later, and specify the Transfer system time ([Transfer upper] or [Transfer lower]). This allows the time on either the V net domain or the Vnet/IP domain connected to the V net router to be transferred to another domain as the master.
- In the case of using a V net router style below S3, the Vnet/IP domain is always the upper domain. It is not possible to transfer the time from the lower domain to the upper domain.

Time discrepancy between domains

A maximum time discrepancy of 5 seconds occurs between two domains connected via a V net router. One way to reduce the time discrepancy is to synchronize each domain with an external absolute time rather than effecting a time transfer via the V net router.

Inter-SCS safety communication in systems in which a V net domain and a Vnet/IP domain are connected

Inter-SCS Safety Communications have different network reach ranges according to the specifications of V net router to be applied.

- Network range for style S3 or above
  In a communications route between two stations, network reach is up to 4 hops for connections between a V net domain and a Vnet/IP domain via a V net router, and up to 2 hops for connections between V net domains via a BCV or CGW.

  The following figure shows the domain configuration for the maximum network range when V net routers of style S3 or above are used.

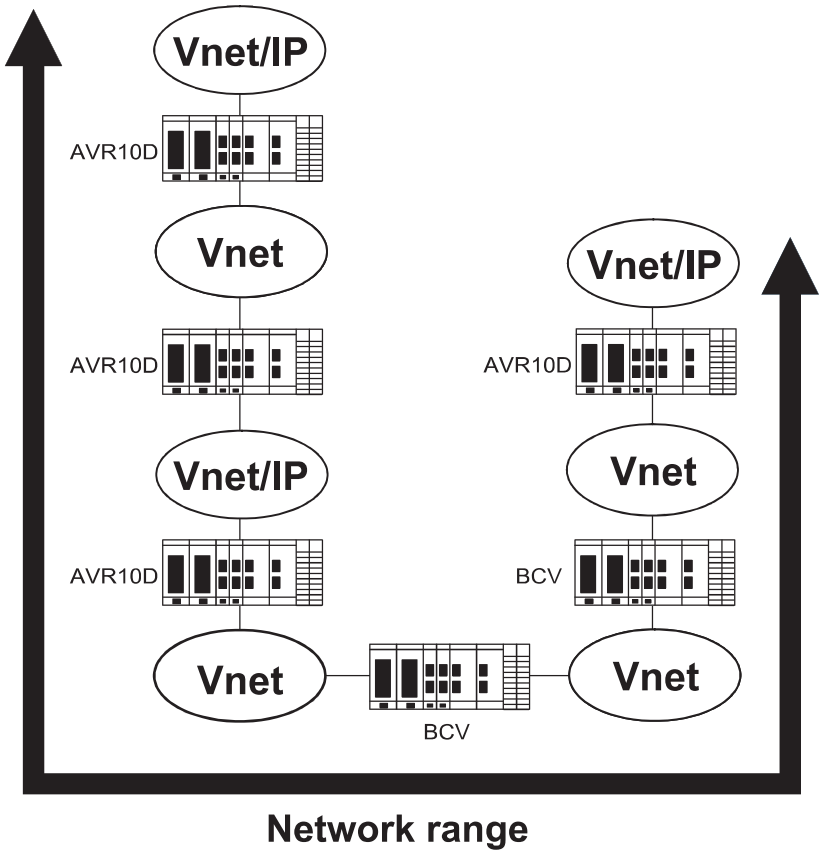


Figure Appendix 4.4-1 Network range when a V net router of style S3 or above is used

- Network range for style below S3
  The network reach range for inter-SCS Safety Communications is up to 2 hops for connections between V net domains via a BCV or CGW. It is not possible to have a V net domain on a mid-stream route communicating between Vnet/IP stations. That is, the configuration of SCSs on two Vnet/IP domains with a V net domain in between is not allowed.

  The following figure shows the domain configuration for the maximum network range when V net routers of a style below S3 are used.

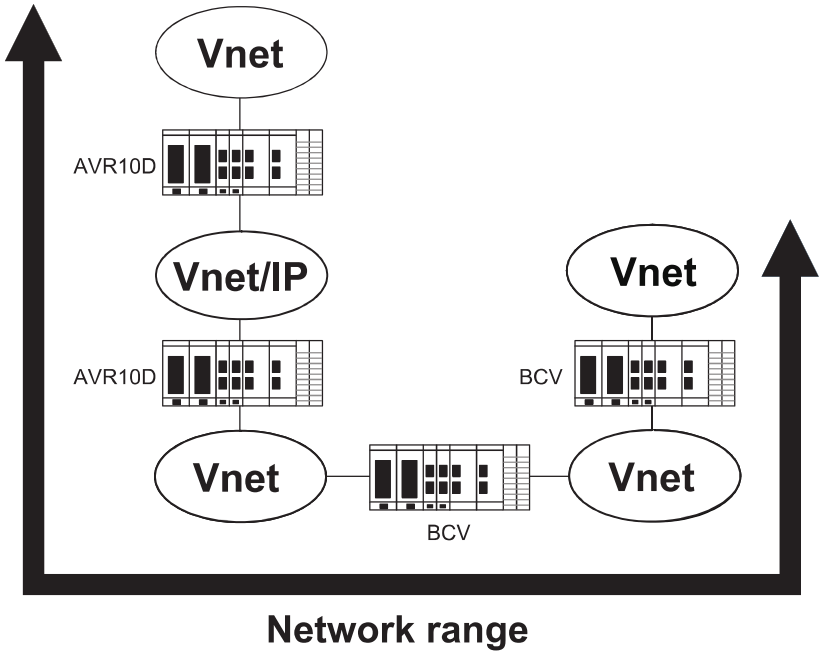


Figure Appendix 4.4-2 Network range when a V net router of a style below S3 is used

Virtual domain link transmission

If you are using a V net router style S3 or above, SCS Link Transmission Global Switch Communication is possible within a virtual domain by deploying the V net domain and Vnet/IP domain connected to that V net router as a single virtual domain.

To enable this feature, you must set up the V net router by using the CENTUM system builder function.

Issues to consider when using Virtual domain link transmission

The following are issues to consider when making a virtual domain link transmission.

- If you are using a V net router style S3 or above and CENTUM VP R5.01 or later, you can enable and disable virtual domain link transmission using the V net router settings included in the system generation function in CENTUM. If you set virtual domain link transmission for the V net router to [Enabled], link transmission is enabled between the V net domain and Vnet/IP domain connected to the V net router.
- To change the Enable/Disable setting for virtual domain link transmission, you will need to perform an offline download to the V net router.
- The guaranteed reach for virtual domain link transmission is within the same virtual domain as the sending station.
- Link transmission is not available between separate virtual domains. When connecting Vnet/IP domain A and B via V net, for example, Vnet/IP(A) – V net and Vnet/IP(B) – V net are discrete virtual domains. Consequently, link transmission can not be made between Vnet/IP(A) and Vnet/IP(B). When connecting V net domain A and B via Vnet/IP, V net(A) – Vnet/IP and V net(B) – Vnet/IP are discrete virtual domains likewise. Consequently, link transmission can not be made between V net(A) and V net(B).
- When you make a virtual domain link transmission, there must be no duplication of the station numbers inside the virtual domain.
- When two or more virtual domains are connected by a domain added to two or more virtual domains, station numbers must be unique in all these virtual domains.

Example use of Virtual domain link transmission

Virtual domain link transmission is useful in situations such as when migrating part of a V net domain and changing it to a Vnet/IP domain. The following figure shows an example configuration.

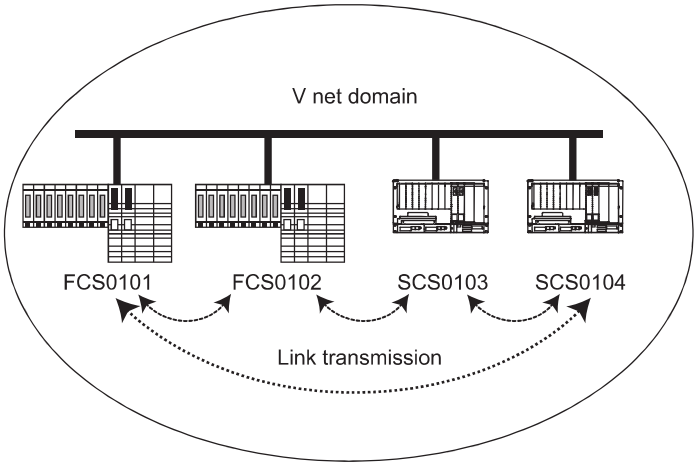


Figure Appendix 4.4-3 Example of the configuration of a Link transmission in a V net domain

The following figure shows an example of a migration in which part of a V net domain is split into a Vnet/IP domain and an FCS0102 and SCS0104 are added to the Vnet/IP domain.

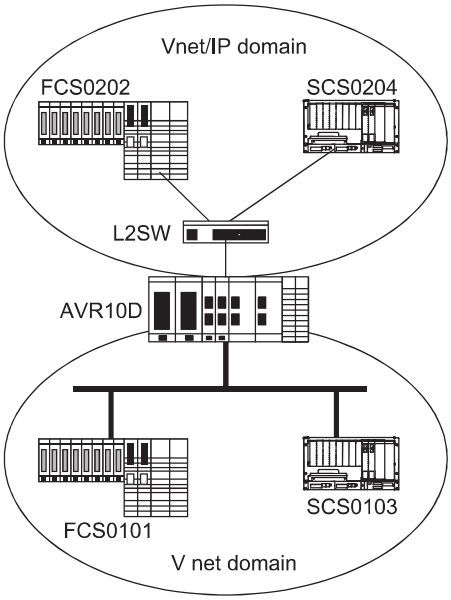
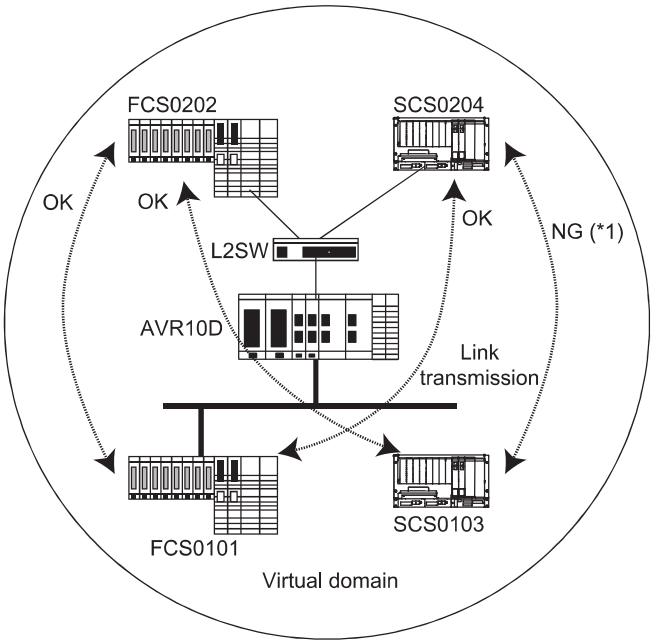


Figure Appendix 4.4-4 An example of a V net domain split into V net and Vnet/IP domains

The following figure shows an implementation of a link transmission.



*1: Virtual link transmission between SCSs (SCS link transmission safety communication) can not be executed.

Figure Appendix 4.4-5 Example of a Virtual domain link transmission

If the global switch for an SCS that has been migrated from V net to Vnet/IP is referenced by an FCS, it may, depending on the referencing method, be necessary to re-engineer the application concerned with the global switch in the FCS.

- If the global switch in the SCS is referenced by specifying the FCS as %GSnnnss (nnn: %GS number, ss: station number)

  You must re-engineer the FCS application if the SCS station number has been changed. It is not necessary to re-engineer the application if only the SCS domain number has been changed.

  Example: In the figure above, if FCS0101 references %GS001 in SCS0204, it is not necessary to change "%GS00104" referred to in the FCS0101 application.

- If the global switch in the SCS is referenced by specifying the FCS as %GSnnnSddss (nnn: %GS number, dd: domain number, and ss: station number)
  You must re-engineer the FCS application if the SCS domain number or station number has been changed.

  Example: In the figure above, if FCS0101 references %GS001 in SCS0204, it is necessary to change "%GS001S0104" referred to in the FCS0101 application to "%GS001S0204."

- If the global switch for an FCS that has been migrated from V net to Vnet/IP is referenced by an SCS.
  Provided that the station number does not change, it is not necessary to re-engineer the application concerned with the SCS link transmission. If the station number has been changed, you must change the station type in the Other Stations tab sheet of the SCS link transmission definition in SCS Link Transmission Builder, and redefine the wiring in Data Wiring Definition.

Revision information

Title : Engineering Guide Vol. 1

Manual No. : IM 32P01C10-01EN

Dec. 2023/11th Edition/R4.10 or later

F2.1.1	Deleted descriptions related to unsupported OS.
Appendix 3.4	Added the changed specifications in R4.10.

Jun. 2023/10th Edition/R4.09

C2.2, D5	Added description about versions that support iDefine.
C3, E1.3, E3.1	Updated descriptions of POU online change download.
Appendix 3.4	Added the changed specifications in R4.09.

Nov. 2022/9th Edition/R4.08

Appendix 3.4	Added the changed specifications in R4.08.

Jan. 2022/8th Edition/R4.07

D4.4	Updated descriptions of reflecting the POU that was defined by using iDefine.
D5.3	Added descriptions of cautionary notes on the use of the POWE/LOGE function.
E1.2	Updated descriptions of procedure for creating an application
Appendix 3.4	Added the changed specifications in R4.07.

Feb. 2021/7th Edition/R4.06

Introduction, A1, A4, A10.6, C2.2, D4.3, I5, I6	Updated FAST/TOOLS to CI Server.
Entire manual	Added descriptions of SIL 2 SCS.
A5.3	Updated the descriptions of when connecting N-IO nodes with fiber-optic cables.
B4	Updated the descriptions of PFD calculation.
C5.2.5	Added descriptions related to the new FB.
D1.4.1, Appendix 1.3.1	Updated the descriptions of P&ID Tag.
E1.3	Updated the descriptions of changing user-defined FB.
F2.1.1	Deleted descriptions related to unsupported OS.
Appendix 3.4	Added the changed specifications in R4.06.

Dec. 2019/6th Edition/R4.05

Introduction	Updated description of registered trademarks and trademarks.
A2.1, I4, I4.1, I4.1.1 to I4.1.9	Added description related to Forced I/O Viewer function.
A5, A7.2	Updated description due to supporting S2CP471.
A5	Improved descriptions regarding the optical ESB bus repeater
C1.2.6, C2.3, E1.2, E1.3, E2.1, E2.3, Appendix 3.4	Added description related to skipping of password of manual operation FB.
C2.2, D43, D5	Updated description due to improvement of workflow with iDefine.

D1.4.1, D1.4.2, D1.4.3, D1.4.5, D1.4.6	Updated description due to improvement of operability of Safety I/O Editor.
D1.5	Added description related to Safety I/O parameter profile.
D2.3, D2.4, D2.6, D2.7, F2.2	Updated description due to improvement of operability of Safety Communication I/O Editor.
D3.4, D3.5, E3.3	Updated description due to improvement of operability of IOM Definition editor.
D3.7, D3.8	Added description of import/export from IOM Definition editor.
E1.1	Improved descriptions of adding variables in online change download
E3.4	Improved descriptions of SCS project duplication procedure
H1.2	Added description of Operation data reset switch.
I5	Added description of stand-alone ProSafe-RS system.
I6	Added procedures and precautions for adding or replacing Vnet/IP devices.
Appendix 4.4	Changed descriptions due to supporting AVR10D extended mode

Aug. 2018/5th Edition/R4.04

Introduction	Updated description of registered trademarks of YOKOGAWA.
A1.1, I5	Changed description due to supporting virtualization platform.
C1.2.4, C2.1, Appendix2.1	Changed explanations due to changing the SCS Manager start-up method.
D1.4.1, D2.3, D5.1	Added descriptions due to adding the Safety I/O Editor mode and the Safety Communication I/O Editor mode.
D1.4, D2.3, D3.2	Updated the figure due to adding the SCS Manager start-up icon.
Appendix 1.3.2	Changed explanations due to changing the IOP upper/lower limit detection level of SAI143-H and S2MMM843.
Appendix 1.3.2	Changed explanations due to changing the transmitter error upper/lower limit detection level of SAI143-H and S2MMM843.

Oct. 2017/4th Edition/R4.03.10

Entire manual	Added Safety Communication I/O List and Safety Communication I/O Editor.
Introduction	Added the fire and gas communication module.
A2, A4, A5, A8, A9, A10, B4, B5, C2, C3, C5, H1, I1.1, C5, G2.2.9, F1	Added and updated descriptions regarding the safety subsystem communication function.
A5, A8, A9, G2.2, G2.2.9, H3.2, I1.2, Appendix 2.2	Added descriptions regarding the fire and gas communication module.
A10.6, C1.1, C3, E1.2	Updated descriptions due to functional enhancement of Version Control Tool and Master Database Restoring Function.
C1, E1.3	Added descriptions of Command Line.
Part D	Added descriptions of engineering based on the safety communication I/O list. Deleted descriptions of grid rules and moved them to Engineering Guide Vol. 2 (IM 32P02C10-01EN). Added and updated descriptions of RS Generation Manager. Added precautions when performing engineering by using iDefine.
D	Added descriptions of settings with PROFINET Configurator.

E1.5	Added precautions related to the fire and gas communication module when performing online change download.
H3.1.2	Added FPGA revision to the IOM Report display format.
I1.4	Added descriptions regarding maintenance of field wireless system devices.
I2	Reorganized the descriptions of proof tests and tests for improving the rate of operation.
Appendix 3.4	Added descriptions of major changes in R4.

May 2017/3rd Edition/R4.03

Entire manual	Changed description regarding the start menu
Introduction	Deleted Windows Vista from explanation of trademarks
A1.2, A1.3, H7, I4.7	Added explanation of Vnet/IP ring topology
A5, B5, E1.6, H3.1.2, H3.1.3, H4, Appendix 1.2, Appendix 1.3, Appendix 2.2	Added explanation of S2MDV843 and changed explanations in accordance with addition of S2MDV843
C1.2.5, C2.3, C5.2.5, D1.1.2, E1.2, E1.3, E2.1, E2.3, E3.1, A1.2, A1.3.2	Added explanation of the fire and gas equipment transmitter power OFF/ON function
C2.3, D1.1.2, E1.3, E2.1, A1.3.2	Added explanation of the chattering alarm suppression function
D2.4	Changed explanation of function blocks
E3.1, E3.2, E3.3, E3.4	Added explanation of the Project Comparing Tool
F2.1.1	Added specifications of the Node Number Setting Tool

Oct. 2016/2nd Edition/R4.02

Entire manual	Changed the symbols that indicate warning and caution.
Introduction	Updated descriptions in "■ Safety, Protection, and Modification of the Product," "■ Symbols," and "■ Trademark Acknowledgments." Added a new term in "■ Full Names and Simplified Terms."
A2.1, B1, B2, C1.2, C2.1, C2.2, D1, D1.1, D1.2, D1.3, D1.3.4, D2, D2.1, D2.2, D2.3, D2.4, E2.2	Added explanations on iDefine
Part A, Part C, Part D, Appendix 2, Appendix 3	Changed layout
A6, A10, A10.2, A10.3, A10.5, C2.3, C3, C6, C7, C9, D1.1, E1.2, E1.5, Appendix 2, Appendix 2.1	Changed explanations

Dec. 2015/1st Edition/R4.01

Newly published

■ For Questions and More Information Online Query: A query form is available on the following URL for online query. http://www.yokogawa.com/iss
■ Written by Yokogawa Electric Corporation
■ Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Attachment 9.3 Engg Guide Vol-2

IM32P01C20-01EN

User's
Manual

ProSafe-RS
ProSafe-RS Lite

Engineering Guide Vol. 2

IM 32P01C20-01EN

YOKOGAWA
Yokogawa Electric Corporation

IM 32P01C20-01EN
10th Edition

Introduction

This manual describes the operating procedures and precautions when building application logics in ProSafe-RS engineering. It also describes the details of engineering and maintenance for connecting ProSafe-RS to CENTUM VP and other systems. You can read it for your necessary information.

For the overview of ProSafe-RS system, the points at the engineering, and the cautionary notes, as well as a description of how to design, make, operate, and maintain a safety system using ProSafe-RS, based on the workflow of engineering, refer to Engineering Guide Vol. 1.

If you are using YFGW520, replace the term “YFGW510” with “YFGW520” in the User’s Manual. For information on how to use YFGW520, refer to “YFGW520 Field Wireless Access Point (IM 01W02E02-01EN).”

This manual consists of the following parts:

- Part A Configuring application
  This part describes the operating procedures and precautions when building application logics in ProSafe-RS engineering.
- Part B CENTUM integration
  This part describes the engineering and maintenance when integrating ProSafe-RS and CENTUM.
- Part C SOE OPC interface
  This part mainly describes specifications of the SOE OPC Interface of ProSafe-RS and compatibility with the OPC specifications. It also describes the setup procedures required to connect to OPC clients using the SOE OPC Interface.
- Part D Subsystem communication
  Subsystem communication is used for connections between the ProSafe-RS and other systems. This part describes the subsystem communication functions and setting items required for connections with other systems.
- Part E Safety subsystem communication
  Safety subsystem communication provides safe communications between ProSafe-RS and other subsystem devices. This part describes the safety subsystem communication function and setting items required to use safety subsystem communication.
- Part F Modbus slave communication
  Modbus slave communication is used for connections between the ProSafe-RS and other systems. This part describes the definition of communication modules, definition of addresses of Modbus devices, and data setting using Modbus slave communication, which are required for connections.
- Part G DNP3 slave function
  DNP3 communication is used for connections between ProSafe-RS and other systems. This part describes the DNP3 slave function as well as engineering and maintenance on the SENG.
- Appendix
  This part describes information about engineering of subsystems.

  This part also describes the DNP3 Field Device Profile.

10th Edition : Dec. 2023 (YK)
All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Safety Precautions for Use

Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Be sure to confirm the specifications and required settings of the devices that are used in combination with the Product by referring to the instruction manual or other documents of the devices.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:



Indicates that caution is required. This symbol for the Product indicates the possibility of dangers such as electric shock on personnel and equipment, and also indicates that the user must refer to the User's Manuals for necessary actions. In the User's Manuals, this symbol is used together with a word "CAUTION" or "WARNING" at the locations where precautions for avoiding dangers are described.

<French> Signale qu'il faut faire preuve de prudence. Ce symbole pour le produit signale la possibilité d'un danger pour le personnel et l'équipement comme un choc électrique, et signale également que l'utilisateur doit se référer au Manuel de l'utilisateur afin de prendre les mesures nécessaires. Dans le Manuel de l'utilisateur, ce symbole est utilisé conjointement avec la mention «CAUTION» ou «WARNING» aux endroits où sont décrites les précautions pour éviter les dangers.



Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.

<French> Signale qu'il faut faire preuve de prudence avec la surface brûlante. Les appareils sur lesquels est apposé ce symbole risquent de devenir brûlants. Tout contact physique ou matériel avec ces appareils risque de provoquer des brûlures ou des dommages.



Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.



Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.

Indicates an AC supply.

Indicates a DC supply.

| Indicates that a component such as a power supply switch is turned ON.

○ Indicates that a component such as a power supply switch is turned OFF.

Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

Warning and Disclaimer

- Except as specified in the warranty terms, YOKOGAWA shall not provide any warranty for the Product.
- YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Product.

Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the Software Product's merchantability or suitability for any particular purpose, except as specified in the warranty terms.
- Purchase the appropriate number of licenses of the Software Product according to the number of computers to be used.
- No copy of the Software Product may be made for any purpose other than backup; otherwise, it is deemed as an infringement of YOKOGAWA's Intellectual Property rights.
- Keep the software medium of the Software Product in a safe place.
- No reverse engineering, reverse compiling, reverse assembling, or converting the Software Product to human-readable format may be performed for the Software Product.
- No part of the Software Product may be transferred, converted, or sublet for use by any third-party, without prior written consent from YOKOGAWA.

Documentation Conventions

Symbols

The following symbols are used in the User's Manuals.

 WARNING	Indicates precautions to avoid a danger that may lead to death or severe injury.
 CAUTION	Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.
IMPORTANT	Indicates important information required to understand operations or functions.
TIP	Indicates additional information.
	Indicates referenced content. In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

Typographical Conventions

The following typographical conventions are used throughout the User's Manuals.

Commonly Used Conventions throughout the User's Manuals

- Δ Mark
  Indicates that a space must be entered between character strings.
  Example:

  ```
  .ALΔPIC010Δ-SC
  ```

- Character string enclosed by braces { }
  Indicates character strings that may be omitted.

  Example:

  ```
  .PRΔTAG{Δ.sheet name}
  ```

Conventions Used to Show Key or Button Operations

- Characters enclosed by brackets [ ]
  When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a button name in a window, or an item in a list box displayed in a window.

  Example:

  To alter the function, press the [ESC] key.

Conventions of a User-defined Folder

- User-defined folder name enclosed by parenthesis ( )
  User definable path is written in a pair of parentheses.

  Example:

  ```
  (RS Project Folder)\SCS0101
  ```

If the RS Project Folder is `C:\MYRSPJT`, the above path becomes `C:\MYRSPJTSCS0101`.

Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.
If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

Definitions of Node and Module Terms

In the User's Manuals, nodes and modules are referred to by using collective terms, another terms, or abbreviations based on the following definitions:

- Definitions of nodes
  - Node: A node is a collective term for an FIO node and an N-IO node.
  - FIO node: This is a collective term for a safety control unit, a safety node unit, and a unit for optical ESB bus repeater module.
  - CPU node: This is another term for a safety control unit. The abbreviation of safety control unit is SCU.
  - I/O node: This is another term for a safety node unit. The abbreviation of safety node unit is SNU.
  - N-IO node: This is a collective term for a node interface unit and an N-IO I/O unit. The abbreviation of node interface unit is NIU.
- Definitions of modules
  - I/O module: This is a collective term for an FIO I/O module and an N-IO I/O module.
  - FIO I/O module: This is a collective term for an analog I/O module and a digital I/O module for FIO, and a communication module.
  - N-IO I/O module: This is a collective term for the modules that can be mounted on an N-IO I/O unit.
  - AIO/DIO module: This is a collective term for an analog I/O module, a digital I/O module, and a universal type I/O module.
  - Analog I/O module: This is a collective term for an analog input module and an analog output module.
  - Digital I/O module: This is a collective term for a digital input module and a digital output module.
  - Universal type I/O module: This is a collective term for the I/O modules for which the channel signal category can be changed by software.

- Input module: This is a collective term for an analog input module, digital input module, and a universal type I/O module with defined input channels.
- Output module: This is a collective term for an analog output module, digital output module, and a universal type I/O module with defined output channels.
- Communication module: This is a collective term for a serial communication module, an Ethernet communication module, and a fire and gas communication module.

Full Names and Simplified Terms

In the User's Manuals, simplified terms listed in the following table are used.

Table Info-1 Full Names and Simplified Terms

Full Name	Simplified Term
Automation Design Suite	AD Suite
Automation Design Organizer	AD Organizer
Automation Design Server	AD Server
Automation Design project	AD project
Automation Design Master Database	ADMDB
Automation Design Suite Administration Tool	ADS Administration Tool
iDefine for ProSafe-RS	iDefine
Modification Package	ModPack
SCSV1-S (SCS supporting the SSC10S/SSC10D safety control units)	SCSV1
SCSP1-S (SCS supporting the SSC50S/SSC50D safety control units)	SCSP1
SCSP2-S (SCS supporting the SSC60S/SSC60D safety control units)	SCSP2
SCSP3-S (SCS supporting the S2SC70S/S2SC70D safety control units)	SCSP3
SCSL2-S (SCS supporting the L1SC70S/L1SC70D safety control units)	SCSL2
SCSU1-S (SCS supporting the SSC57S/SSC57D safety control units)	SCSU1

Copyright and Trademark Notices

All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, PRM, Exaopc, FieldMate Validator, and STARDOM are registered trademarks or trademarks of Yokogawa Electric Corporation.
- The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

Engineering Guide Vol. 2

IM 32P01C20-01EN 10th Edition

CONTENTS

PART-A Configuring application..... A-1

A1. Precautions for creating an application..... A1-1

A1.1 Creating an application logic..... A1-4

A1.2 Windows used to create application logic..... A1-5

A2. Creating an application for the diagnostic function of the SCS..... A2-1

A3. Creating an application for monitoring the status and process state of the SCS..... A3-1

A3.1 Monitoring SCS status..... A3-2

A3.2 Monitoring process with process alarm message and annunciator message..... A3-3

A3.3 Fire and gas device application..... A3-4

A3.4 Device reset function for smoke detectors and heat detectors..... A3-5

A3.4.1 Device reset function with FIO..... A3-7

A3.4.2 Device reset function with N-IO..... A3-9

A3.4.3 Device reset function and alarm suppression during device reset..... A3-11

A3.4.4 Engineering regarding the device reset function and alarm suppression during device reset..... A3-14

A3.5 Utilization of override when performing maintenance of fire and gas devices..... A3-19

A4. Example of creating an application logic..... A4-1

A4.1 Use of analog input value..... A4-2

A4.2 Shutdown due to channel failure..... A4-7

A4.3 Example of displaying I/O status..... A4-12

A4.4 Relations among AIO/DIO, Communication module and System FBs..... A4-13

A4.5 Example of using BOOL-type Data Manual Operation FB (MOB_*)..... A4-15

A4.6 Construction example of First-up Alarm function..... A4-18

A4.7 Considerations on using Time Synchronization Function Block (SYS_SETTIME)..... A4-20

A5. Library projects..... A5-1

A5.1 Creation of library projects..... A5-2

A5.2 Items set for library projects..... A5-4

A5.3 Precautions on library projects..... A5-6
A5.3.1 Software revision of SCS project and library project.....A5-7
A5.3.2 Operations when incorporating library projects into SCS project..... A5-8
A5.3.3 Differences between SCS projects and library projects.....A5-9
A5.3.4 Operations on SCS projects and relationship with libraries.....A5-10
A5.3.5 Precautions when testing library projects.....A5-11
A5.3.6 Precautions when using Integrity Analyzer.....A5-12
A5.3.7 How to make changes to library projects.....A5-13
A6. SCS link transmission..... A6-1
A6.1 Overview of the SCS link transmission..... A6-2
A6.2 Data structure and definition of the SCS link transmission..... A6-5
A6.3 SCS link transmission definition..... A6-11
A6.4 Actions taken for SCS link transmission when SCS is unsteady..... A6-21
A6.5 SCS global switch communication..... A6-24
A6.5.1 Referencing FCS data from SCS.....A6-25
A6.5.2 Data setting from SCS to FCS.....A6-27
A7. Inter-SCS safety communication.....A7-1
A7.1 Inter-SCS safety communication definition.....A7-12
A7.2 Combination of communication data and FBs for Inter-SCS safety communication.....A7-15
A8. SOER functions and how to use them.....A8-1
A8.1 Overview of SOER.....A8-2
A8.2 Event collection.....A8-4
A8.3 Event storage..... A8-8
A8.4 Management of event information when SCS is unsteady..... A8-10
A8.5 SOER collection definition.....A8-12
A9. HART communication..... A9-1
A9.1 Description..... A9-2
A9.2 PST engineering.....A9-4
A9.3 HART communication function specific to N-IO.....A9-6
A9.3.1 Status change notification function of HART devices..... A9-7
A9.3.2 Precautions for the transfer method of the status change in HART devices.....A9-9

Engineering Guide Vol. 2

IM 32P01C20-01EN 10th Edition

CONTENTS

PART-B CENTUM integration.....B-1

B1. Overview of CENTUM integration.....B1-1

B2. Integration with CENTUM.....B2-1

B3. Tag name interfaces for CENTUM.....B3-1

B3.1 Overview of tag name interfaces.....B3-2

B3.2 Tag name interfaces for internal variables and I/O variables.....B3-10

B3.3 Tag name interfaces of function blocks.....B3-14

B4. Override operation from HIS.....B4-1

B4.1 Overview of override FB.....B4-2

B4.2 Tag name interfaces and process alarms of override function blocks.....B4-4

B4.3 Overview of grouping override function block.....B4-8

B4.4 Tag name interfaces and process alarms of grouping override function block.....B4-12

B4.5 Status management of function blocks used for override.....B4-15

B4.6 Permission for override by password FB.....B4-17

B4.7 Tag name interfaces and process alarms of password function blocks.....B4-21

B4.8 Application for override.....B4-23

B5. Manipulation of manual operation function blocks from HIS.....B5-1

B5.1 HIS interfaces of MOB_11 and MOB_21 (BOOL-type data manual operation function block with answerback).....B5-3

B5.1.1 Manual operation permission function.....B5-8

B5.1.2 Password at manual operations.....B5-9

B5.1.3 The Output Enable status display function.....B5-11

B5.1.4 Answerback check function.....B5-12

B5.1.5 Monitoring IOP and OOP.....B5-16

B5.1.6 Tag name interfaces and process alarms of MOB_11 and MOB_21.....B5-17

B5.2 HIS interfaces of MOB_RS (auto-reset BOOL-type data manual operation).....B5-21

B5.2.1 Operations of MOB_RS from HIS.....B5-22

B5.2.2 Tag name interfaces and process alarms of MOB_RS.....B5-27

B5.3 HIS interfaces of MOA (analog-type data manual operation).....B5-29

B5.3.1 Operations of MOA from HIS..... B5-30
B5.3.2 Tag name interfaces and process alarms of MOA..... B5-33
B6. Data setting using external communication function blocks..... B6-1
B6.1 Confirmation of setting data..... B6-2
B6.2 Tag name interfaces of external communication function blocks..... B6-3
B7. Engineering for CENTUM integration..... B7-1
B7.1 Engineering on the SENG side..... B7-3
B7.1.1 Setting of SCS project property..... B7-4
B7.1.2 Defining alarm priorities..... B7-5
B7.1.3 How to change the display color of alarms..... B7-9
B7.1.4 Defining the alarm processing table..... B7-11
B7.1.5 Defining tag names..... B7-12
B7.1.6 Engineering for overriding from HIS..... B7-29
B7.1.7 Settings for exchanging data between FCS and SCS..... B7-32
B7.1.8 Accessing subsystem's data from CENTUM..... B7-34
B7.1.9 Plant hierarchy..... B7-36
B7.1.10 Saving and downloading operation marks..... B7-38
B7.2 Engineering on the CENTUM side..... B7-39
B7.2.1 SCS creation..... B7-40
B7.2.2 SCS taglist generation..... B7-43
B7.2.3 Other builders..... B7-45
B7.2.4 Items to note on CENTUM engineering..... B7-48
B8. Overview of safety system operation and monitoring using HIS..... B8-1
B8.1 Windows used for operation and monitoring of SCS..... B8-3
B8.1.1 System Alarm view..... B8-4
B8.1.2 Process Alarm view..... B8-7
B8.1.3 Instrument faceplates..... B8-10
B8.1.4 SCS Station Status Display view..... B8-15
B8.1.5 Adjust Time dialog box..... B8-25
B8.1.6 Software for Managing the Alarms..... B8-26
B8.2 Other functions used for operation and monitoring of SCS..... B8-27
B8.2.1 Equalizing..... B8-28
B8.2.2 Trend recording..... B8-29
B8.2.3 Security function of CENTUM..... B8-30
B8.2.4 Alarm inhibition (AOF)..... B8-31
B8.2.5 Chattering alarm suppression..... B8-33

Engineering Guide Vol. 2

IM 32P01C20-01EN 10th Edition

CONTENTS

PART-C SOE OPC Interface..... C-1
C1. Overview of SOE OPC Interface..... C1-1
C2. Setup for using the OPC server..... C2-1
C2.1 Settings of the SOE OPC Interface..... C2-2
C2.2 Overview of product security settings..... C2-5
C2.3 Operations after operation parameters are configured..... C2-9
C2.4 Connection with host system computer via an OPC server..... C2-10
C3. Setup for using the OPC client..... C3-1
C3.1 Settings using the setup tool and Windows account settings..... C3-2
C3.1.1 Preparations on the OPC server..... C3-3
C3.1.2 Operation procedure for the OPC client..... C3-4
C3.2 Security Settings..... C3-5

Engineering Guide Vol. 2

IM 32P01C20-01EN 10th Edition

CONTENTS

PART-D Subsystem communication..... D-1

D1. Common items regarding subsystem communication functions..... D1-1

D1.1 Overview of subsystem communication..... D1-2

D1.2 Dual-redundant communication..... D1-9

D1.2.1 Dual-redundant communication in ALR111 and ALR 121..... D1-10

D1.2.2 Dual-redundant communication in ALE111..... D1-12

D1.3 Error handling actions..... D1-15

D1.4 Setting items relating to subsystem communication..... D1-18

D1.4.1 Settings using the I/O Parameter Builder..... D1-22

D1.4.2 Settings using the Communication I/O Builder..... D1-28

D1.5 Engineering for subsystem communication modules..... D1-37

D1.6 Storage formats of subsystem data..... D1-42

D1.7 Troubleshooting..... D1-45

D2. Modbus communication (ALR111, ALR121)..... D2-1

D2.1 Communication specifications..... D2-2

D2.2 Connection of serial communication module and Modbus PLC..... D2-8

D2.3 Modbus PLC devices accessible from SCSs..... D2-10

D2.4 Builder setting items specific to Modbus PLCs..... D2-14

D2.4.1 Settings in the I/O Wiring View..... D2-15

D2.4.2 Items set in the I/O Parameter Builder..... D2-16

D2.4.3 Items set in the Communication I/O Builder..... D2-17

D2.5 Readback communication..... D2-20

D2.6 Recovery communication..... D2-25

D2.7 Communication text..... D2-27

D2.8 Communication time between serial communication module and Modbus PLC..... D2-29

D2.9 Precautions for engineering..... D2-31

D3. Modbus communication (for ALE111)..... D3-1

D3.1 Communication specifications..... D3-2

D3.2 Modbus/TCP PLC devices accessible from the SCS..... D3-5

D3.3 Builder setting items in the Modbus communication..... D3-8

D3.3.1 Settings in the I/O Wiring View..... D3-9

D3.3.2 Settings in the I/O Parameter Builder..... D3-10
D3.3.3 Settings in the Communication I/O Builder..... D3-13
D3.4 Actions during unsteady state.....D3-15
D3.5 Communication time between Ethernet communication module and Modbus/TCP PLC..... D3-17
D4. ProSafe-SLS communication (for ALR121)..... D4-1
D4.1 Operating environment.....D4-2
D4.2 System configuration..... D4-3
D4.2.1 Connection configuration of SCS and ProSafe-SLS.....D4-4
D4.2.2 System overview of ProSafe-SLS.....D4-5
D4.3 Data access..... D4-6
D4.4 Event acquisition..... D4-8
D4.5 Time synchronization..... D4-10
D4.6 Alarm notification.....D4-13
D4.7 Communication specifications..... D4-14
D4.8 ProSafe-SLS devices that SCS can access..... D4-16
D4.9 Communication time between communication module and CO-920..... D4-19
D4.10 Data types handled by the ProSafe-SLS communication function..... D4-21
D4.11 Message specifications..... D4-22
D4.12 Engineering flow and builders to be used.....D4-25
D4.13 Determining ProSafe-SLS data to be managed by ProSafe-RS.....D4-28
D4.13.1 Determination of data and event and diagnostic information of ProSafe-SLS to monitor.....D4-29
D4.13.2 Determining the time for time synchronization.....D4-30
D4.14 Engineering ProSafe-RS.....D4-31
D4.14.1 Preparation..... D4-32
D4.14.2 System engineering of ProSafe-RS.....D4-33
D4.14.3 Engineering to configure applications on ProSafe-RS.....D4-35
D4.15 Engineering for ProSafe-SLS.....D4-37
D4.15.1 Initial configuration required to operate CO-920.....D4-38
D4.15.2 Processing of events in CO-920..... D4-40
D4.15.3 Initial time setting of CO-920..... D4-41
D4.15.4 Engineering required to set the time by DI input.....D4-42
D4.16 Engineering for CENTUM..... D4-43
D4.17 Application Examples of the ProSafe-SLS communication function..... D4-44

Engineering Guide Vol. 2

IM 32P01C20-01EN 10th Edition

CONTENTS

PART-E Safety subsystem communication.....E-1

E1. Fire and gas communication..... E1-1

E1.1 System overview..... E1-2

E1.1.1 System configuration and components.....E1-3

E1.1.2 Structure of functions.....E1-6

E1.1.3 Operating environment..... E1-8

E1.2 Fire and gas communication function specifications..... E1-9

E1.2.1 Data I/O function of PROFINET.....E1-10

E1.2.2 PROFINET modules used with fire and gas communication..... E1-11

E1.2.3 FB to connect to PROFINET modules.....E1-16

E1.3 Safety communication of fire and gas communication.....E1-17

E1.3.1 Flow of data for the fire and gas communication I/O..... E1-18

E1.3.2 Data and status upon starting the SCS.....E1-20

E1.3.3 Functions and roles of the safety layer..... E1-21

E1.4 Monitoring of fire and gas communication.....E1-22

E1.4.1 Behavior when an error occurs.....E1-23

E1.4.2 Fire and gas communication status notification.....E1-27

E1.5 Engineering for fire and gas communication.....E1-29

E1.5.1 Creating a safety communication I/O list..... E1-33

E1.5.2 Applying settings by using PROFINET Configurator..... E1-34

E1.5.3 Applying settings after ending PROFINET Configurator.....E1-39

E1.5.4 Reflecting items onto the SCS project..... E1-42

E1.6 YFGW-PROFINET Configuration Support Tool.....E1-43

E1.6.1 Overview of YFGW-PROFINET Configuration Support Tool..... E1-44

E1.6.2 Using YFGW-PROFINET Configuration Support Tool..... E1-47

E1.7 Application logic for obtaining the gas concentration of GS01..... E1-53

E1.8 Precautions for engineering.....E1-57

E1.9 Error handling action.....E1-58

E1.10 Troubleshooting..... E1-59

Engineering Guide Vol. 2

IM 32P01C20-01EN 10th Edition

CONTENTS

PART-F Modbus slave communication.....F-1

F1. Common items regarding the Modbus slave communication function..... F1-1

F1.1 Overview of Modbus slave communication.....F1-2

F1.2 Data access using the Modbus communication functions..... F1-5

F1.3 Setting items relating to Modbus slave communication..... F1-7

F1.4 Definition of communication modules..... F1-8

F1.4.1 Definitions in I/O Wiring View.....F1-9

F1.4.2 Definitions in I/O Parameter Builder.....F1-10

F1.5 Definition of addresses of Modbus devices.....F1-11

F1.5.1 Definitions in Modbus Address Builder..... F1-12

F1.5.2 Window configuration of Modbus Address Builder.....F1-17

F1.6 Data setting using Modbus slave communication..... F1-20

F1.7 Messages communication.....F1-23

F1.8 Troubleshooting..... F1-31

F2. Serial communication modules..... F2-1

F2.1 Connection between the Modbus master and SCS.....F2-2

F2.2 Definitions in I/O Parameter Builder.....F2-6

F3. Ethernet communication modules..... F3-1

F3.1 Connection between the Modbus master and SCS.....F3-2

F3.2 Definitions in the I/O Parameter Builder.....F3-5

F4. Precautions for engineering.....F4-1

Engineering Guide Vol. 2

IM 32P01C20-01EN 10th Edition

CONTENTS

PART-G DNP3 slave function.....G-1

G1. Overview of the DNP3 slave function..... G1-1

G1.1 DNP3 communication system configuration and components.....G1-2

G2. DNP3 slave function of SCS..... G2-1

G2.1 Data access using the DNP3 slave function..... G2-2

G2.1.1 Referencing DNP3 data.....G2-4

G2.1.2 Setting DNP3 data.....G2-5

G2.1.3 Freeze command, Freeze & Clear command.....G2-8

G2.1.4 Response time.....G2-10

G2.2 Event buffering.....G2-11

G2.2.1 Event generation..... G2-12

G2.2.2 Event response.....G2-13

G2.2.3 Event deletion.....G2-14

G2.3 DNP3 function support for each data type..... G2-15

G2.4 Time synchronization..... G2-16

G3. Engineering and maintenance with SENG..... G3-1

G3.1 Enabled DNP3 slave function..... G3-2

G3.2 Definition of communication modules.....G3-3

G3.2.1 Definitions in I/O Wiring View..... G3-4

G3.2.2 Definitions in I/O Parameter Builder..... G3-5

G3.3 DNP3 slave setting.....G3-8

G3.4 Definition of instances for DNP3 communication FBs.....G3-11

G3.5 Definition of DNP3 data.....G3-12

G3.5.1 Window configuration of the DNP3 Communication Builder..... G3-13

G3.5.2 Definition in the DNP3 Communication Builder..... G3-15

G3.6 Creating an application logic.....G3-18

G3.7 Precautions for engineering..... G3-19

G3.8 Troubleshooting.....G3-23

Engineering Guide Vol. 2

IM 32P01C20-01EN 10th Edition

CONTENTS

Appendix

Appendix 1. Information regarding engineering for subsystems..... App.1-1

Appendix 1.1 Differences between safety subsystem communication I/O, subsystem communication I/O, and AIO/DIO modules I/O..... App.1-2

Appendix 1.2 Items of I/O Parameter Builder..... App.1-4

Appendix 1.3 Items of Communication I/O Builder..... App.1-5

Appendix 2. DNP3 field device Profile..... App.2-1

Appendix 2.1 Device properties..... App.2-2

Appendix 2.2 Capabilities for device database..... App.2-9

Appendix 2.3 Implementation table..... App.2-13

A. Configuring application

This section describes how to configure applications after design completion. Depending on the purpose, the following applications can be created:

- Application logic for implementing the safety system
- Applications that use safety communication between multiple SCSs
- Applications for event analysis that utilize SOE
- Applications that are integrated with CENTUM and CI Server

TIP

CI Server Integration Package also contains FAST/TOOLS Integration function. If FAST/TOOLS Integration is used, replace the term “CI Server” with “FAST/TOOLS” in the user's manual.

- Applications that connect with other systems that utilize Modbus communication and SOE OPC

When an application is created, you need to use Safety Analyzer to check the application that is created.

A1. Precautions for creating an application

This section describes the precautions to take when creating applications. Before creating the actual application, make sure you have read and understood the precautions.

Editing project files

Files in the SCS project folder must be edited only in the SCS Manager and AD Organizer.

Precautions for creating an application

You need to observe the following precautions when creating an application logic:

IMPORTANT

- A value must be set to each input parameter of a function (FU) or function block (FB). Also to each output parameter of an FU. They cannot be omitted.
- The data type of variables received by FU and FB must be in accord with that of input/output parameters in FU and FB.

- Arrays cannot be used in a program of a function block diagram (FBD) or ladder diagram (LD). When the Integrity Analyzer finds an array, an error will result.
- In the application logic, POU called from a program can have a hierarchy of up to 8 levels. If the hierarchy exceeds 8 levels, the Integrity Analyzer generates an error.
- Instance names connected in the hierarchy should be defined so as to have up to 80 characters.
- Four FBs (ANN, SOE_B, SOE_I, and SOE_R) are Interference-free. However, the Integrity Analyzer does not issue any alarms. As the four FBs do not have output parameters, using the FBs in FBD (Function Block Diagram) has no effects on the safety loop. On the other hand, these FBs have ENO output parameters when used in LD (Ladder Diagram) and thus make sure that they do not affect the safety loop.
- When looping the output of FU/FB back without using intermediate variables as shown in left of the following figure, a warning is issued at building. To avoid this, you should use a variable in looping back the output, specified in right of the following figure. You need to place the output variable on the right of FU/FB in the loop back.

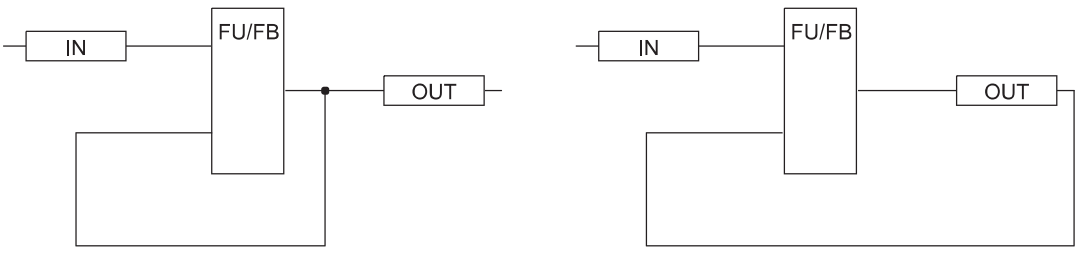


Figure A1-1 Example when a warning is output (left) and example when a warning is not output (right)

- Integrity Analyzer displays yellow warning icons if it detects Null functions of LD. Null functions refer to diagrams where one of the signals that branch out in a parallel coupling is directly connected and the value of the contact connected to the other line is ignored. In the example in the following figure, the value of the variable bIN is ignored.

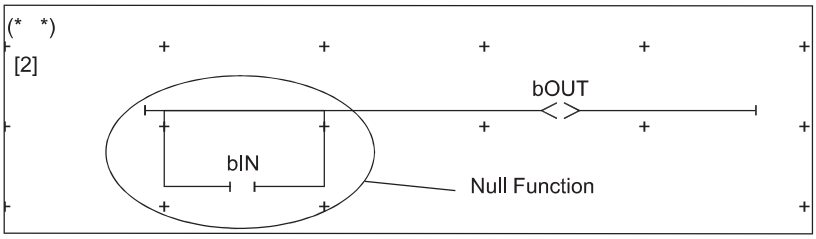


Figure A1-2 Example of Null function in LD

- An FB with a variable name assigned must not be called more than once. Be especially careful when you copy and paste an FB. For example, if the same REPEATTIMER is used in two programs, the timer may count at double-speed. If Integrity Analyzer detects one instance that is called multiple times, it raises a warning.
- If a calculation of equal (=) or Not equal (<>) is used for real numbers, the Integrity Analyzer will display a warning message.
- If variables of COM_BOOL type, COM_DINT type, or COM_REAL type undefined in Binding List View are used in POU, the Integrity Analyzer displays a warning message.
- At least one output parameter must be wired for function blocks that have no input parameter. Otherwise, such function blocks are not executed. The following FBs are appropriate: ECW_B, ECW_I, ECW_R, SYS_DIAG, SYS_IOALLST, SYS_TIME, SYS_ALARM, SYS_NETST, SYS_ESBINF, SYS_PSUDSP, SYS_CPUDSP, SCI_B, SCI_I, SCI_R, PSI_I, PSI_R, PNI_I, PNI_R, LTRCV, LTFCS.
- If you repeat building operations on the SCS Manager, the database size of SCS projects become larger. If the database size becomes too large, phenomena such as the build time becoming very long occur. In order to avoid this, execute [Compact Database] at an appropriate timing.

Precautions and actions to take when an abnormal calculation error occurs

IMPORTANT

If abnormal calculations such as division by zero, access to the outside of an array, overflow in floating-point calculation, and overflow in casting occur during POU execution, SCS behaves according to the specification made by [Behavior at Abnormal Calculation] in the SCS Constants Builder. If this specification is [SCS fails] (default), the SCS stops. If you specify [SCS continues], the SCS continues the operation without failing, but there is a potential risk that it cannot properly respond upon generation of a demand related to the corresponding POU while an abnormal calculation persists. Be sure to take measures to prevent abnormal calculations in applications and, if necessary, specify [SCS continues] just in case.

If SCS continues operating under the conditions where it cannot properly respond to related demands due to occurrence of abnormal calculation, the user must identify the condition immediately and take corrective measure to solve the error by modifying the application. If [SCS continues] is specified and an abnormal calculation occurs, the occurrence of error and the cause are notified to SENG and HIS via diagnostic information messages. Moreover, if you use the SYS_CERR function block, it is possible to output the abnormal calculation status to external devices by the application.

- If division by zero occurs in division of REAL- or DINT-type, SCS behaves according to the specification of [Behavior at Abnormal Calculation] in the SCS Constants Builder.
- If you specify a positive constant or 0 to an array index, index range check is performed at building and a build error will occur if the index points to the outsides of the array. On the other hand, if you specify a variable, expression, or negative constant for an array in-

dex, the range check is not performed at building. In this case, if access to the outside of the array occurs, SCS behaves according to the specification of [Behavior at Abnormal Calculation] in the SCS Constants Builder.

- If you convert floating point data to DINT with the ANY_TO_DINT function, SCS behaves according to the specification of [Behavior at Abnormal Calculation] in the SCS Constants Builder if the converted result is larger than the maximum value or smaller than the minimum value of integer-type data (that is, when an overflow occurs).
- Always use DINT-type for ANY_TO_TIME to restrict the value in the range from 0 to 86400000. If you enter a value outside this range, a correct TIME value cannot be obtained. In particular, if you specify a REAL value larger than 4294967295 (i.e., the maximum unsigned 32-bit integer) or a REAL value smaller than -2147483648 (i.e., the minimum signed 32-bit integer), SCS behaves according to the specification of [Behavior at Abnormal Calculation] in the SCS Constants Builder.

Note that, in the following cases, SCS continues the operations regardless of the specification of [Behavior at Abnormal Calculation] but the intended calculation result cannot be obtained.

- If you input 0 or less to LOG, a fixed value (-1E35) is output.
- If you input 0 or less as the denominator for MOD, a fixed value (-1) is output. In this case, there is no distinction from the case where -1 is obtained from the correct calculation.
- If an overflow occurs in calculation of integer values, the calculation result is not limited by the maximum value. Be sure to apply limits on the result of calculation if it is expected that the maximum value is exceeded.
- Be sure to specify the TIME-type value to less than 24 hours. No error occurs at building even if 24 hours is exceeded. Since the timer returns to 0 hours when it reaches 24 hours, it never reaches time beyond 24 hours. For example, if you set the timeout of TON to 25 hours, TON will no longer time out, which will be different from the intended operation.

SEE ALSO

For more information about considerations for calculation errors, refer to:

“■ Coding” in 3., “Guidelines for developing application logic” in POU Reference Manual (IM 32P03B20-01EN)

For more information about behavior of SCS upon calculation errors, refer to:

G2.1.3, “Behavior at abnormal calculation” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

A1.1 Creating an application logic

This section describes the definitions of variables and parameters, user-defined function blocks, and user-defined functions that are required when you create an application logic.

Definitions of variables and parameters

Use Dictionary View of SCS Manager to define I/O variables, internal variables and parameters used in an application logic.

It is possible to perform the following operations in Dictionary View.

- Creation and deletion of variables
  It is possible to create and delete variables used in application logics.
- Creation and deletion of parameters
  It is possible to create and delete parameters used in function blocks and functions.

You can define variables directly on the Dictionary View or by using the Safety I/O Editor of AD Suite and iDefine.

I/O variables can be defined by using AD Suite, while internal variables and FB instances can be defined by using iDefine.

Variables that are defined with AD Suite and iDefine are read-only on the Dictionary view and cannot be edited.

Variables defined using other tools will not be affected when reflecting variables that are defined with AD Suite and iDefine into the Dictionary view.

For example, after changing I/O variables using AD Suite and reflecting the values into the Dictionary View, internal variables and FB instances defined using iDefine and variables defined directly by the user on the Dictionary View are not changed.

Similarly, changing internal variables and FB instances defined using iDefine and reflecting the values into the Dictionary View does not change the I/O variables defined using AD Suite and the variables defined directly by the user on the Dictionary View.

SEE ALSO For more information about Dictionary View details, refer to:

"Dictionary View" in "Workbench" in the Workbench User's Guide

User-defined Function Blocks and user-defined functions

ProSafe-RS provides standard function blocks and functions such as "TON" and "AND" but the user can define customized function blocks and functions to implement a logic used commonly in several applications.

Function blocks and functions defined by users are called user-defined function blocks and user-defined functions, respectively.

User-defined function blocks and user-defined functions can be used in any programs, function blocks and functions in the same way as standard function blocks and functions.

You can define user-defined function blocks and user-defined functions by using the Multi-Language Editor or iDefine.

User-defined function blocks and user-defined functions that were created using iDefine cannot be edited in the Multi-Language Editor. Similarly, user-defined function blocks and user-defined functions that were created using the Multi-Language Editor cannot be edited in iDefine.

A1.2 Windows used to create application logic

You can create application logics by using the Link Architecture View of SCS Manager and Multi-Language Editor, or by using iDefine. Application logics that were created using iDefine cannot be edited in the Multi-Language Editor. Similarly, applications that were created using the Multi-Language Editor cannot be edited in iDefine.

SEE ALSO For more information about creating an application logic by using iDefine, refer to:

iDefine User Guide (PR03076-MAN-970_01)

Link Architecture View

You can create, remove or copy POUs in Link Architecture View of SCS Manager. You can change the execution order of POUs on the Link Architecture View. After reflecting the POU that is created by using iDefine, you can change the execution order, add and delete POUs that were created on the Link Architecture View as needed.

To show Link Architecture View, click the [Link Architecture View] on the toolbar of SCS Manager.

SEE ALSO For more information about Link Architecture View details, refer to:

"Link Architecture View" in "Workbench" in the Workbench User's Guide

Multi-Language Editor

Multi-Language Editor is used to create and edit application logics for SCSs using the following programming languages defined by IEC 61131-3.

The following three languages can be used in ProSafe-RS.

- Function block diagram (FBD)
- Ladder diagram (LD)
- Structured Text (ST)

A window for editing an FBD, a window for editing an LD and a window for editing an ST can be opened at the same time in one Multi-Language Editor. In order to create a new POU, select a language by selecting[Insert] > [Add Program], [Add Function], or [Add Function Block] menu in Link Architecture View. Multi-Language Editor automatically launches.

IMPORTANT

Do not use ST for creating Programs.

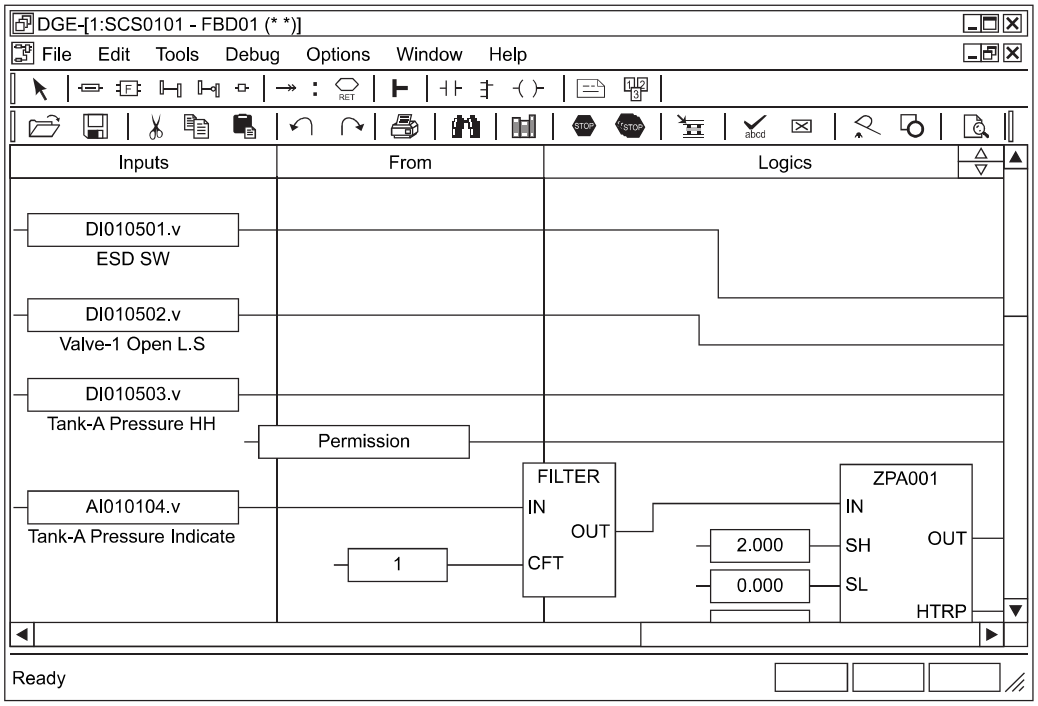


Figure A1.2-1 Multi-Language Editor window structure (example of editing an FBD program)

TIP

The scripts of FB and FU written in Structured Text are decorated with the following colors:

- Structured Text Statements of IEC 61131-3: Pink
- Numbers: Brown
- Comments: Green
- Other Texts: Black
  The background color can be changed. Click [Option] menu to open Customize dialog box. On the "Colors and Fonts" tab, choose the [ST editor] to change the background color. However, the color of texts cannot be changed.

Showing or hiding the toolbar in the Multi-Language Editor window is the same as that in SCS Manager.

POUs that were created using iDefine cannot be edited in the Multi-Language Editor. Similarly, POUs that were created using the Multi-Language Editor cannot be edited in iDefine.

SEE ALSO

For more information about showing or hiding the tool bar on the Multi-Language Editor window, refer to:

"■ Show/hide SCS Manager toolbars" in A10.2, "SCS Manager" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about Multi-Language Editor, refer to:

"Multi-Language Editor" in "Language Editor" in "Workbench" in the Workbench User's Guide

A2. Creating an application for the diagnostic function of the SCS

The SCS notifies the user of the status of the SCS in operation, the information on detected errors and on operations by the user. Monitoring the notified information enables the user to take appropriate actions. The SCS controls to bring the process to a safe state when the SCS detects an error in itself. The user is able to create applications for the diagnostic function of the SCS.

This section describes the following:

- Overall diagnostic function of SCS
- The SCS operations at fault detection that should be considered when creating an application for error detection

Overall diagnostic function of SCS

SCS has diagnostic functions for hardware and software.

When SCS detects an error by diagnosis, actions corresponding to the error are taken. A notification of the error appears in the Diagnostic Information Message and Status Display to alert the user.

Diagnosis for hardware

SCS carries out diagnosis with the following timing to check whether various types of hardware including I/O modules are in the normal state.

- At the start of the hardware.
- At specified periodical intervals during operation.

Diagnosis for software

SCS carries out diagnosis to check that the following actions of software are correctly performed.

- Task actions
- Application execution time

The following table shows an overview of actions when SCS detects an error by diagnosis.

Table A2-1 SCS actions on fault detection by SCS diagnosis

Fault level (*1)	Definition	Overview of SCS actions
Fatal error	Fatal hardware/software errors disabling continuous operation of the SCS.	CPU on both sides stops (SCS FAIL). Stopping CPU results in the change of output values of all output modules to the Output value at fault (All outputs shutdown) (*2)
Major error	This is not a fatal error that stops the CPU, but an error that disables some of the execution function of the application logic.	SCS performs an action against the error and notifies the application logic of the error state. In this case, creating an application by the user allows actions to be performed at the occurrence of an error (Shutdown actions (*2), and so on.) SCS notifies the user that an error occurs with diagnostic information message and the Status Display.

Continues on the next page

Table A2-1 SCS actions on fault detection by SCS diagnosis (Table continued)

Fault level (*1)	Definition	Overview of SCS actions
Minor error	Other errors • Error that have no influence on the application logic execution function itself, such as switching in redundant configuration • Errors related to functions not associated with the application logic execution functions • Operation mistakes by users	The application logic execution function continues. SCS notifies the user with diagnostic information message and the Status Display that an error occurs. Notification to the application logic depends on what kind of error occurs. When a module in a dual-redundant configuration fails, the failed module is regarded as FAIL state and switching-over to the stand-by is executed.

*1: Classification of error level
The SCS classifies the error level according to the result of error analysis, which determines the type of error that occurred, as well as the system state at which the error happened.
*2: Shutdown actions
Shutdown actions control output modules in appropriate conditions. There are three kinds of shutdown actions.
- The Shutdown that is operated with the logic that was created by user.
- Shutdown that makes CPU hold the output value in a failed channel.
- Shutdown of the output modules when they detect an error in communication with the CPU.
  When all output modules are shut down by stopping CPU due to a fatal error, this is called All Output Shutdown.

Actions on error detection

To keep the process in a safety state when an error is detected by the diagnosis of SCS, you need to understand the actions of the system in the case of error and design the safety application appropriately for the error levels.

Major SCS errors and actions of I/O modules against the error status are shown as follows.

They are very important issues in designing the safety applications.

Table A2-2 Actions on error detection

Failure location	Cause	Configuration	Actions	Fault level
CPU module	Hardware failure CPU node failure Software failure	Single	CPU stops. All output modules output the Output value at fault. (All output shutdown)	Fatal error
		Dual-redundant	CPU on failure side stops. The control is continued by switching the control right.	Minor error
Input module	Hardware failure	Single	The Input value at fault is set to all input channels of the module and data status changes to BAD.	Major error
		Dual-redundant	The control is continued by switching the control right.	Minor error
Input channel	Failure of Hardware for individual channel Failure on field side	Single (*1)	The Input value at fault is set to failed input channels and data status changes to BAD.	Major error
		Dual-redundant (*2)	When a failure is on the field side, the same action as the single configuration is performed.	Major error
			When a failure other than the above occurs, the control is continued by switching the control right.	Minor error
Output module	Hardware failure	Single	The output becomes 0 (*3) for all the output channels on the module, they are put in output disable state, and their data statuses change to BAD.	Major error
		Dual-redundant	The control is continued by switching the control right.	Minor error

Continues on the next page

Table A2-2 Actions on error detection (Table continued)

Failure location	Cause	Configuration	Actions	Fault level
Output channel	Failure of Hardware for individual channel Failure on field side	Single (*1)	When output shutoff switch works (*4), the output becomes 0 (*3) for all the output channels on the module, they are put in output disable state, and their data statuses change to BAD.	Major error
			Others except for the above case: Output value at fault is set to physical data of this channel and it is put in output disable state, and data status changes to BAD state.	Major error
		Dual-redundant (*2)	When a failure is on the field side, the same actions as the single configuration are performed.	Major error
			When a failure other than the above occurs, the control is continued by switching the control right.	Minor error

*1: When the module is in single configuration
*2: When the module is in dual-redundant configuration
*3: DO channel: FALSE AO channel: 0.0 [mA]
*4: This works if dangerous failure (DO module channel is fixed to ON) or failures requiring the protection of internal module (such as an overcurrent of AO module) occur. If you want to set the output shutoff switch to go on when dangerous failure requiring no protection of module occur, you can set the I/O parameter of the output module channel.

Considering application actions on fault detection

- In the logic of NC input like ESD application, etc, setting "the input value at the error occurrence" to FALSE permits the application logic to handle a failure of the input module as a demand and perform actions like shutdown.
- For De-energize To Safe (DTS) output in ESD application and so on, it is necessary to set the I/O Parameters for Output value at fault in order that the process is in a shutdown state when all the outputs become the Output value at fault.
- When a failure of an output module occurs, a shutdown action for different related output modules is required depending on the process. In this case, it is necessary to create the application logic to shut down the output of different related modules when the output channel data status changes into a BAD state.

SEE ALSO For more information about example of creation for an application logic which monitors the channel data status and performs a shutdown, refer to:

A4.2, “Shutdown due to channel failure” on page A4-7

For more information about procedures for setting I/O parameters, behavior of SCS upon occurrence of errors, and procedures for recovery, refer to:

G2., “Operations and recovery procedures during the SCS error occurrence” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Setting of parameters of I/O modules

This section explains the precautions to be taken when setting the parameters of an I/O module. When performing RS original engineering, you can set parameters by using I/O Parameter Builder. When performing I/O list engineering, you can specify the parameters by using AD Organizer.

Parameters of I/O modules include the specifications of actions on error detection. It is necessary to be careful when setting them.

Issues to consider when setting the parameters (by channel) of the Analog Input module (SAI143/L1AI143)

- Select two-wire or four-wire according to field devices for "Field power supply diagnosis." For all specified items for detection, the default settings are recommended.

- When two-wire or four-wire for Field power supply diagnosis is set, specify it to set pins on hardware for the current input module. In the case of different settings in the "Field power supply diagnostics" and hardware pins, the module will not start due to diagnosis error.

SEE ALSO For more information about parameters for each channel of the analog input module for current/voltage, refer to:

Appendix 1.3.2, “Settings for the AI channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Issues to consider when setting the parameters (by channel) of the Analog Input module (SAT145/L1AT145, SAR145/L1AR145)

Enter the Input Value at Fault, Threshold of the IOP (High) level, and the Threshold of the IOP (Low) level as % units. If the input signal is engineering data, convert the setting value from engineering data to a % unit based on the upper and lower range values.

Setting (%) = (Setting in engineering data - lower range value) / (upper range value - lower range value) x 100

Example:

When you select [Type K] for the Signal Conversion and select [C] for the Engineering Unit.

- The permissible range is -200 to 1200 deg. C.
- To set the Input Value at Fault to 900 deg. C, set (900 + 200) / (1200 + 200) x 100 = 78.6 %.

IMPORTANT

You must use the upper and lower range values of the I/O Parameter Builder. Be careful to ensure that you do not use the upper and lower scale values of Tag Name Builder. If you have set the upper and lower scale values to between 0 and 800 deg. C in Tag Name Builder, ensure that you do not specify the Input Value at Fault as a % unit corresponding to between 0 and 800 deg. C.

SEE ALSO For more information about parameters for each channel of the analog input module for thermocouple/resistance temperature detector, refer to:

Appendix 1.3.2, “Settings for the AI channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Issues to consider when setting the parameters (by channel) of the Analog Output module (SAI533/L1AI533)

- If the short circuit detection level is not properly set when the wiring resistance exceeds 50 Ω, the short circuit may not be detected on outputting the "Output Value at Fault" or the Tight-shut value. To avoid this problem, set properly the short circuit detection level with reference to the following information.
- The "Output Value at Fault" is output to the field exactly as it was set when the fault is detected. If you want to do Tight-shut or Full-open on fault detection, set the same value as the Tight-shut value or the Full-open value to the "Output Value at Fault." If the Tight-shut value or the Full-open value is changed, check if the "Output Value at Fault" should also be changed.

SEE ALSO For more information about Tight-shut/Full-open settings for conducting HART communication, refer to:

A9., “HART communication” on page A9-1

For more information about short circuit detection level settings, refer to:

“■ Command Line” in Appendix 1.3.3, “Settings for the AO channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about parameters for each channel of the analog output module, refer to:

Appendix 1.3.3, “Settings for the AO channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Issues to consider when setting the parameters (by module) of the Digital Input module (SDV144/L1DV144)

- When the software filter is set to 1, if an ON state is detected twice in the scan timing of the DI module, the input value is fixed to ON, and its value referenced by the application logic.
- When a software filter is set to 0, the PV value is effected noise. Ensure that the software filter is not set to 0.
- In addition to the software filter for making the input values, the DI module also has a filter to make SOE events. The filter for verifying the SOE events will be disabled if the software filter is set to 0 (no filter). If set to 1 or a bigger value, the digital filter will be 10 ms filter.
- If you have set Automatically Delete Noisy Event to [Yes] and more events than the specified number occur in the channel in the specified event time, the extra events are automatically deleted.

SEE ALSO For more information about parameters for each module of the discrete input modules, refer to:

Appendix 1.3.4, “Settings for the DI channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Precautions for setting channel parameters of Digital Input module

- The Wiring Check Adapter (SCB100) and a sensor switch must be connected in parallel to detect disconnection. When the check adapter is not installed, specify "No detection."
- The following setting is recommended as the disconnection detection value.
  - Specify "No detection of disconnection" (default) for NC (Normally Close) input.
  - Specify "Detection of disconnection" (Wiring Check Adapter is required to be installed.) for NO (Normally Open) input.
- Wiring Check Adapter(SCB110) and a sensor switch must be connected in series to detect a short circuit. When the check adapter is not installed, specify "No detection."
- For specifying the detection of a short circuit, the following settings are recommended. Specify "Detection of a short circuit" (default) for both of NC input and NO input.

  (Wiring Check Adapter need to be installed. For detecting both open and short circuits, while NO is selected, Wiring Check Adapters, both SCB100 and SCB110 are necessary.)
- In case of an NC input, to conduct a pulse test, the wiring check adapter (SCB110) and a sensor switch must be connected in series. When the input is NC and the check adapter is not installed, specify "No pulse test." In case of a NO input, a pulse test can be conducted without a check adapter.
- For a pulse test, the following settings are recommended.
  In case both of an NC input and a NO input, a pulse test should be conducted.(Default)

  (In the case of NC input, the wiring check adapter is required to be installed.)

SEE ALSO For more information about parameters for each channel of the discrete input module, refer to:

Appendix 1.3.4, “Settings for the DI channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Precautions for setting channel parameters of Digital Output module

- Set a proper value to the Output value at fault after carefully considering the operation of the application and the operation of the field in error condition.
- The following setting is recommended as the disconnection detection value.
  Specify "Detect Disconnection circuit" in both cases of DTS (De-energize To Safe) output and ETS (Energize To Safe) output (Default).
- For a pulse test on OFF, the following setting is recommended.
  Specify "Pulse Test" in both cases of DTS output and ETS output (Default).
- For a pulse test on ON, the following settings are recommended.
  - Specify "No pulse test" in the case of DTS output (Default).
  - Specify "Pulse Test" in the case of ETS output.

SEE ALSO For more information about parameters for each channel of the discrete output module, refer to:

Appendix 1.3.5, “Settings for the DO channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

A3. Creating an application for monitoring the status and process state of the SCS

The SCS status and process state can be monitored from SENG and HIS in CENTUM Integration structure.

In CENTUM Integration structure, HIS can monitor both CENTUM System and SCS.

It is possible to monitor faults in the system by annunciator panel.

This section describes the requirements for creating applications for monitoring process and system.

A3.1 Monitoring SCS status

The status of SCS can be checked on SENG and HIS. When a fault occurs in SCS, the fault can be located in a visual way.

Monitoring I/O data and application logic data

User can monitor I/O data and application logic data from SENG, HIS and external equipment via Modbus.

Notification of the SCS status with an external alarm panel

Creating the application logic of SCS makes it possible to output the data about SCS fault status to the external alarm panel so that the fault status can be informed to an operator.

It is recommended to put such alarm panel in a place where the operator can see the panel for continuous monitoring in order to monitor faults occurring in hardware of SCS.

When the occurrence of a fault in hardware is recognized on the external alarm panel, the detailed information on the fault is confirmed on the Diagnostic Information Window in SENG.

The following example shows the application logic to inform the fault status to the external alarm panel in SCS using a system function block.

An example of using the SYS_DIAG to output SCS fault status to an external Alarm panel

Diagnostic Information FB (SYS_DIAG) detects all system faults except user's operation mistakes. The following example shows how to use the SYS_DIAG to output system faults, I/O and control bus-related faults to an external Alarm Panel.

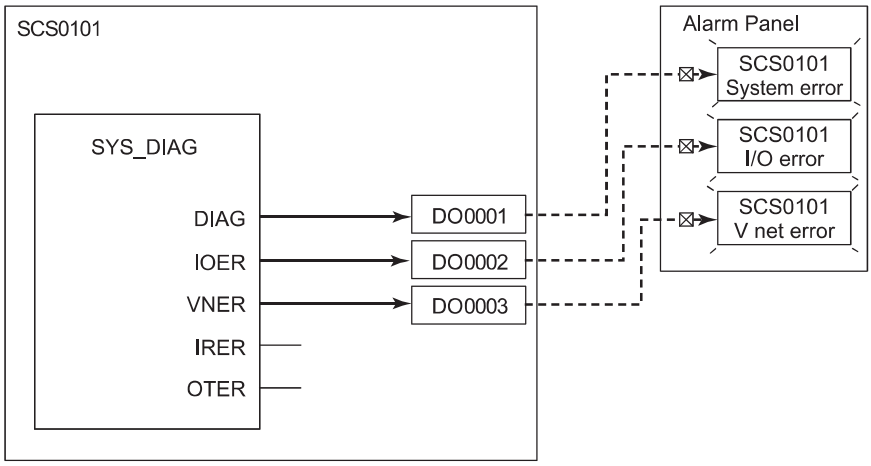


Figure A3.1-1 Example of the logic to output SCS fault status to external Alarm panel

SEE ALSO For more information about function details of the SYS_DIAG system function block, refer to:

11.7, "SYS_DIAG (diagnostic information output)" in POU Reference Manual (IM 32P03B20-01EN)

A3.2 Monitoring process with process alarm message and annunciator message

In CENTUM Integration configuration, information on a process state can be notified to HIS as a process alarm or annunciator messages from the application logic of SCS.

The process alarm and annunciator messages can be used as a pre-alarm before generating a trip in SCS. In the CENTUM system, they inform the operator that the appropriate action should be taken in the plant.

The following example shows the application logic to output a process alarm and annunciator message.

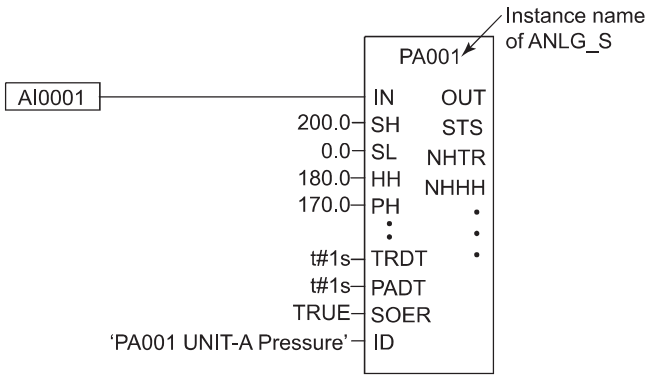


Figure A3.2-1 Example for the output of process alarm of analog input to HIS

Creating such an application logic and then setting a tag name for the instance name generates a mapping block for CENTUM integration. The mapping block allows alarm for the Analog input value (AI001) to be displayed as process alarm on HIS. Note that the alarm setting value (HH/PH/PL/LL) cannot be changed on HIS.

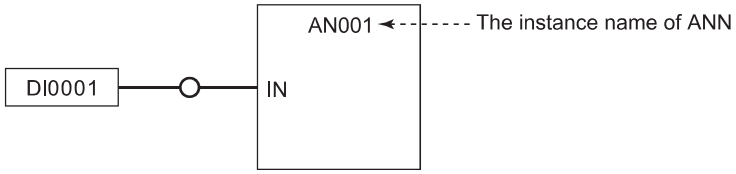


Figure A3.2-2 Example for the output of annunciator message to HIS

If you create ANN for such an application logic and define the annunciator message string in the %AN mapping element for the ANN instance name, the annunciator message appears on HIS.

A3.3 Fire and gas device application

This section gives an overview of the functions for fire and gas device applications, the SCSs that support the functions, and the function blocks for fire and gas devices.

Overview of functions for fire and gas device applications

ProSafe-RS has functions for applications that use fire and gas devices such as smoke detectors, heat detectors, gas detectors, and flame detectors.

For smoke and heat detectors, a device reset function and a function that suppresses alarms during device reset are provided, which are implemented by using the function blocks developed for them. For gas and flame detectors, a function block which has the function to manage the operation state of the device is provided.

SCSs that support the functions for fire and gas device applications

Each function for fire and gas device application functions is supported by the following types of SCS.

Table A3.3-1 SCSs that support the functions for fire and gas device applications

Function	Type of SCS supporting the function
Device reset function (N-IO)	S2SC70
Device reset function (FIO)	S2SC70, L1SC70, SSC60 , SSC50 , SSC57
Alarm suppression during device reset	S2SC70, L1SC70, SSC60 , SSC50
Function block for fire and gas devices	S2SC70, L1SC70, SSC60, SSC50 , SSC57

Function blocks for fire and gas devices

There are the two following types of function blocks for fire and gas devices:

- HSDTR (analog input function block for smoke and heat detectors)
  HSDTR is a function block for smoke detectors and heat detectors. We recommended that you use HSDTR when using the device reset function. If you create an application logic using HSDTR, you can reset a smoke or heat detector by manipulating the mapping block of HSDTR from the instrument faceplate on HIS, for example. It is also possible to suppress the system alarms for occurrence and recovery of channel errors that accompany reset, and suppress the IOP process alarm.
- GASDTR (analog input function block for gas and flame detectors)
  Even after detecting a field error, when the field returns to the normal state, gas and flame detectors output normal values according to the status of the field. For this reason, an external reset is not required. Some types of gas and flame detectors notify their own operation status by sending a value outside the range of process values. GASDTR has a function to manage such device operation status in three levels.

An override can be performed for HSDTR and GASDTR. We recommend that you perform an override in combination with the override function block (OVR_* and GOV_*).

SEE ALSO For more information about details of HSDTR, refer to:

5.17, “HSDTR (analog input function block for smoke and heat detectors)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about details of GASDTR, refer to:

5.18, “GASDTR (analog input function block for gas and flame detectors)” in POU Reference Manual (IM 32P03B20-01EN)

A3.4 Device reset function for smoke detectors and heat detectors

With smoke detectors and heat detectors (hereinafter referred to as devices), there is a type of device that retains the analog output as a value indicating the occurrence of an error when a field-side error is detected. With such device, unless the device is reset by turning the power OFF/ON, the status where the value indicating the occurrence of an error is retained will not be released. ProSafe-RS is equipped with a module that supports the function of resetting devices by once cutting off and then resuming the supply of power to the devices. By using this module, you can reset 2-wire type devices without setting up an external circuit. This function is referred to as the device reset function. However, in the case of a device powered from the outside, you cannot cut off/reconnect the power supply using this function. You need to use an external circuit.

This function is supported with both FIO and N-IO types of modules.

The reset can be performed with one of the following methods:

- From a window such as the instrument faceplate of HIS when using a CENTUM integration configuration
- From hardware such as an external button switch

The following figure shows a conceptual diagram of implementing a reset from HIS by using the FIO module.

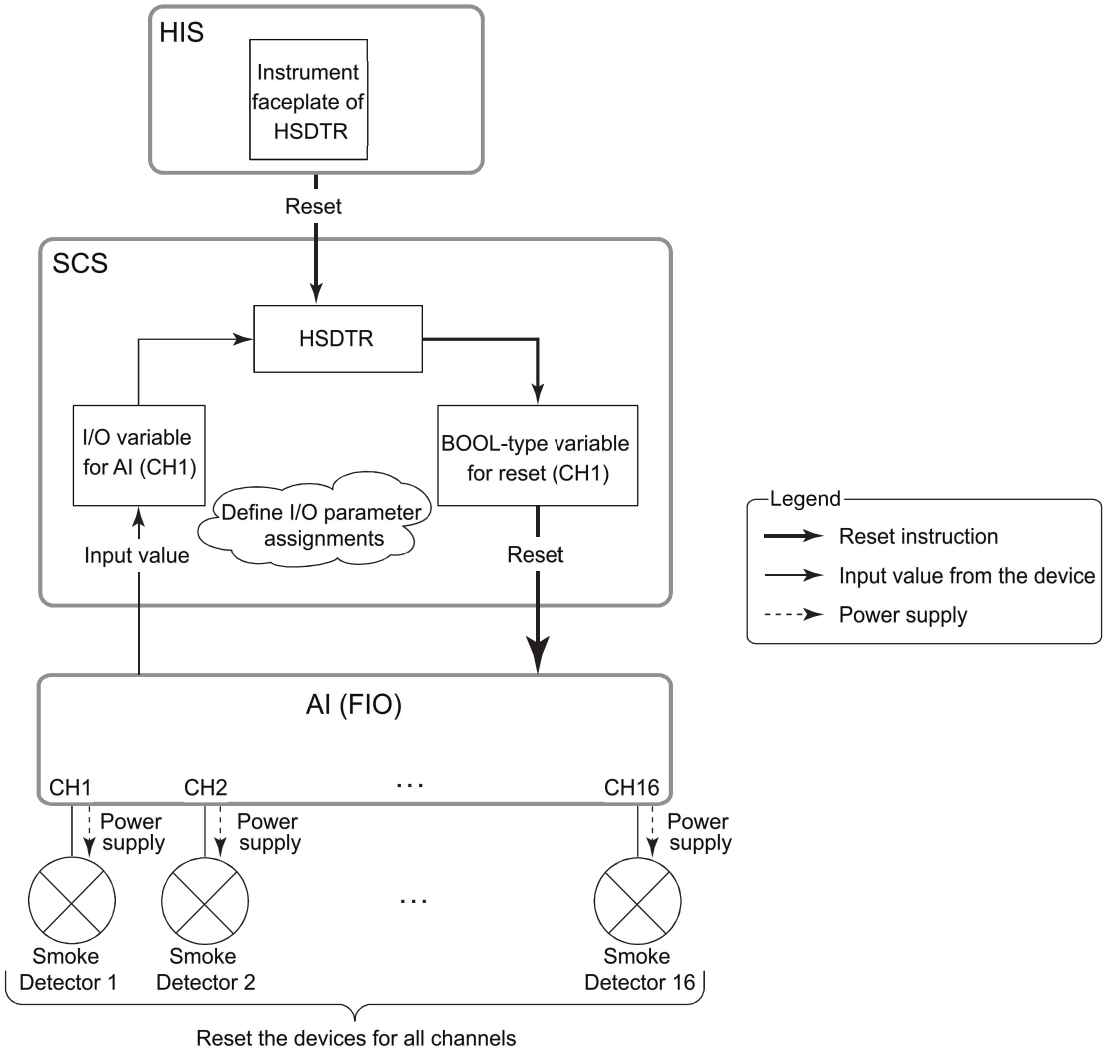


Figure A3.4-1 Example of implementing a reset from HIS by using the FIO module

TIP

This function does not apply to devices powered from outside. You must use an external circuit to reset such devices.

A3.4.1 Device reset function with FIO

This section explains the types of FIO modules supporting the device reset function, the behavior thereof, and precautions.

Modules subject to the device reset function

FIO modules that support this function are style S4 and later of SAI143-S and SAI143-H, and L1AI143-S and L1AI143-H. For SAI143-S and SAI143-H, the devices cannot be reset with modules earlier than style S4. For dual-redundant modules, make sure the both modules are style S4 or later. Only 2-wire type devices connected to the channels of 2-wire type settings are subject to this function.

TIP

If a module earlier than style S4 of SAI143-S or SAI143-H is used, the following behavior will take place when Device Reset Function (per module) is set to the I/O parameter of the module:

After startup of the module, a system alarm (No. 0749) will be generated, indicating that an error was detected in self-diagnosis. Also when the reset operation is performed, the system alarm for a self-diagnosis error (No. 0749) will be generated. The device will not be reset.

Behavior of reset

- When the reset operation is performed, all devices connected to the channels of the corresponding module will be subject to the reset.
- When the reset operation is performed, the module will stop, and therefore the supply of power to the devices will also be cut off. At this time, the logical data values on all input channels become the input value at error occurrence, which is set with the I/O parameter, and the data status will become BAD. Upon startup of the module, the supply of power to the devices is resumed and the devices will also start up.
- When the reset operation is performed, the input behavior of the module and the generation of alarms will follow the behavior of IOM Fail/Recover.
- When the modules are in dual-redundant configuration, the both modules will Fail/Recover. The control rights will not switch. When the modules stop, the ACT lamp of both modules will turn off.

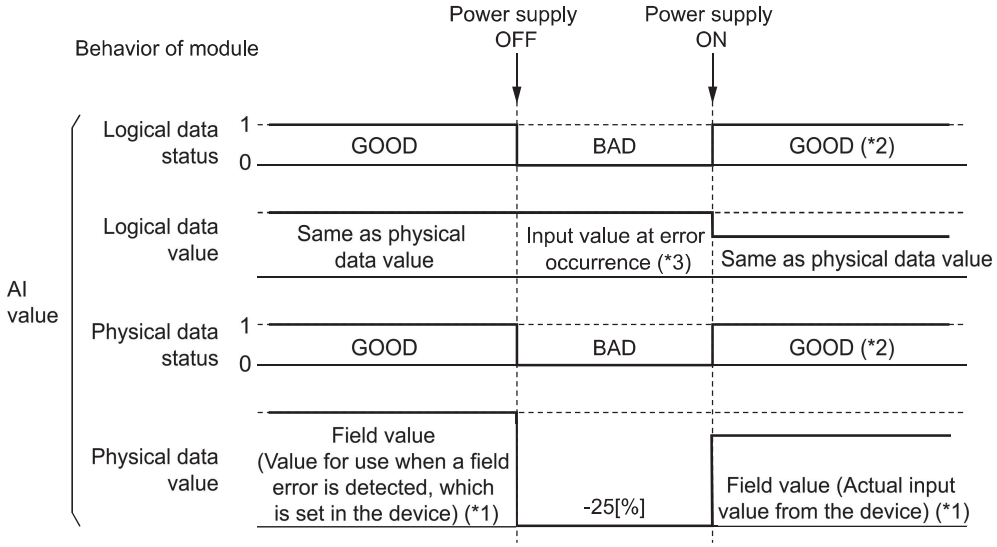
Behavior when channels of 2-wire and 4-wire settings are mixed

With SAI143-S/L1AI143-S and SAI143-H/L1AI143-H, behavior of the input of all channels is the same even when channels of 2-wire and 4-wire settings are mixed. However, because power is supplied externally with 3-wire and 4-wire devices connected to a 4-wire setting channel, it will not be possible to turn such devices OFF/ON by using the device reset function.

Change of input value upon reset operation: FIO

The input behavior of the module after turning the power supply OFF is the same as the behavior of IOM Fail/Recover. The data status will change in accordance with the IOP/TRNS detection specification set with the I/O parameters of the module. The following figures show examples where a device reset is performed after the field has recovered the safe state.

- When set to detect IOP/TRNS

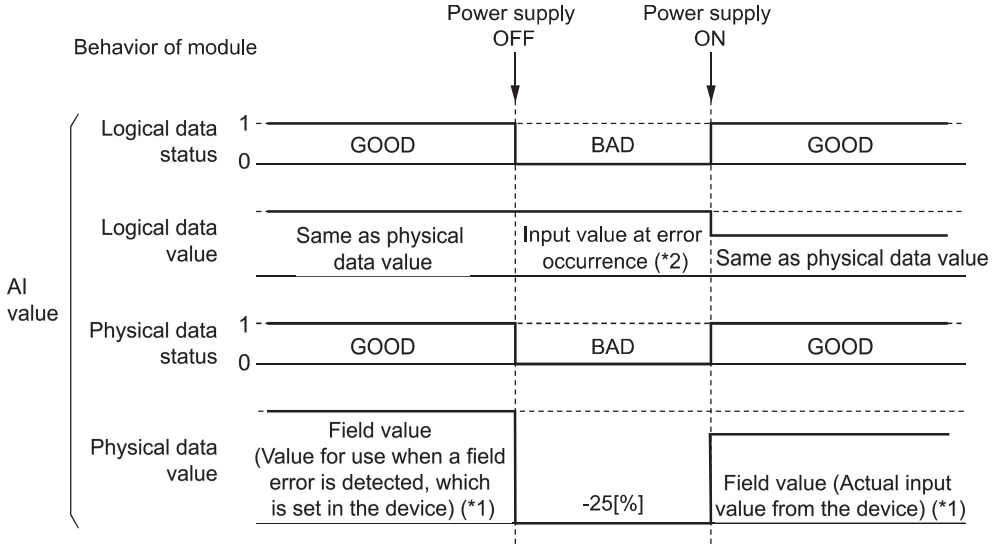


*1: The specific values vary with each device.
*2: The status changes according to whether the field value exceeds or falls below the upper or lower limit of IOP/TRNS.
*3: This figure assumes that [Input Processing at Fault] is set to [Hold] for the I/O parameter.

Figure A3.4.1-1 Input value from the device when set to detect IOP/TRNS

- When set to not detect IOP/TRNS

  Because of the setting to not detect IOP/TRNS, the data status after the supply of power is resumed is GOOD.



*1: The specific values vary with each device.
*2: This figure assumes that [Input Processing at Fault] is set to [Hold] for the I/O parameter.

Figure A3.4.1-2 Input value from the device when set to not detect IOP/TRNS

A3.4.2 Device reset function with N-IO

The device reset function can be used with devices connected to AI channels with 2-wire settings of the N-IO module S2MMM843. Reset of devices can be performed per channel.

IMPORTANT

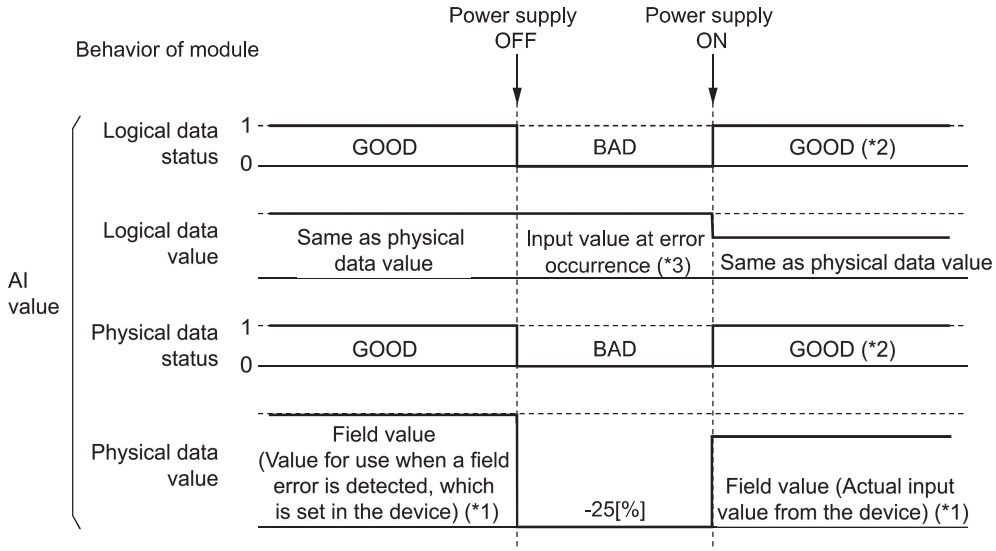
For devices with an intrinsic safety barrier, the barrier card powers 2-wire type devices. You must use an external circuit to reset such devices.

Change of input value upon reset operation: N-IO

The input operation for the AI value that is connected to devices varies depending on whether or not it is set that IOP/TRNS is detected with the I/O parameters of the module.

The following figures show the input values from the devices when IOP/TRNS is set to be detected or when it is not. The following figures show examples where a device reset is performed after the field has recovered the safe state.

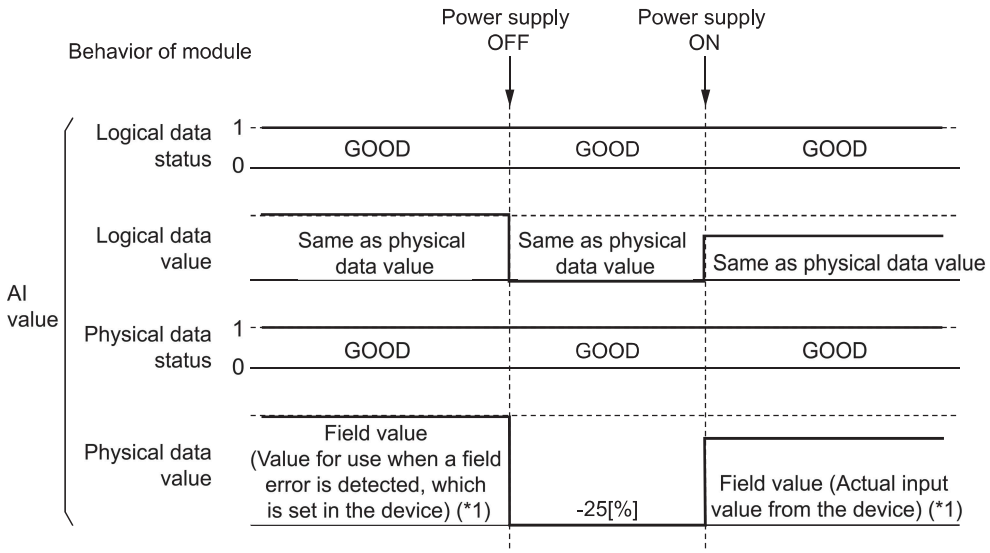
- When set to detect IOP/TRNS



*1: The specific values vary with each device.
*2: The status changes according to whether the field value exceeds or falls below the upper or lower limit of IOP/TRNS.
*3: This figure assumes that [Input Processing at Fault] is set to [Hold] for the I/O parameter.

Figure A3.4.2-1 Input value from the device when set to detect IOP/TRNS

- When set to not detect IOP/TRNS



*1: The specific values vary with each device.

Figure A3.4.2-2 Input value from the device when set to not detect IOP/TRNS

TIP

The behaviors of logical data status and logical data value from when the power supply is turned off until the power supply is turned on differ from those of FIO. With FIO, the power supply is turned off and on in module units, therefore it is accompanied by IOM Fail/Recover actions. With N-IO, the power supply is turned off and on for each channel.

SEE ALSO

For more information about IOP, TRNS, refer to:

Appendix 1.3.2, “Settings for the AI channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

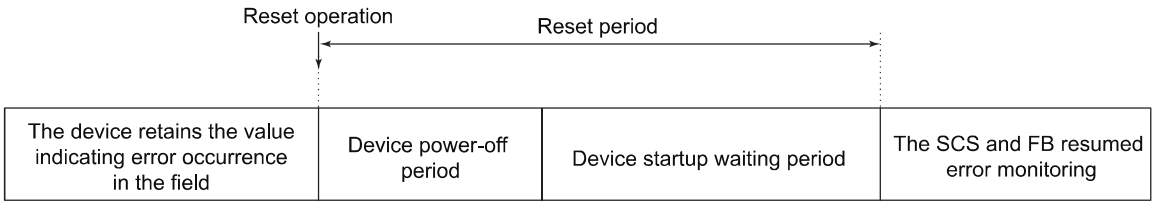
A3.4.3 Device reset function and alarm suppression during device reset

With the device reset function, multiple devices can be reset simultaneously. Also, the display of messages and the sounding of buzzers for system alarms and process alarms generated when a device is in the reset status can be suppressed.

- The reset group ID is an identifier for handling all the channels and HSDTR that are reset at the same time as being in the reset status. SCS manages the reset operation of multiple devices by reset group ID. Assign the same reset group ID to devices that are to be reset at the same time.
- The function to suppress alarms during device reset can be used in the following cases. However, process alarms can be suppressed only when using HSDTR.
  - When using the device reset function of FIO and the N-IO module
  - When using an external reset circuit
  - When using HSDTR
  - When creating an application logic without using HSDTR

■ Definition of reset period

The time from when the reset process is started up to when the power of the device is turned OFF/ON and SCS and FB resume monitoring of errors is referred to as the reset period. The definition of the reset period is shown in the following figure.



Reset period = Device power-off period + Device startup waiting period
Device power-off period: The time period during which the power supply to the device is stopped
Device startup waiting period: The time from when the power supply to the device is started until the SCS and FB resume error monitoring

It may take about one or two scan periods of time from when a reset operation is performed until the device is powered off.

Figure A3.4.3-1 Reset period

The Device Power-Off Period and Device Startup Waiting Period are values set by the user to suit the actual devices.

SEE ALSO For more information about how to set the device power-off period and device startup waiting period, refer to:

"■ Setting the I/O parameters" on page A3-14

■ Behavior of alarm suppression during reset period

When using alarm suppression during device reset, SCS and HIS will behave in the following manner during the reset period:

- When the occurrence of or recovery from an error is detected during the reset period, SCS notifies HIS with a system alarm to which an instruction to suppress messages is attached.

- HIS follows the instruction from SCS and suppresses the display of messages and the sounding of buzzers for system alarms.
- SCS only notifies HIS of the suppression of messages and still detects the occurrence of and recovery from errors during suppression.
- The mapping block of HSDTR uses the function of AOF to suppress the display of process messages and the sounding of buzzers during the reset period.

IMPORTANT

When a device is reset while in the status where a system alarm for No. 0081 IOM Fail or No. 4125 Channel Error has been generated, the alarm will remain displayed even if such error is recovered during the reset period. Because of still being in the reset period, a system alarm for recovery will not be displayed.

After the reset period ends, use the SCS Status Display view of HIS to confirm the status of the I/O module and channel. If the status has been recovered to the normal status, manually delete the system alarm for No. 0081 IOM Fail or No. 4125 Channel Error.

In the following cases, alarms that were suppressed during the reset period will be sent again after the reset period ends:

- System alarms and process alarms that were generated during the reset period but were not recovered by the end of the period will be sent again with the next scan after the reset period has ended.
- In order for process alarms to be sent again, setting is required with SCS Constants Builder.

SEE ALSO For more information about how to set SCS Constants Builder, refer to:

"■ Setting the SCS constants" on page A3-14

Display of alarms subject to alarm suppression

The types of alarms suppressed during the reset period are as follows:

Table A3.4.3-1 Type of alarm subject to suppression

System alarms (*1)	Process alarms
• No. 0081 IOM Fail (*2) • No. 0082 Recover (*2) • No. 0459 IOM In Service (*2) • No. 0460 IOM Out Service (*2) • No. 4125 Channel Error • No. 4126 Channel Recover	All process alarms of the mapping block of HSDTR performing the reset process

*1: These alarms, even when generated during the reset period for a reason other than that of the reset, will be subject to suppression.
*2: Alarms subject to suppression only when the device reset function (per module) is enabled using SAI143/L1AI143.

With HIS, the display of alarms subject to the function are suppressed. This is the same with CAMS for HIS. With CAMS for HIS, historical data subject to suppression is displayed as events. In the instrument faceplate corresponding to the mapping block of HSDTR, AOF is displayed and tag marks are displayed in blue.

System alarms subject to alarm suppression are communicated to the OPC clients as logging alarms. Whether logging alarms are displayed will depend on the settings of the OPC client.

The following items will not be affected by the alarm suppression function:

- Historical message report window of HIS

- Alarm status
- SCS station status display view of HIS
- SOE viewer
- SCS maintenance support tool of SENG
- Diagnostic Information window of SENG
- System function block SYS_IOALLST

Behavior of HSDTR

The instance of HSDTR receiving the reset request will behave as follows during the reset period:

- System alarm No. 4207 for notifying the reset operation will be generated.
- TRUE (Occurred) is output to POFF for the specified device power-off period and once the device power-off period has elapsed, FALSE is automatically output.
- With the instance receiving the reset request and all instances to which the same reset group ID as that instance has been set, HTRP will be FALSE during the reset period. STS will be GOOD.

The mapping block of HSDTR will behave as follows with HIS during the reset period:

- A value according to the input value from the field will be reflected onto the alarm status of the mapping block.
- The block status of the mapping block will become RST (reset status).
- When alarm suppression during device reset is enabled, the display of messages and the sounding of buzzers for process alarms are suppressed.

IMPORTANT

In order to link the behavior of field devices with the behavior of FB, match the value of the argument HH of HSDTR with the setting value of the devices. HH is an argument for specifying the HI trip level.

SEE ALSO For more information about details of HSDTR, refer to:

5.17, “HSDTR (analog input function block for smoke and heat detectors)” in POU Reference Manual (IM 32P03B20-01EN)

A3.4.4 Engineering regarding the device reset function and alarm suppression during device reset

In order to use the device reset function and alarm suppression during device reset, perform settings with SCS Constants Builder and set the I/O parameters for the modules and channels.

■ Setting the SCS constants

Perform the following settings with SCS Constants Builder when using the device reset function and alarm suppression during device reset.

Perform the settings that decide the reset period. The reset period is a parameter used by the SCS when performing the reset process of devices and when suppressing alarms during the reset period. As this value is decided per station, decide the value in consideration of the behavior of all field devices that will actually be used.

- Device power-off period
  Set the time for which TRUE is output to the POFF of HSDTR. Set a time by which all devices connected to the corresponding station will surely come to a stop.

  Set the value to [Device Power-Off Period] of the [SCS] tab.
- Device startup waiting period
  Set the time from when the supply of power to the device is resumed to when the device completes normal startup. Set a time that suits the device that takes the greatest amount of time for startup among the devices connected to the corresponding station.

  Set the value to [Device Startup Waiting Period] of the [SCS] tab.

In order to use alarm suppression during device reset, under the [SCS] tab, set [Alarm Suppression During Device Reset] to [Enable].

To use HSDTR and resend process alarms not recovered during the reset period, under the [Communication] tab, set [Alarm Notify Action when AOF Released] to [Yes].

SEE ALSO For more information about definition of reset period, refer to:

"■ Definition of reset period" on page A3-11

■ Setting the I/O parameters

The following is a setting example of the I/O parameters with I/O list engineering. The necessary settings are different depending on the modules being used and the function to be used. The following table shows the relationships between the functions to be used (column) and necessary setting items (row).

Table A3.4.4-1 Setting items necessary for use of each function for smoke detectors and heat detectors

	Device reset function	Alarm suppression during device reset	HSDTR
I/O parameter of the module	Setting required with SAI143/L1AI143	-	-
BOOL-type variable for reset to the channel	Setting required with SAI143/L1AI143 and S2MMM843	Setting required with SAI143/L1AI143, SAV144/L1AV144, and S2MMM843	Setting required with SAI143/L1AI143, SAV144/L1AV144, and S2MMM843
Reset group ID for the channel	Setting required with SAI143/L1AI143 and S2MMM843	Setting required with SAI143/L1AI143, SAV144/L1AV144, and S2MMM843	Setting required with SAI143/L1AI143, SAV144/L1AV144, and S2MMM843

Setting procedures

- Setting the I/O parameter of the module
  With IOM Definition Editor, set [Device Reset Function (per module)] of the module's I/O parameter item to [Enable].
- Setting the BOOL-type variable for reset to the channel
  With Safety I/O Editor, set a BOOL-type variable for reset to [Device OFF-ON Variable Name] for the channel to which the device subject to the reset will be connected. For this BOOL variable, create application logic so that the device power OFF/ON command is input from the function block.
- Setting the reset group ID for the channel
  With Safety I/O Editor, set the reset group ID to [Reset Group ID] of the channel to which the device subject to the reset will be connected. Set a value in the range of 1 through 1000.

Precautions when setting the reset group ID

- When there are multiple devices to be reset at the same time, set the same reset group ID to all channels to which such devices are connected. This is necessary in order to handle channels to be reset at the same time as being in the reset status.
- Even for channels for which devices will be reset independently, be sure to set a reset group ID that is unique within the range of the same SCS.
- When using HSDTR, set the reset group ID that you set as the I/O parameter for the connected channel to the argument RID of the HSDTR that corresponds to the device.

TIP

Set the reset group ID of the channel to 0 when not using alarm suppression during device reset nor HSDTR. The default value is 0.

Example of application logic

The following figure shows an example of application logic where HSDTRs are used to monitor and reset the smoke detectors or heat detectors that are connected to all channels of SAI143. The device reset function and alarm suppression during device reset are used. The application logic should be created as follows:

- The BOOL-type variable for reset is connected to POFF of HSDTR.
- The same reset group ID as that which has been set to CH1 through CH16 of the module is set to RID of HSDTR01 through HSDTR16. In this example, the reset group ID is set to 1.

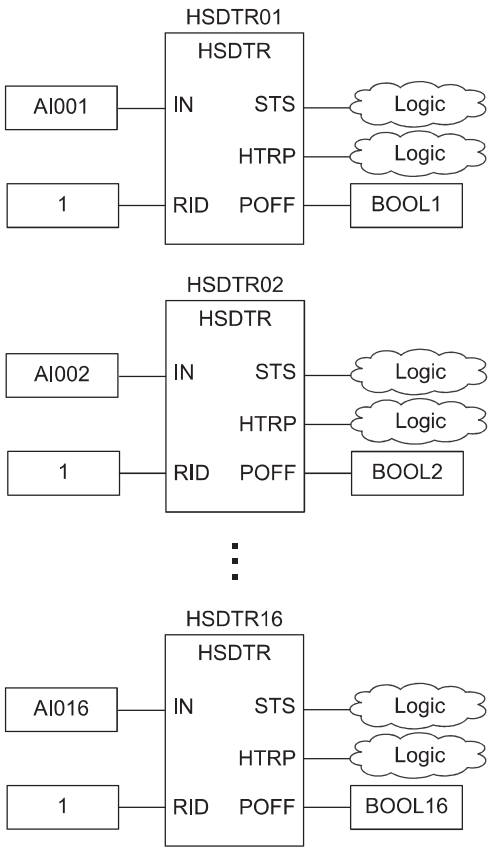


Figure A3.4.4-1 Example of application logic for monitoring and resetting smoke and heat detectors

In this example, Device Power-Off Period is set to 3 seconds and Device Startup Waiting Period is set to 20 seconds. The reset period is 3 + 20 = 23 seconds.

Behavior of the example application logic

This section explains the behavior from when a field-side error is detected with HSDTR01 that is connected to CH1 of SAI143, followed by starting of a device reset after recovery of the safe state in the field, up to when the reset period ends. The following behavior of 1 through 3 corresponds to 1 through 3 shown in the top part of the following figure “Behavior from error occurrence on field-side to the end of the reset period.”

1. With HSDTR01, when the status where the value of OUT is larger than HH continues for at least the time specified with TRDT, TRUE is output to HTRP. The status of HTRP being TRUE will remain latched until the reset process is started.

   It is assumed that at this time, with HSDTR02 through HSDTR16, OUT is equal to or less than HH in the normal status and FALSE is being output to HTRP.

2. The following behavior will take place during the reset period:

   - HSDTR01 generates a system alarm for notifying the reset operation.
   - HSDTR01 outputs FALSE to HTRP.
   - HSDTR01 starts the testing of whether the conditions for FALSE are established with HTRA and reflects the results thereof onto the alarm status of the mapping block. If the device has a function to retain the value indicating a field-side error, TRUE is output to HTRA because the conditions for FALSE are not established with HTRA.
   - Instance HSDTR01 receiving the reset request and instances to which the same reset group ID as this instance has been set (HSDTR02 through HSDTR16) will output GOOD to STS.

- HSDTR01 will communicate an instruction to turn the power of the device OFF/ON to the input module through a BOOL-type variable for reset. As the reset will be performed per module, the power of the devices connected to CH2 through CH16 will also be turned OFF/ON.
  As the time for shutting off the power supply to the device is the Device Power-Off Period, this is 3 seconds.
- During the reset period, process alarms are suppressed for instance HSDTR01, which receives the reset request, and the instances (HSDTR02 through HSDTR16), which have the same reset group ID as HSDTR01. Also, system alarms for channels to which the same reset group ID has been set will also be suppressed. In this example, the duration is 23 seconds from the start of the reset.
- HSDTR01 through HSDTR16 will not perform testing of whether the conditions for TRUE are established with HTRP. HSDTR01 through HSDTR16 will constantly output TRUE (GOOD) to STS.
- When the channel is set to detect IOP/TRNS, until the output of the device exceeds the TRNS- detection value, an input value at error occurrence will be input as the logic data value. Also, at the same time, BAD will be input as the logic data status and BAD will be output to STSR. When the output value of the device exceeds the TRNS- detection value, OUT will become the output value of the device.

3. When the reset period ends, HSDTR01 through HSDTR16 will resume the testing of whether the conditions for TRUE are established with HTRP and output the result to HTRP. HSDTR01 through HSDTR16 will again output IN.status to STS.

TIP

When the status where the input to the channel of SAI143 is equal to or less than the TRNS- detection value continues even after the reset period has ended, a system alarm for Ch Fail and a process alarm for IOP will be sent again.

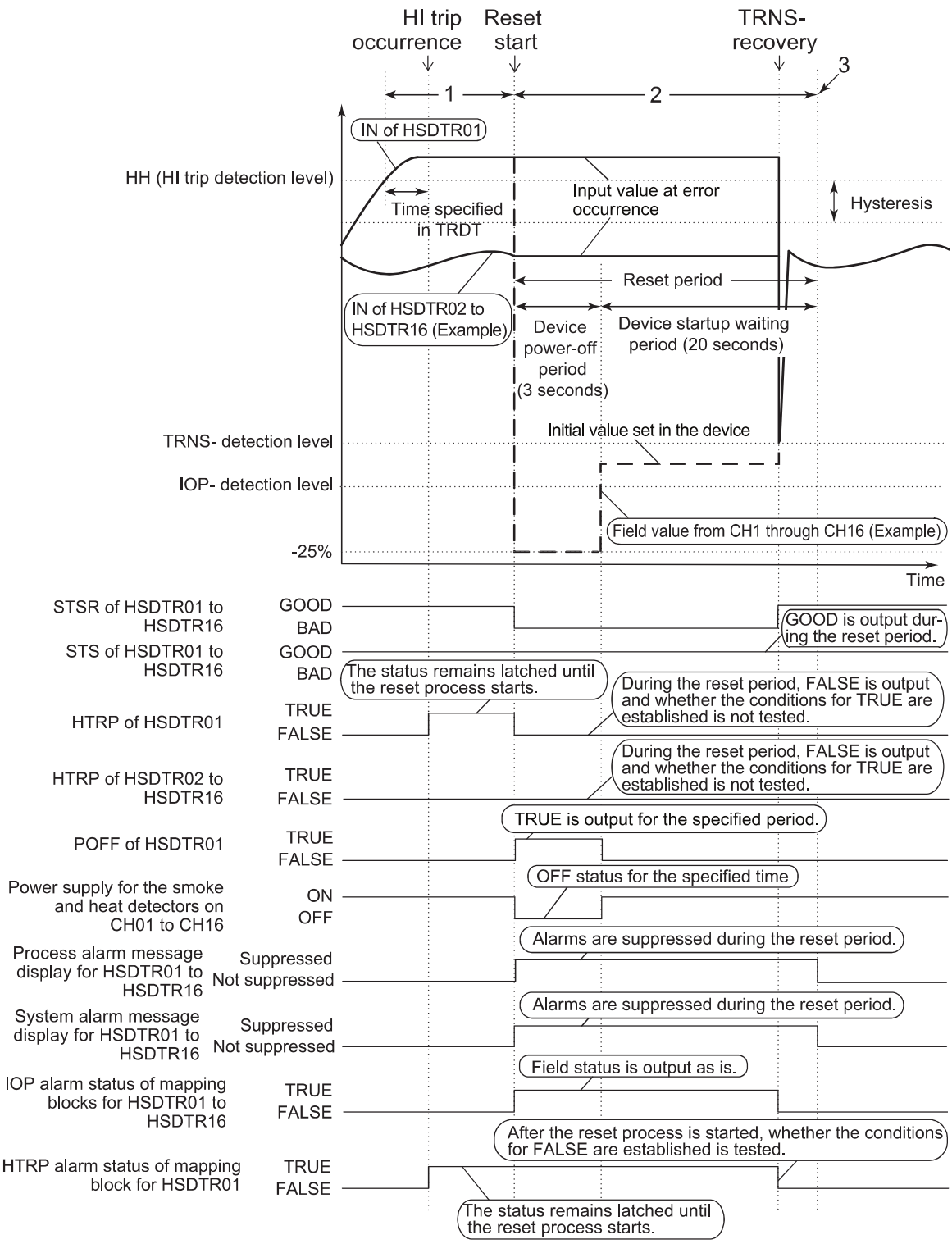


Figure A3.4.4-2 Behavior from error occurrence on field-side to the end of the reset period

A3.5 Utilization of override when performing maintenance of fire and gas devices

By combining the override function block with HSDTR or the GASDTR function block, it is possible to use the override function when performing maintenance of fire and gas devices. The following shows an example of HSDTR.

IMPORTANT

If a device connected to a channel of SAI143/L1AI143 is reset while override operation is being performed, the supply of power to the module will be shut off and then resumed. Because of this, all the channels of SAI143/L1AI143 having the channel that received the reset request will be reset. You must provide countermeasures in advance in order to prevent unintended operation of the devices that will be reset together.

Example of creating an application logic to enable override

Connect OVR_B to HSDTR.

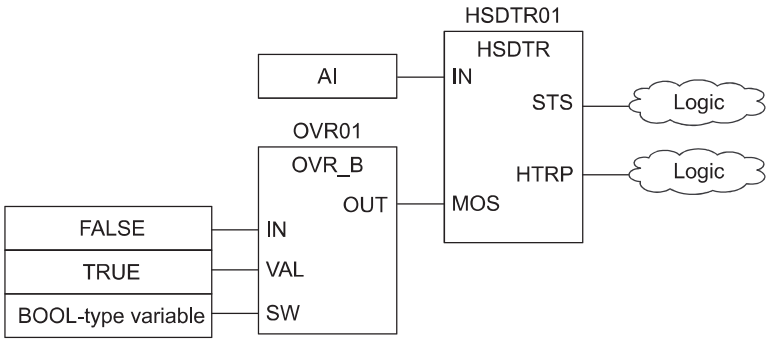


Figure A3.5-1 Example of connecting an override function block

Override operation procedure and behavior of the targets of operation

This section describes the procedure for override operation and the behavior of the targets of operation.

1. Set the BOOL-type variable connected to the SW of OVR01 to TRUE to allow override.
2. Start the override operation through OVR01 from the instrument faceplate on HIS.
   - System alarm No. 4115 for the override setting will be generated. The tag name displayed in the system alarm is the tag name defined for OVR01.
   - A process alarm indicating the override status will be generated from the mapping block of OVR01.
   - The alarm status of the mapping block of OVR01 will change to OVR.
   - The block status of the mapping block of HSDTR01 will change to OVR and process message No. 1405 for a change of the block status will be generated.
3. The behavior of HSDTR01 before and after the start of override is described as follows for each device status:
   - If override is started when the device is normal, HSDTR01 will continue to output FALSE to HTRP and TRUE to STS.

- If the device has detected a HI trip before override is started, HSDTR01 will output TRUE to HTRP and TRUE to STS. After override is started, HSDTR01 will output FALSE to HTRP and TRUE to STS.
- If the device has become faulty before override is started, the output values of HTRP and STS will depend on the type and fault status of the device and how the device has been engineered. However, after override is started, HSDTR01 will output FALSE to HTRP and output TRUE to STS.

TIP

During the override status, the value of HTRA and the alarm status of the mapping block of HSDTR01 will change in accordance with the value input to HSDTR01.

4. HSDTR01 and the mapping block thereof will behave in the following manner with operations during the override status:
   - When a device is removed for the purpose of replacement, etc. during the override status, the behavior will be as follows:
     - The input value to HSDTR01 will be an input value at error occurrence and the data status will change to BAD when the channel is set to detect IOP/TRNS. HSDTR01 will output FALSE to HTRP and output TRUE (GOOD) to STS.
     - The alarm status of the mapping block of HSDTR01 will follow the input value to HSDTR01.
   - When a reset operation is performed for HSDTR01 from the instrument faceplate of HIS or an external switch during the override status, the behavior will be as follows:
     - Due to being in the override status, HSDTR01 will continue to output FALSE to HTRP and output TRUE (GOOD) to STS.
     - During the reset period, HSDTR01 and the mapping block thereof will behave as they would during the reset period.
     - During the reset period, on HIS, the block status of the mapping block of HSDTR01 will be displayed not as OVR but as RST.
5. When maintenance of the device is finished, confirm that the input to HSDTR01 has recovered to the normal status and end the override operation through OVR01 from the instrument faceplate on HIS.
   System alarm No. 4116 for the cancellation of override will be generated.
6. Set the BOOL-type variable connected to the SW to FALSE to prohibit override.

A4. Example of creating an application logic

In ProSafe-RS, an application logic is created by combining programs, function blocks and functions.

Programs, function blocks and functions are referred as POU for a generic name. You can create POUs by using the Link Architecture View of SCS Manager and Multi-Language Editor, or by using iDefine. POUs that were created using iDefine cannot be edited in the Multi-Language Editor. Similarly, POUs that were created using the Multi-Language Editor cannot be edited in iDefine.

How to define POUs is described as follows:

- Program
  Implemented by combining variables, function blocks and functions
- Function block
  Implemented by combining input/output parameters, internal variables, function blocks and functions
- Function
  Implemented by combining input/output parameters and functions

SEE ALSO

For more information about precautions when creating an application, refer to:

A1., “Precautions for creating an application” on page A1-1

For more information about overview of POU, refer to:

1., “Overview of POU” in POU Reference Manual (IM 32P03B20-01EN)

For more information about creating an application logic by using iDefine, refer to:

iDefine User Guide (PR03076-MAN-970_01)

A4.1 Use of analog input value

Analog input modules include modules to handle current and voltage and modules to handle data from a thermocouple (TC) and Resistance Temperature Detector (RTD). Modules to handle input from TC or RTD hereinafter called TC/RTD input module.

Input signals input to the current/voltage input module are normalized and passed to the application logic in the form of 0.0-100.0% data. The user can convert this data into engineering data in the application.

Input signals input to the TC/RTD input module are passed directly to the application logic in the form of engineering data.

The following shows an example of application logic for comparison between an analog input value and a constant value.

Example 1: Application logic using the analog input values of the Current/Voltage Input module

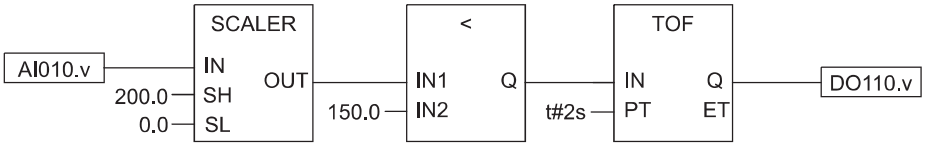


Figure A4.1-1 Example 1: Using current/voltage analog input value

In example 1 above, only Analog values are input. These are then converted to values in engineering units for comparison. If the Analog input value is larger than the reference value (150.0) for the specified period of time in Off Delay Timer (2 s), output is turned OFF.

Example 2: Application logic using the analog input values of the Current/Voltage Input module

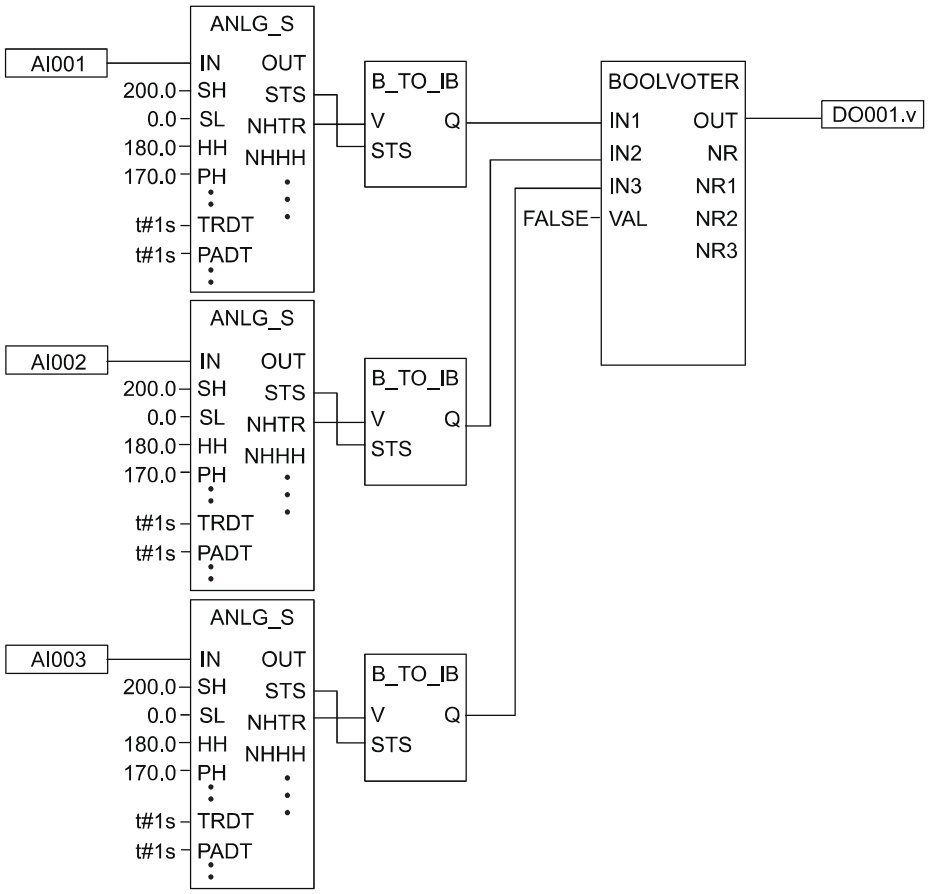


Figure A4.1-2 Example 2: Using current/voltage analog input value

In example 2, each of the three analog inputs is scale-converted by each ANLG_S and output. 2oo3 (2 out of 3) Voting result of the Trip outputs (NHTR) or a Fail-safe value is output as DO. Each ANLG_S produces a Trip output when the input value exceeds the Trip limit value for the period that is set in Off-Delay Timer (TRDT = 1 s in Example 2).

Example 3: Application logic using the analog input values of the Current/Voltage Input module

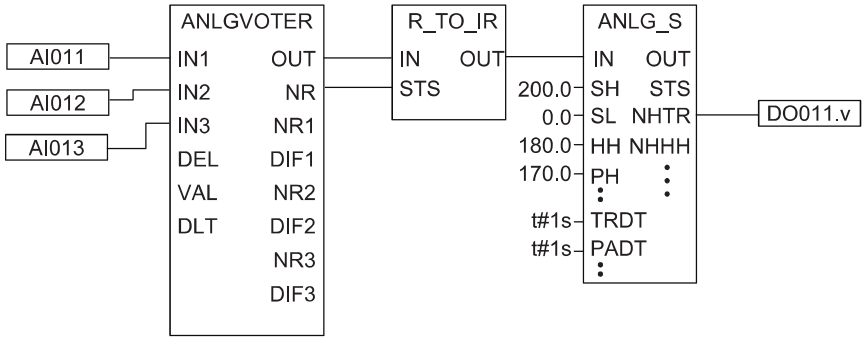


Figure A4.1-3 Example 3: Using current/voltage analog input value

The ANLGVOTER gets an intermediate value of analog inputs or a fail-safe value. The R_TO_IR converts the value to IO_REAL type and inputs it to the ANLG_S. The ANLG_S out-

puts the Voting result and Hi-Trip (NHTR). The ANLG_S produces a Trip output when the input value exceeds the Trip limit value for the period that is set in Off-Delay Timer (TRDT = 1 s in Example 3).

Example of application logic using the analog input values of the Thermocouple/Resistance Temperature Detector(TC/RTD)

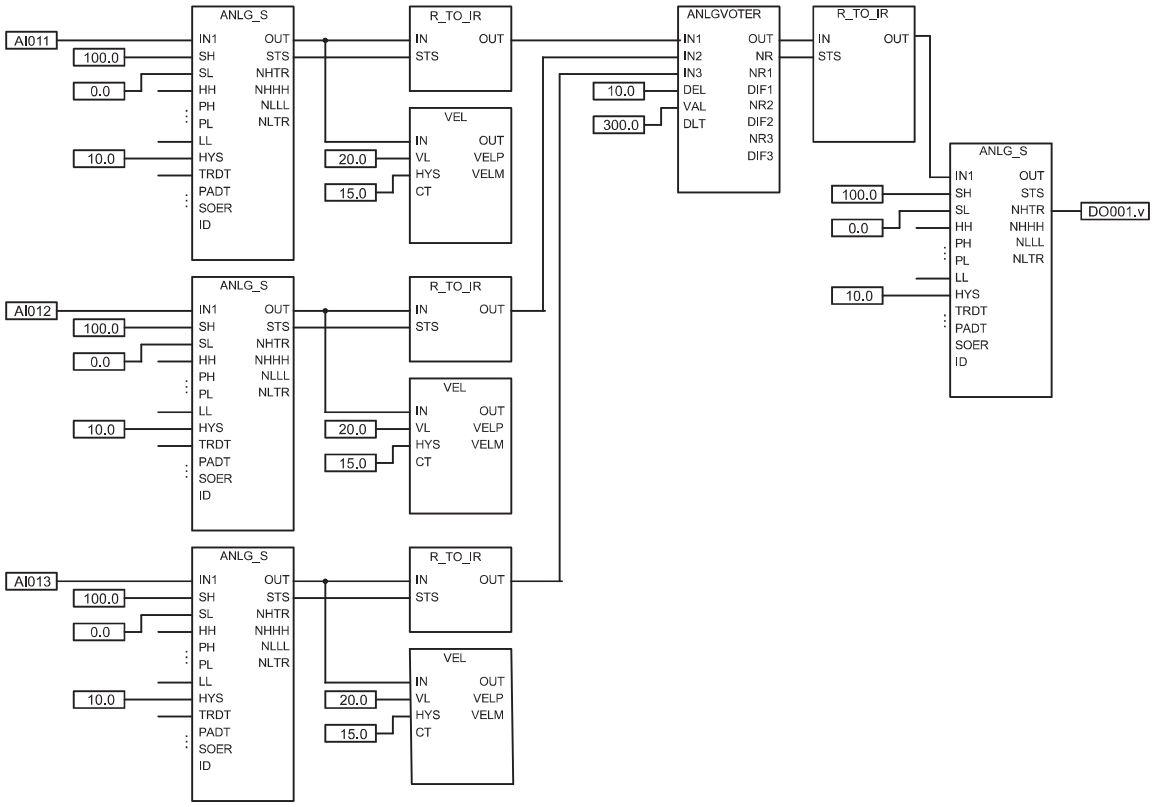


Figure A4.1-4 Example of application logic using the analog input values of the TC/RTD Input module

In the above logic example, the following processes are carried out.

1. Three analog inputs from TC/RTD input modules are each indicated by ANLG_S and the rate of change of each value is simultaneously monitored by VEL to ascertain whether the rate of change is exceeded from allowable range.
2. The intermediate values of the three types of data or the fail-safe values are obtained with ANLGVOTER.
3. The results are indicated by ANLG_S, monitored HI trip status and output to DO.

The input data from TC/RTD input module to ANLG_S is engineering data, which means that 100.0 and 0.0 are input to SH and SL respectively, and input to HYS is in the form of engineering data. The indicated value for ANLG_S (input value to VEL) is engineering data, and so VL and HYS of VEL should be input in engineering data. The same value should be converted to IO_REAL type using R_TO_IR. In R_TO_IR, there is no difference in the handling of input data, whether it is normalized or engineering data. The converted values are each input to ANLGVOTER and the median value or fail-safe value obtained, but since this value is also engineering data, the values input to DEL and VAL in ANLGVOTER are also engineering data. The value obtained is again converted to IO_REAL type using R_TO_IR and input to ANLG_S. In the same way, 100.0 and 0.0 are input to SH and SL respectively and the values input to HYS in the form of engineering data. The Voting result is indicated based on the input value and Hi-Trip (NHTR) is output to DO.

Precautions when using the analog input values from the Thermocouple/Resistance Temperature Detector (TC/RTD)

The input signal entered into the TC/RTD analog input module is passed to the application logic in the form of direct engineering data rather than normalized data.

Caution is required in the case of the ANLG_S, VEL, ANLG1OO2D, and ANLGVOTER, because there are differences in the way of making application logic whether the input data is engineering data or normalized data.

Case of ANLG1OO2D

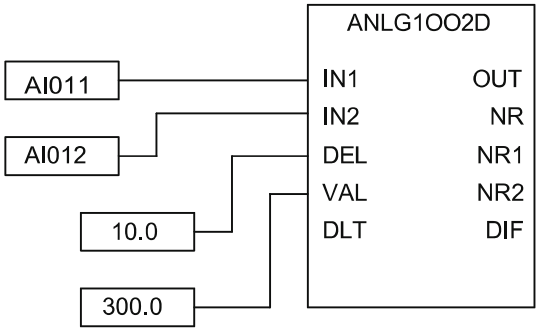


Figure A4.1-5 Example of ANLG1OO2D application logic

The data (AI011, AI012) from the TC/RTD input module is engineering data, and so the input values (IN1, IN2) and output value (OUT) are also engineering data. In this case, DEL and VAL are also entered as engineering data.

This means that, in the figure above, the values of DEL and VAL are specified as 10.0 deg. C and 300.0 deg. C respectively (if the engineering unit specified in I/O Parameter Builder is deg. C).

Case of ANLGVOTER

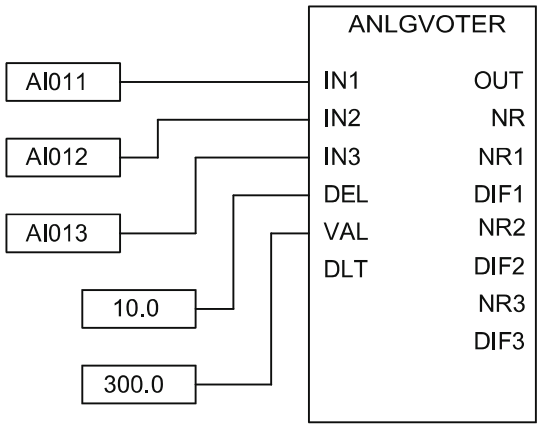


Figure A4.1-6 Example of ANLGVOTER application logic

As with ANLG1OO2D, if the input values (IN1, IN2, IN3) are engineering data, the output value (OUT) will also be engineering data.

DEL and VAL are also entered as engineering data.

Case of VEL

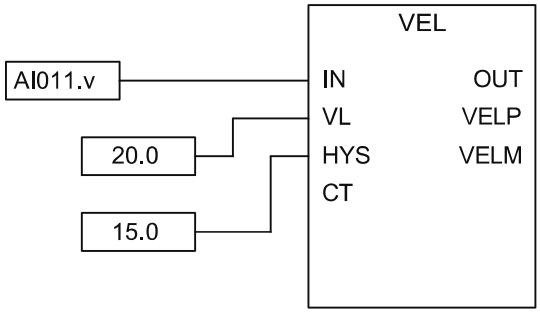


Figure A4.1-7 Example of VEL application logic

If the input value (IN) is engineering data, the output value (OUT) will also be engineering data.

VL and HYS are entered as engineering data.

Case of ANLG_S

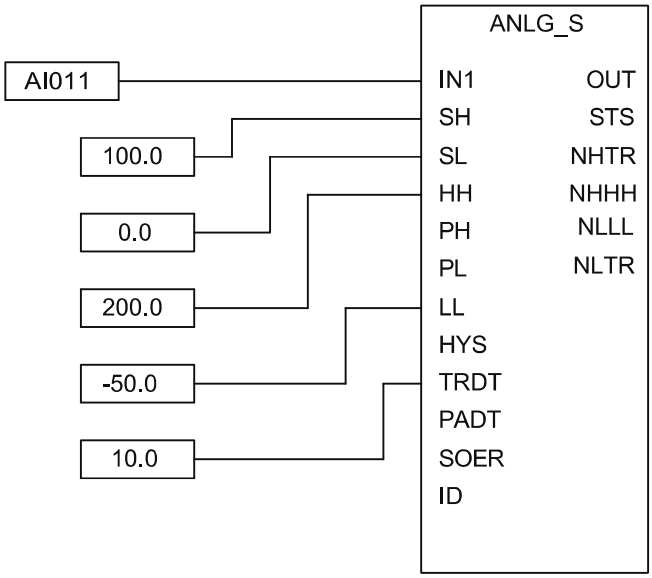


Figure A4.1-8 Example of ANLG_S application logic

In ANLG_S, make sure that you enter the following value if the input value (IN) is engineering data.

SH=100.0

SL=0.0

HYS is entered as engineering data.

TIP

When using ANLGI, apply the same process as ANLG_S.

A4.2 Shutdown due to channel failure

The following examples show how to create application logic for SCS shutdown in case of channel failure.

System Function Block for detecting channel failure

The following table shows the overview of function blocks for creating application logic for shutdown due to a channel failure.

Table A4.2-1 Function Blocks for shutdown due to channel failure

Example of failure to be detected	N-IO	FIO
At least one channel of all the AIO/DIO modules in SCS has failed.	SYS_IOALLST	
At least one channel of an AIO/DIO module in some node has failed.	SYS_N_NODEST	SYS_NODEST
At least one channel of an AIO/DIO module has failed.	SYS_N_IOST16	SYS_OUTST or SYS_OUTST16 for output modules. SYS_INST for input modules.
All channels of an AIO/DIO module have failed.		
The specified channel of an AIO/DIO module has failed.		SYS_CHST. SYS_OUTST or SYS_OUTST16 can also be used for output modules.

A failure in any channel of an FIO AIO/DIO module in a whole SCS or one node as well as a failure in a specific channel can be used as the condition for shutdown. You can combine these two conditions if necessary.

For maintenance of an I/O module, you can prevent shutdown logic from being activated by locking the appropriate module. For maintenance of an output module, the actuator connected with the output channels needs to be bypassed.

Shutdown after detection of any channel failures in a specified unit

The application logic can be created so that shutdown is executed if any output channel has failed in a certain unit (a whole SCS or specified node).

Shutdown due to any output channel failures in a node

You can use SYS_NODEST for FIO nodes, and SYS_N_NODEST for N-IO nodes to create application logic that executes shutdown in case of a failure of any output channel in a node. The following figure shows an example of application logic for FIO nodes.
First, add important outputs to one specific FIO node, as shown in the following figure. Next, create SYS_NODEST, specify a node number as an input parameter for the SYS_NODEST, and then connect the output parameter with the shutdown logic.

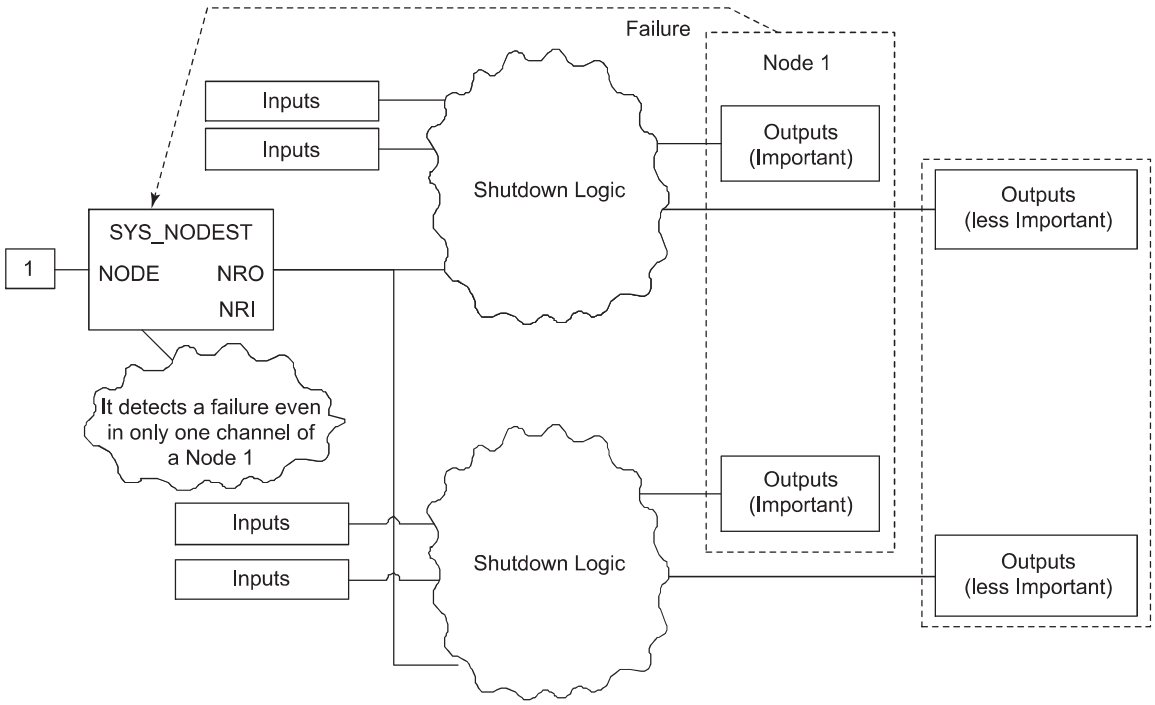


Figure A4.2-1 Shutdown due to any output channel failure in an FIO node

Shutdown due to any output channel failures of an SCS

The SYS_IOALLST is available to create application logic to execute shutdown in case of a failure in any output channel of an SCS.

The creation method of application logic is the same as the one for detecting a failure in a node. However, take appropriate care when using this logic, as the output channels that are not important are also checked for failure by this logic.

SEE ALSO

For more information about SYS_NODEST, refer to:

11.16, “SYS_NODEST (all I/O channels of FIO node status indicator)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about SYS_IOALLST, refer to:

11.15, “SYS_IOALLST (all I/O channels of SCS status indicator)” in POU Reference Manual (IM 32P03B20-01EN)

Shutdown after detection of a failure in a specific channel

The application logic can be created to execute shutdown in case of a failure in specific I/O channels. This allows control of shutdown by responding to the failures of individual I/O channels.

Shutdown due to failures in several specific output channels

For FIO output modules, you can use SYS_OUTST, SYS_OUTST16, and SYS_CHST to create application logic that executes shutdown in case of a failure in specific output channels. For N-IO output modules, you can use SYS_N_IOST16.
In the case of an FIO output module, as in the following figure, create SYS_OUTST and specify the installation location (node number and slot number) of the output module as an input parameter in order to detect a failure in the output channels that acts as the shutdown trigger. The output parameter receives the failure status of each channel. Connect only the necessary channels with the shutdown logic.

For checking fewer channels in an FIO output module, the SYS_CHST can be used instead of the SYS_OUTST and SYS_OUTST16. To use the SYS_CHST, you need to specify installation locations of the channels (node number, slot number, and channel number).

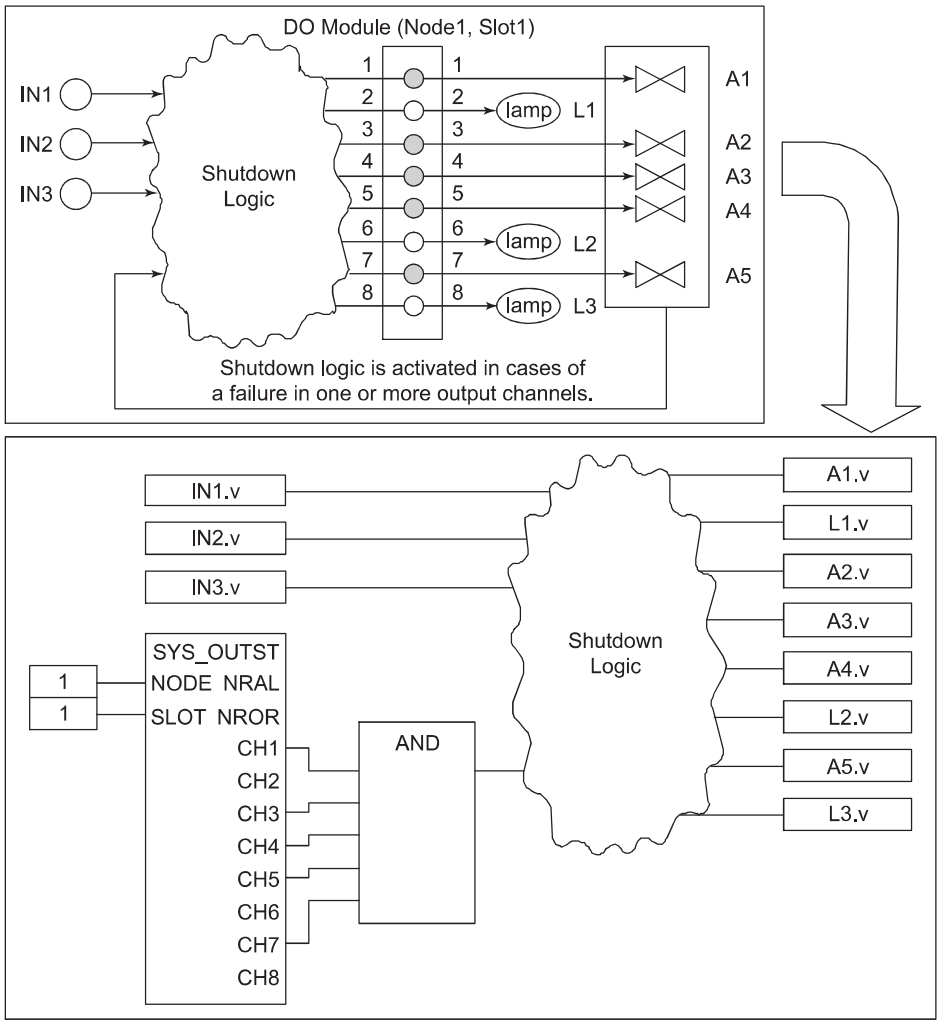


Figure A4.2-2 Example of shutdown logic to which a failure in each output channel is inputted in an FIO Output module

SEE ALSO For more information about SYS_OUTST, refer to:

- 11.18, “SYS_OUTST (FIO output module 8 channels indicator)” in POU Reference Manual (IM 32P03B20-01EN)
- 11.19, “SYS_OUTST16 (FIO output module 16 channels indicator)” in POU Reference Manual (IM 32P03B20-01EN)

Shutdown due to a failure in important input channels

To create application logic for shutdown in case of a failure in important input channels, specify the channel’s input value for a failure which invokes the shutdown demand. Additional application logic is not necessary.

When failure in an input channel is expected, after multiplexing inputs, use the Voter FB including BOOLVOTER, to create application logic.

Shutdown when all multiplexed input channels fail

You can use SYS_N_IOST16 for N-IO input modules, and SYS_INST or SYS_CHST for FIO input modules to create application logic that executes shutdown when all multiplexed input channels fail.

For this type of application logic, the channel's input value for a failure needs to be specified as a value that keeps the channel's NORMAL status in order to avoid shutdown due to only one input channel failure.

Shutdown when all multiplexed input channels fail

There are two methods of creating this type of application logic.

You can implement all multiplexed inputs on one input module with the other channels kept unused. This method detects the failures of all channels with simple logic by using SYS_INST for FIO input modules, and SYS_N_IOST16 for N-IO input modules.

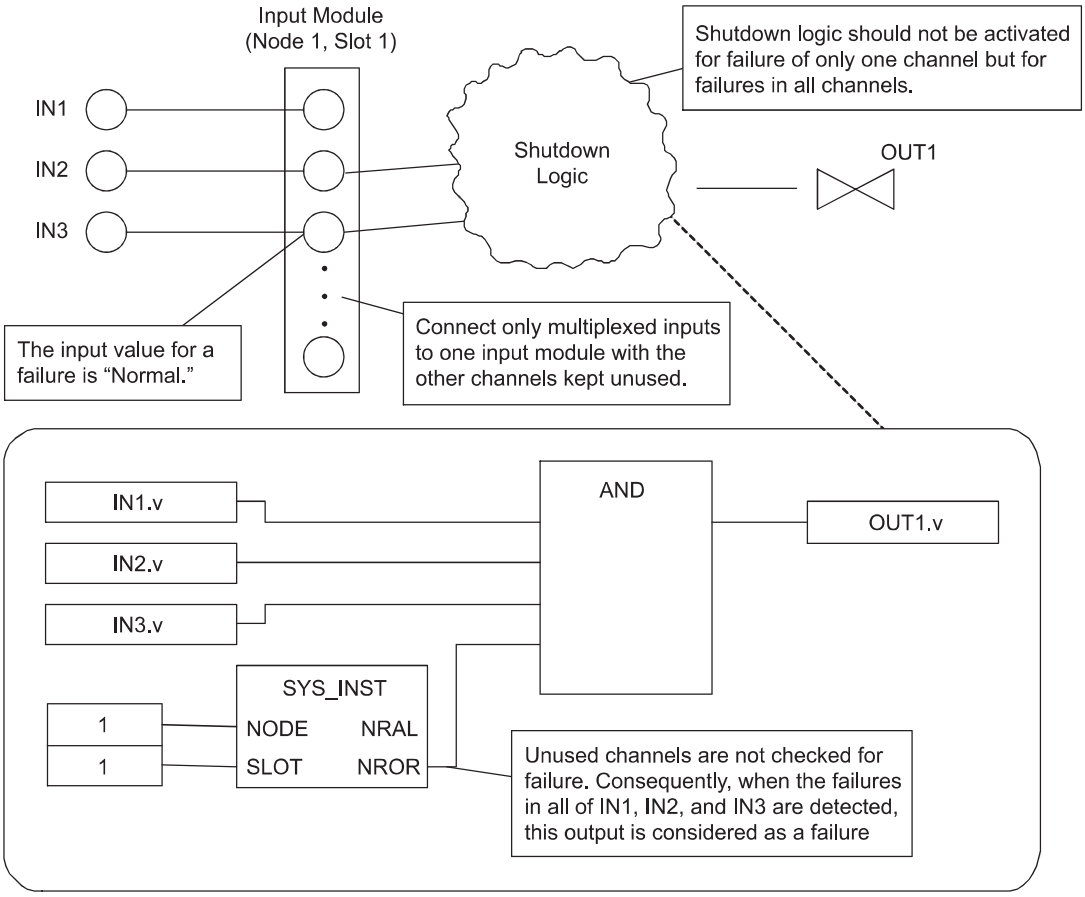


Figure A4.2-3 Example of application to execute shutdown when all multiplexed input channels fail in FIO Input modules (1)

In the other method, you can implement several multiplexed inputs on separate input modules. The advantages of this method are easier maintenance of modules and resistance to module failures; however, the logic of this method is quite complicated as compared to that of example 1. This case requires an AND operation after detecting the failure status of all multiplexed channels. For FIO input modules, use SYS_CHST to detect the failure status of each channel. For N-IO input modules, use SYS_N_IOST16 to detect the failure status of each channel.

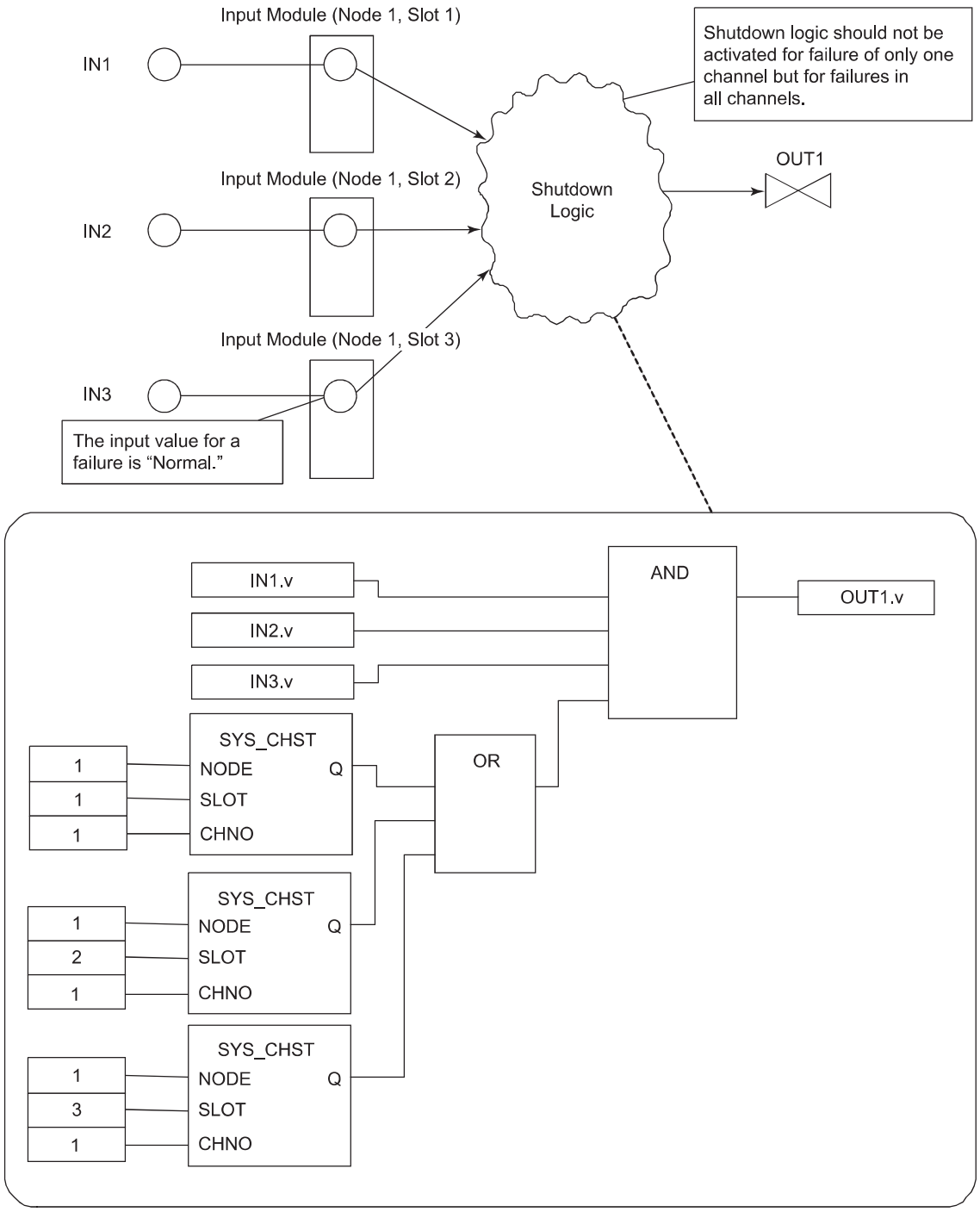


Figure A4.2-4 Example of application to execute shutdown when all multiplexed input channels fail in FIO Input modules (2)

SEE ALSO

For more information about SYS_INST, refer to:

11.20, “SYS_INST (FIO input module status indicator)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about SYS_CHST, refer to:

11.21, “SYS_CHST (status indicator of FIO module channel)” in POU Reference Manual (IM 32P03B20-01EN)

A4.3 Example of displaying I/O status

This section provides an example of displaying I/O module status using function blocks.

TIP

This type of application is rarely needed to be created because I/O status is displayed on SENG.

Example of displaying I/O operating status

The SYS_DIAG is available if I/O operating status needs to be indicated on an external display. You can use SYS_IOMDSP for FIO I/O modules and SYS_N_IOMDSP for N-IO I/O modules.

To detect a failure in a whole SCS, the SYS_DIAG is available.

To display the status of individual modules, use SYS_N_IOMDSP for N-IO I/O modules and SYS_IOMDSP for FIO I/O modules. One function block is needed to display the status of one module.

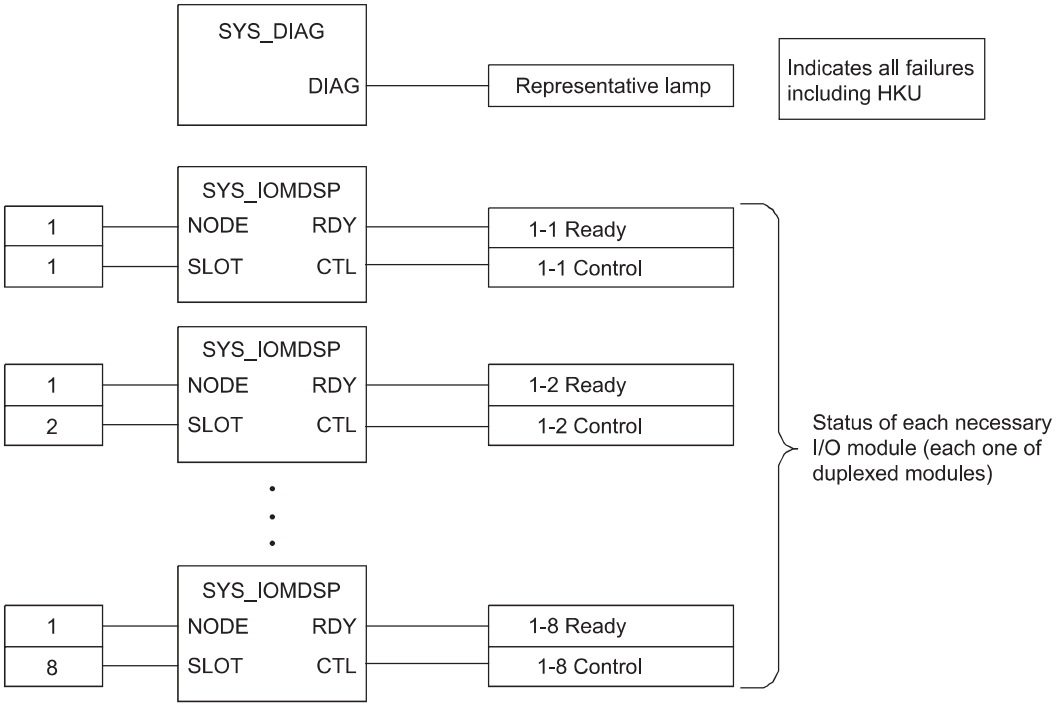


Figure A4.3-1 Example of displaying operating status of FIO I/O modules

SEE ALSO

For more information about SYS_DIAG, refer to:

11.7, “SYS_DIAG (diagnostic information output)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about SYS_IOMDSP, refer to:

12.9, “SYS_IOMDSP (FIO module status indicator)” in POU Reference Manual (IM 32P03B20-01EN)

A4.4 Relations among AIO/DIO, Communication module and System FBs

This section describes the relationship between AIO/DIO modules that can be used in SCSs, communication modules and system function blocks. “Related” in this context refers to cases where an output value of an FB is changed if an error occurs in a module or data, or the data output to a module changes depending on the operation of the FB.

Table A4.4-1 Safety FBs

	FIO input module (*1)	FIO output module (*1)	N-IO I/O module (*1)	Subsystem communication module (Communication I/O data) (*1)	Safety subsystem communication module(*1)	Modbus slave communication module (*1)
SYS_STAT	No	Yes	Yes (*2)	No	No	No
SYS_FORCE	Yes	Yes	Yes	No	No	No
SYS_FORCE_SF	No	No	No	No	Yes	No
SYS_DIAG (*3)	Yes	Yes	Yes	Yes	Yes	Yes
SYS_IOALLST (*4)	Yes	Yes	Yes	No	No	No
SYS_NODEST (*4) (*5)	Yes	Yes	No	No	No	No
SYS_N_NODEST (*4) (*6)	No	No	Yes	No	No	No
SYS_OUTST (*5)	No	Yes	No	No	No	No
SYS_OUTST16 (*5)	No	Yes	No	No	No	No
SYS_INST (*4) (*5)	Yes	No	No	No	No	No
SYS_N_IOST16 (*4) (*6)	No	No	Yes	No	No	No
SYS_CHST (*4) (*5)	Yes	Yes	No	No	No	No
SYS_ALLSD	No	Yes	Yes (*2)	No	No	No
SYS_IOSD (*5)	No	Yes	No	No	No	No
SYS_N_IOSD (*6)	No	No	Yes (*2)	No	No	No

*1: Yes: Related
No: Not related
*2: Only output channels
*3: If a failure or data error occurs, the output parameter IOER is set to TRUE.
*4: When errors occurred in the communication route between CPU and I/O modules (except for the error occurred in one of the redundant ESB buses with that routed properly), the output becomes FALSE.
*5: For FIO
*6: For N-IO

Table A4.4-2 Interference-free FBs

	FIO input module (*1)	FIO output module (*1)	N-IO I/O module (*1)	Subsystem communication module (communication I/O data) (*1)	Safety subsystem communication module (*1)	Modbus slave communication module (*1)
SYS_IOMDSP (*2) (*3)	Yes	Yes	No	Yes	Yes	Yes
SYS_N_IOMDSP (*2) (*4)	No	No	Yes	No	No	No

Continues on the next page

Table A4.4-2 Interference-free FBs (Table continued)

	FIO input module (*1)	FIO output module (*1)	N-IO I/O module (*1)	Subsystem communication module (communication I/O data) (*1)	Safety subsystem communication module (*1)	Modbus slave communication module (*1)
SYS_ALRDSP (*2)	No	No	No	Yes	Yes	No
SYS_STAT_SC	No	No	No	Yes	No	No
SYS_FORCE_SC	No	No	No	Yes	No	No

*1: Yes: Related
No: Not related
*2: When errors occurred in the communication route between CPU and I/O modules (except for the error occurred in one of the redundant ESB buses with that routed properly), the output of the I/O modules will hold the previous output values.
*3: For FIO
*4: For N-IO

A4.5 Example of using BOOL-type Data Manual Operation FB (MOB_*)

By using the Bool-type Data Manual Operation Function Block with Answerback (MOB_11/ MOB_21), you can operate the valve(s) using switch-type face plate from HIS.

In addition to making the switch operation available from HIS, this type of function blocks is capable of outputting a shutdown instruction immediately regardless of the manipulated output value from the HIS if a shutdown event occurs. They also have the function to check the answerback input against the manipulated command value, security password function, manual operation enabling function and so on. The manual operation of MOB_11 or MOB_21 from HIS can be used for operating valves at the startup of a plant or for testing the behavior of devices when you perform maintenance work. Note that when you manually operate MOB_11 or MOB_21, entry of password is required.

You can request an output of pulse status from an Auto-Reset Bool-type Data Manual Operation FB (MOB_RS) by using CENTUM HIS. This FB is used to reset from the shutdown status or to reset alarms.

SEE ALSO For more information about functions of the bool-type manual operation function blocks, refer to:

7., “Function blocks for integration with CENTUM (Safety FBs)” in POU Reference Manual (IM 32P03B20-01EN)

Example of using BOOL-type Data Manual Operation FB (MOB_21)

This is an example where the MOB_21 FB is used under the following conditions:

- During the start-up of the plant.
- Shutdown of the SCS occurred and the cause of the shutdown has been cleared.
- The valve is opened one by one using manual operation from HIS.

This example is applicable if a shutdown event is the only criterion to disable manual operation, and if manual operation is enabled whenever the shutdown event is solved.

For DTS, SHDN is connected to signals from the shutdown logic, SS to FALSE.

To enable the manual operation immediately after the shutdown event is solved, connect TRUE to SW. If the SW is always TRUE, the value of IN never be referenced, so set any value to IN.

Since the shutdown signal has higher priority, when the input value of SHDN becomes FALSE, the manual operation becomes disabled even if the SW is always TRUE.

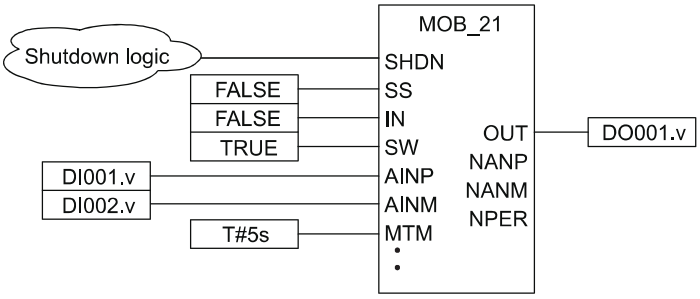


Figure A4.5-1 Example of using BOOL-type Data Manual Operation FB (MOB_21)

The above figure is an example of DTS. For ETS, set the SS input to TRUE.

Example of valve with only Full Close Limit Switch

For manipulating the valve with only Full Close Limit Switch, use the Bool-type Data Manual Operation with Two-Position Answerback (MOB_11) and enter an inverted Full Close Limit Switch signal into AIN.

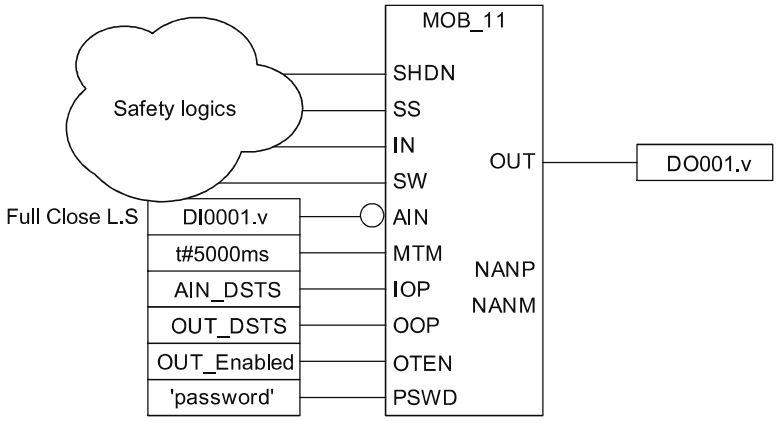


Figure A4.5-2 For valve with only Full Close Limit Switch

Example of manipulating Two-position analog valve

Connect analog signal to SCS.To allow an HIS to manipulate an analog valve having only two statuses, Full Open and Full Close, configure the loop as shown in the following figure.

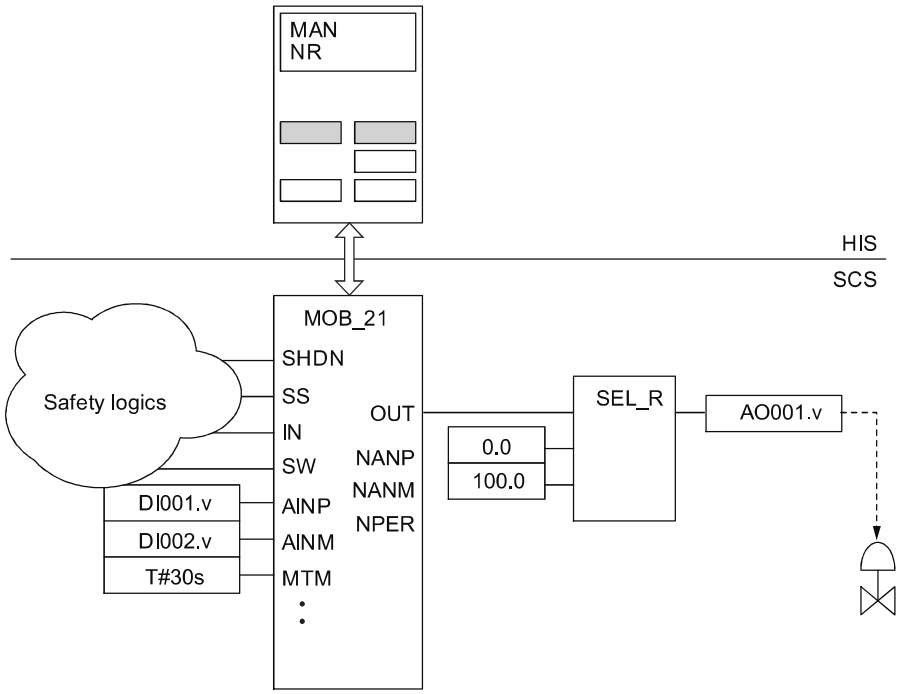


Figure A4.5-3 For manipulating Two-position analog valve

Example of No Answerback check

If Answerback check is not required, looping back the output value to Answerback input disables the Answerback check function. In this case, PV can be used for checking (visually) operations from CENTUM.

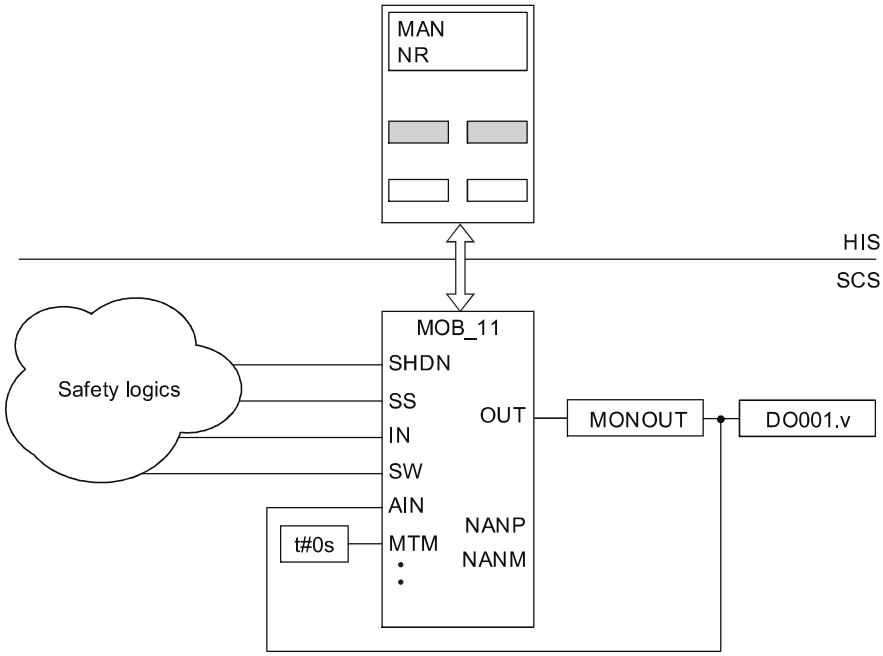


Figure A4.5-4 Case where No Answerback check is required

A4.6 Construction example of First-up Alarm function

In ESD applications and similar, even if the system is shut down due to a certain cause, it might lead to other shutdown causes immediately or multiple shutdown-causing factors may mutually interact in the application logic. As a result, it is not always possible to identify the first cause.

The first-up function allows you to identify the event (factor) that was generated first among grouped events.

Overview of First-up Alarm function and application examples

The first-up alarm function is constructed by combining First-up Alarm Annunciator (ANN_FUP) and First-up Alarm Annunciator Reset (FUR_RST). A First-up Alarm Annunciator (ANN_FUP) allows identifying and outputting events that occurred first and second among grouped events. If a CENTUM HIS is connected, an annunciator message is output for the event that occurred first. A First-up Alarm Annunciator Reset (FUP_RST) is used to reset the first-up alarm status of ANN_FUP.

An example of constructing the first-up alarm function using these FBs is shown below.

Example of First-up Alarm and outputting failure of rest operation to HIS

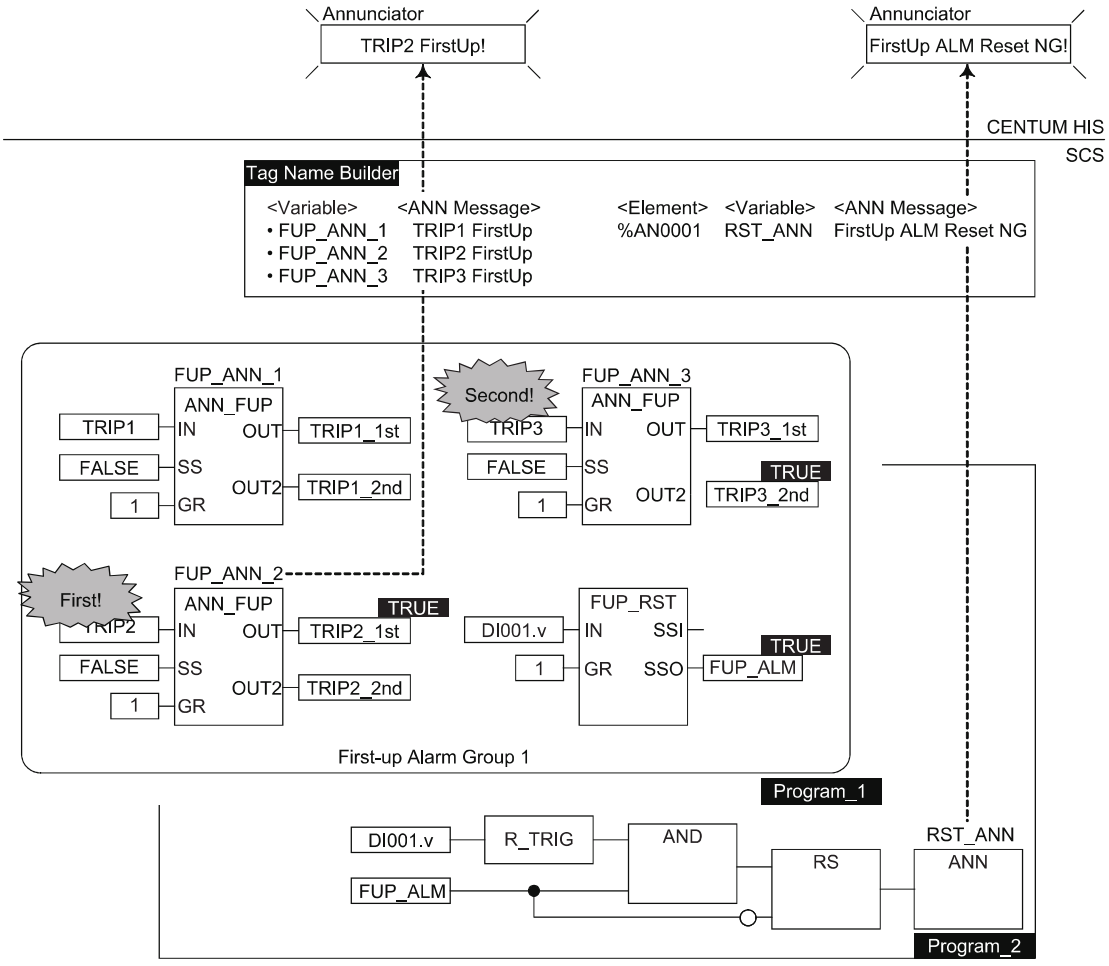


Figure A4.6-1 Application of detecting First-up Alarm

Program_1 inputs events TRIP1, TRIP2, and TRIP3 to their respective ANN_FUPs and set them as First-up alarm group 1. Each ANN_FUP is assigned an instance name. A DI signal

DI001, which is operated by a hardware console, etc. and input to SCS for alarm reset, is input to FUP_RST.

Program_2 creates logic to check if the first-up alarm status is cancelled when alarm reset operation is performed.

Annunciator messages corresponding to each instance are defined in the Tag Name Builder or iDefine.

In the example above, events are generated in the order of TRIP2, TRIP3, and then TRIP1. In this case, OUT (TRIP2_1st) of the instance name FUP_ANN_2 and OUT2 (TRIP3_2nd) of FUP_ANN_3 become TRUE and the annunciator message for the first-up alarm (annunciator message of FUP_ANN_2) is output to HIS. When the first-up alarm is generated, SSO (FUP_ALM) of FUP_RST becomes TRUE. In the status where FUP_ALM is TRUE, the first-up alarm status is not cancelled even if the alarm reset signal (DI001) is received. In such cases, an annunciator message notifying that the alarm reset operation failed is output. Since ANN_FUP does not have SOE functions, connect SOE FB as required.

A4.7 Considerations on using Time Synchronization Function Block (SYS_SETTIME)

Observe the following usage limitations and considerations when you set the system time of SCS and the Vnet/IP or V net time by using the function block (SYS_SETTIME).

The following figure shows an example to set 2:00:00 on input of a trigger signal by using the SYS_SETTIME function block.

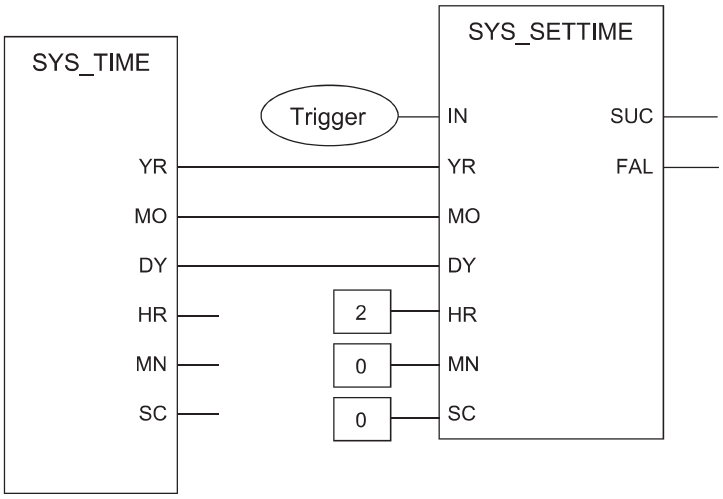


Figure A4.7-1 Usage example of SYS_SETTIME

Considerations on setting the time in the usage example are as follows:

- At the moment the time setting is executed, the date must match between the trigger signal providing side and the SCS to which the time is set. To ensure matching dates, offset more than one minute from 0:00 AM. If the time is set around 0:00 A.M.If the function block is used to set a time around 0:00 A.M. If the date of the trigger signal providing side and the date of the SCS may become different. Therefore, a wrong date may be set to the SCS.
- Before using the time synchronization function block, set the time using the time setting function of SENG or HIS.

SEE ALSO For more information about time synchronization function block (SYS_SETTIME), refer to:

12.3, “SYS_SETTIME (SCS time setting)” in POU Reference Manual (IM 32P03B20-01EN)

Usage limitations of Time Synchronization Function Block

Do not use the time synchronization function block under the following states: An alarm may occur, due to resetting of the time or time diagnostic error in inter-SCS safety communication.

- Using IRIG-B time synchronization in the time synchronization method
- Using the time synchronization function block in two or more SCSs.
- Using two or more time synchronization function blocks in one SCS.
- A station with Vnet/IP firmware earlier than Rev. 8 is connected to Vnet/IP.
  The time synchronization function block can be used when the Vnet/IP firmware of the station is updated to Rev. 9 or later.
- SCS with SCS system program R2.03.58 or earlier is connected to the same control bus.

The time synchronization function block can be used when all SCS system program release numbers of all SCSs are updated to R2.03.59 or later.

In addition, if the SNTP server is connected to Vnet/IP, the time setting by the time synchronization function block is disabled.

Time span for the Time Synchronization Function Block for detecting DI input and setting the SCS time

Use the DI input that is connected to the SCS using this function block as the input signal for IN.

The maximum time (Tsettime), which is from detection of DI input to change of the SCS time, is obtained from the following formula:

Tsettime = Tscan x 2 + Processing time of Input module + 50 ms - Idle time

Idle time = Tscan - Application logic execution time

SEE ALSO For more information about check application logic execution time, refer to:

“● CPU processing time” in “■ Confirmation of CPU processing time and consideration of idle time” in A7.1, “Definition of SCS scan period” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about application logic execution time, refer to:

12.1, “SYS_SCAN (execution time indicator)” in POU Reference Manual (IM 32P03B20-01EN)

A5. Library projects

It is possible to improve engineering efficiency by creating functions and function blocks commonly used in multiple SCSs as library projects and use them from SCS projects. This section explains how to create library projects and precautions on how they differ from SCS projects.

When performing engineering using iDefine, you cannot use function blocks in library projects, which are created using SCS Manager, from iDefine or add function blocks to the library projects from iDefine.

Overview of library projects

IMPORTANT

Create an individual copy of the necessary library projects for each SCS project that uses them. Avoid using one library project from multiple SCS projects in order to prevent modification of one library project from affecting multiple SCS projects.

Library projects are a part of an SCS project. It is possible to use multiple library projects from one SCS project. When using multiple library projects, be careful so that names of functions and function blocks do not overlap.

Note that it is not possible for a library project to reference another library project.

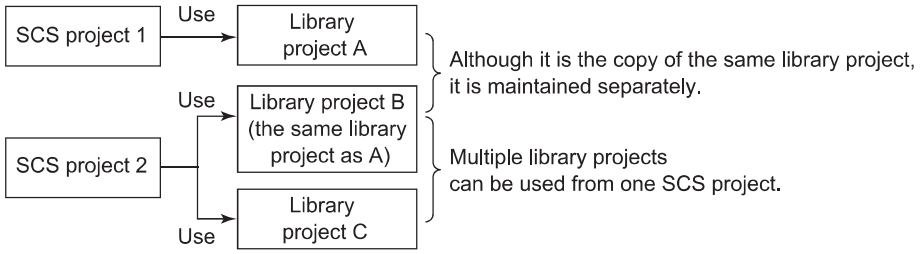


Figure A5-1 Overview of library projects

A5.1 Creation of library projects

Create an original library project and debug it; it can be copied and used for several SCS projects.

Creation procedure of library projects

1. On SCS Manager, choose [New Project/Library] from the [File] menu, and then choose [SCS Library] from "Template" so as to create a new library project.
   It is recommended to create a folder called "USERLIB" immediately below the `C:\RS-Projects` folder created at installation and place library projects there.

TIP

When using AD Suite, the name of the folder where you place the original library projects should consists of up to eight single-byte characters.

2. Use SCS Manager and Multi-Language Editor to define commonly used functions and function blocks.
3. Use SCS Manager and Multi-Language Editor to create a program to test the functions and function blocks defined in step 2.
4. Check that there are no programming errors in the build.
5. Execute a simulation test and confirm that functions and function blocks work as intended.
   Note that an actual SCS is not required at debugging. Library projects cannot be debugged using SCSs.
6. Analyze the project using Integrity Analyzer to confirm that there are no problems.

SEE ALSO

For more information about library project settings, refer to:

"Libraries" in "Workbench" in the Workbench User's Guide

Procedure to copy library projects for each SCS project

1. Use SCS Manager and create an SCS project.
2. Use Windows Explorer to copy the original library project immediately below the `LIBRARIES` folder located in the SCS project folder.
3. Select [Add/Remove Dependencies] from the [Tools] menu of SCS Manager.
   The copied library is associated with the SCS project. This allows using one library only from one SCS project.
4. User-defined functions and user-defined function blocks created as part of the library can be used when creating POUs with the FBD, LD and ST languages. If the user-defined function block is used in an ST, an Integrity Analyzer warning message will be displayed to prompt for authorization.

With the procedure above, the library project will become available to access from the SCS project. If the library project is to be used in other SCS projects as well, repeat copying the library project for each SCS project.

IMPORTANT

Library projects are divided into the original library projects created in the `C:\RS-Projects\USERLIB` folder and those copied to the `LIBRARIES` folder for each SCS project. Make sure to keep the library projects updated so that the libraries in both folders maintain the same contents.

TIP

If you refer to an SCS project from a remote PC, specify the library project path of the Dependencies in the UNC format.



Figure A5.1-1 Specification example of UNC-format library project path

SEE ALSO

For more information about defining the dependency of a library project, refer to:

"Using Libraries in a Project" in "Libraries" in "Workbench" in the Workbench User's Guide

Folder structure of library projects

The figure below shows the folder structure for library projects.

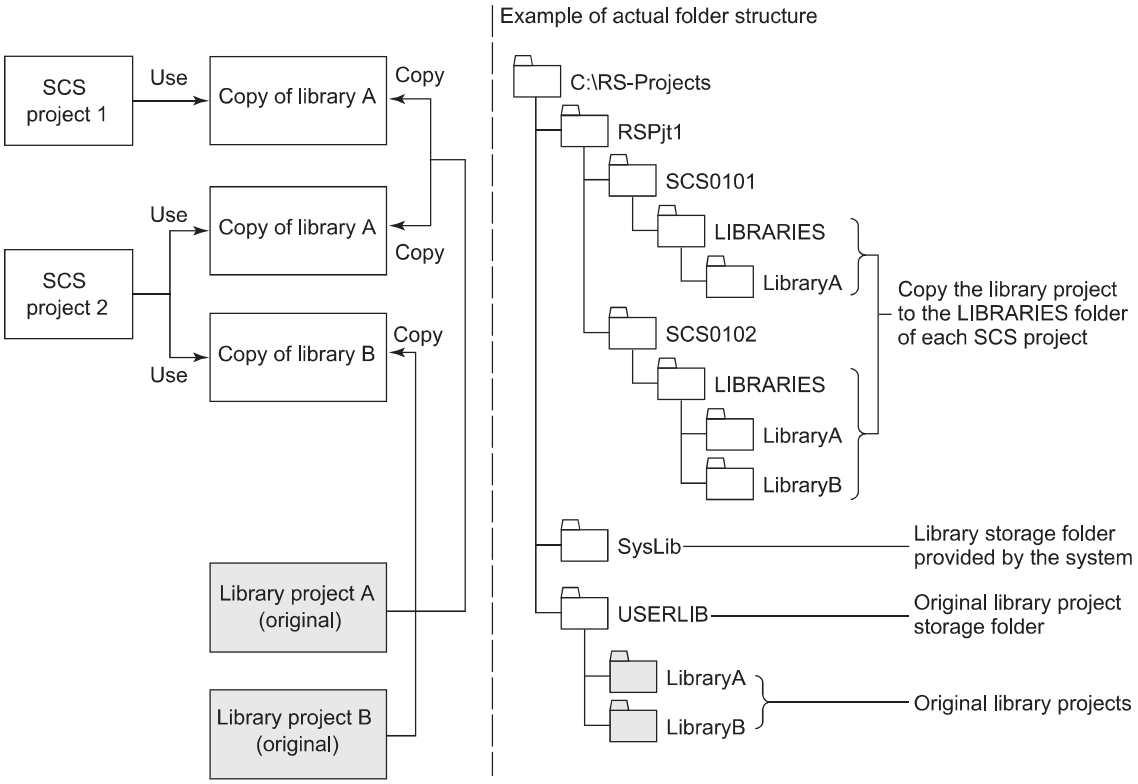


Figure A5.1-2 Folder structure of library projects

A5.2 Items set for library projects

When creating user-defined functions and function blocks for library projects, it is mandatory to set certain items for projects, configuration, resources, functions and function blocks, while some items can be set arbitrarily.

Items set for library projects

The table below summarizes items that must be set to create user-defined functions and user-defined function blocks for a library project.

Table A5.2-1 Items set for library projects

Classification	Item	Setting	Remarks
Project	Project name	Mandatory	
	Project comment	Arbitrary	
	Password setting	Arbitrary	
	Project description	Arbitrary	
Configuration	Configuration name	Mandatory	
	Configuration comment	Arbitrary	
	Target	Mandatory	
	Password setting	Arbitrary	
	Configuration description	Arbitrary	
	Network	No need to specify	
	Connection IP address	No need to specify	

Continues on the next page

Table A5.2-1 Items set for library projects (Table continued)

Classification	Item	Setting	Remarks
Resource	Resource name	Mandatory	
	Resource comment	Arbitrary	
	Resource number	Mandatory	Enter any value in the range from 1 to 4094
	Target	Mandatory	
	Generate debug information	Arbitrary	
	Code for simulation	Mandatory	
	Code generation setting	Mandatory	Specify TIC code
	Embed Symbol Table	No need to specify	
	Embed Zip Source	No need to specify	
	Trigger cycles	Arbitrary	
	Cycle Timing	Arbitrary	
	Detect errors	No need to specify	
	Nb of stored errors	No need to specify	
	Cycle to cycle/Real time	Arbitrary	
	Memory for Retain	No need to specify	
	Password	Arbitrary	
	Resource description	Arbitrary	
User-defined function/ user-defined function block	POU name	Mandatory	
	POU comment	Arbitrary	
	Debug information	Arbitrary	
	Password	Arbitrary	
	POU description	Arbitrary	

A5.3 Precautions on library projects

Pay attention to the following points when creating and using library projects.

- How to use library projects
- Software revision of SCS project and library project
- Operations when incorporating library projects into SCS project
- Differences between SCS projects and library projects
- Operations on SCS projects and relationship with libraries
- Precautions when testing library projects
- Precautions when using Integrity Analyzer
- How to make changes to library projects

How to use library projects

- With a library project, it is possible to create logic for user-defined functions and user-defined function blocks and debug them in a simulation test. Note, that unlike in the case of SCS projects, it is not possible to download them to an SCS or perform debugging using an SCS.
- In order to debug user-defined functions and user-defined function blocks, a special program for testing them is required. Create a program for testing purposes if you inspect user-defined functions and user-defined function blocks by Integrity Analyzer.

A5.3.1 Software revision of SCS project and library project

Match the revision numbers of software for creating SCS Project and for creating Library Project.

However, even if the revision number of software for creating Library POU is later than the revision number of software for creating the SCS Project, you don't have to match the revision numbers unless the Library POU includes FB/FU that is unsupported by the SCS Project.

A5.3.2 Operations when incorporating library projects into SCS project

User-defined functions and user-defined function blocks created in a library project have restriction as follows in an SCS project.

- They cannot be opened with Multi-Language Editor.
  They must be referenced using the library project.
- The logic cannot be printed out.
  Print the logic via the library project.

A5.3.3 Differences between SCS projects and library projects

The table below summarizes functions that can only be used in library projects and cause errors when creating SCS projects.

Table A5.3.3-1 Functions that can only be used in library projects

Function	Library project specification	SCS project specification
Library project name, configuration name, resource name	Up to 64 characters including alphabets, numbers and underscore. The first letter must be an alphabet character.	Fixed to SCSddss
Resource number	In the range from 1 to 4094	Fixed to ddss

Note that, in library projects, variable names should be kept within 18 characters and POU names (user-defined functions and user-defined function blocks) used in a library project should be kept within 16 characters, although longer names will not cause errors at building.

A5.3.4 Operations on SCS projects and relationship with libraries

Once pasted from the original library projects into SCS projects, the libraries constitute a part of the SCS projects. Therefore, operations on the SCS projects are also applied to the pasted libraries as well.

- The data of libraries is also saved in the master database. The same rule applies to restoration as well.
- The data of libraries is saved in the version control of an SCS project. The same rule applies to restoration as well.

A5.3.5 Precautions when testing library projects

In order to test functions and function blocks defined in a library project, it is necessary to open the original library project in SCS Manager and perform a logic simulation test. In order to perform this test, create a program for testing purposes in the original library project. In the SCS project that uses the libraries, it is possible to check the inputs and outputs of user-defined functions and user-defined function blocks from the library project, but the internal operations cannot be checked.

Note that if it is not necessary to debug functions and function blocks defined in the library project, the abovementioned test program is not required.

A5.3.6 Precautions when using Integrity Analyzer

Test program

When using Integrity Analyzer to analyze user-defined functions and user-defined function blocks, the original library project requires a test program that calls its functions and function blocks. This is because Integrity Analyzer analyzes functions and function blocks via the program and display warnings and errors that occur during the test. This test program is used purely for analysis by Integrity Analyzer and has nothing to do with the operation of an SCS project that uses the library.

"Authorize" operation

It is possible to perform "authorize" on a library project as well. However, performing "authorize" on a library project does not mean that the SCS project that uses the library is authorized.

The "authorize" of the SCS project does not become valid until the library project is incorporated in the SCS project and built using the SCS project.

Starting operation of Integrity Analyzer

Integrity Analyzer is started in the same way as for an SCS project. Choose [Engineering] from [Tools] menu of SCS Manager. The Engineering launcher menu appears; select [Integrity Analyzer] to launch Integrity Analyzer.

A5.3.7 How to make changes to library projects

To make changes to library projects, follow the procedure below.

1. Make the desired changes to an original library project and debug them.
2. Copy the original library project and paste it to the corresponding library folder of an SCS project.

It is not always necessary to make changes to an original library project, but the changes must be reflected in all the libraries including the original library project eventually.

A6. SCS link transmission

There are the following types of SCS link transmission.

- SCS link transmission safety communication (Safety function)
  This establishes a safety communication between SCSs in the same domain. A safety loop can be established between the sending side and receiving side SCSs.
- SCS global switch communication (Interference-free function)
  This establishes interference-free communication between SCS and CENTUM stations (FCS, APCS, and GSGW; hereafter collectively referred to as FCS) in the same domain.

SEE ALSO

For more information about basic functions of SCS link transmission, refer to:

A6.1, “Overview of the SCS link transmission” on page A6-2

For more information about engineering for SCS link transmission, refer to:

A6.3, “SCS link transmission definition” on page A6-11

For more information about SCS global switch communication, refer to:

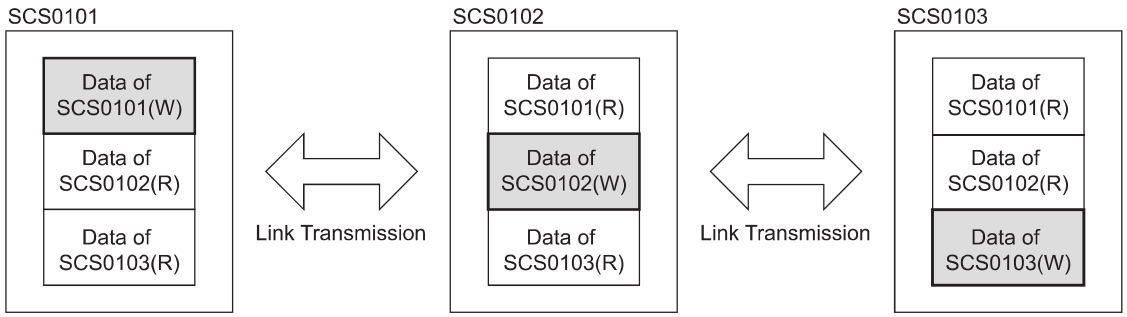
A6.5, “SCS global switch communication” on page A6-24

A6.1 Overview of the SCS link transmission

This section describes the overview of the SCS link transmission.

■ SCS link transmission

You can use the link transmission function of control bus to broadcast data of a station periodically to all other stations in the same domain (simultaneous notification). Vice versa, a station can also receive the broadcasts of other stations and you can use the received data in the application logics.



W: An SCS can write its own data.
R: Data of other SCS are read only.

Figure A6.1-1 SCS link transmission

● Communication specification

The main communication specifications of SCS link transmissions are as follows:

- Communication range: within a domain. However, V net router style S3 or above enables to make SCS Link Transmission Global Switch Communications between V net domain and Vnet/IP domain connected with V net router. Please consult the explanation in the reference link.
- Control bus: V net, Vnet/IP (either of them)
- Max. number of stations: 64 (Max. number of stations to communicate with stations: 63)
- Transmission period: Every 100 ms (fixed)
- Type of data exchanged among SCSs through SCS link transmission: BOOL type data only (Analog-type and integer-type is not supported)

SEE ALSO For more information about virtual domain link transmission when using a V net router of style S3 or above, refer to:

"■ Virtual domain link transmission" in Appendix 4.4, "System expansion with V net router connection" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

● Read and write transmission data

In SCS link transmission, bits in the received data are assigned to the dedicated FBs as input and read by the application logic. Bits in the data to be sent are assigned to the dedicated FBs as output and sent to other stations.

- Up to 1000 FBs can be used as input FBs of SCS link transmission per SCS (This is irrelevant to the sending station types such as SCS or FCS). The number of FBs for receive data per station is not limited.
- Up to 128 bits can be assigned to the output FB of SCS link transmission per SCS.

SCS link transmission types

SCS link transmission is mainly for the safety data communications among SCSs, and the interference-free communications between SCS and FCS (including APCS and GSGW). There are two types of communications:

- Data communications among SCSs: SCS link transmission safety communication
- Data communications between SCS-FCS: SCS global switch communication

SCS link transmission safety communication

SCS link transmission safety communication is a feature for communicating safety data among SCSs.

Safety communication

SCS link transmission safety communication attaches safety information to the communication data values, therefore, the receiving SCS can validate the received data values according to the safety information (safety-layer). Due to this validation, SCS link transmission safety communication data can be used in the following safety loops that across SCSs: The supported SIL varies depending on the SCS used.

- Between SIL3 SCS and SIL3 SCS, it can be used in safety loops up to SIL3
- Between SIL2 SCS and SIL2 SCS, it can be used in safety loops up to SIL2
- Between SIL3 SCS and SIL2 SCS, it can be used in safety loops up to SIL2

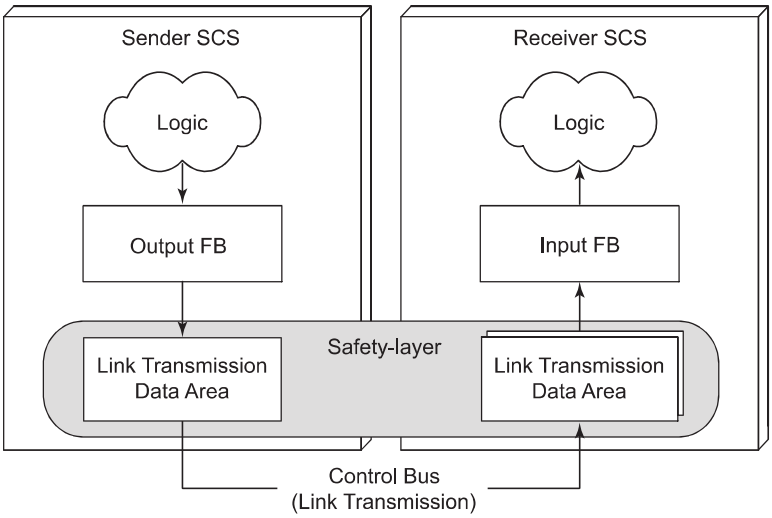


Figure A6.1-2 SCS link transmission safety communication overview

SCS actions on abnormality

When an error is detected by safety-layer, SCS will act as follows:

- Initiate a system alarm on the diagnosis error (alarm class 1).
- Set the statuses of the data received from the corresponding station to BAD.
- Use the fail-safe data values specified on the builder to replace the data values of input FBs.

When the diagnosis error is recovered, SCS will act as follows: Since the error status is not latched, it may be necessary to make the application to latch the error status.

- Initiate a system alarm on the recovery.
- Set the statuses of the data received from the corresponding station to GOOD.

- Input FBs use the data values that are refreshed after recovery.

SCS link transmission global switch communication

Global switch communication

Through link transmission, SCS can read data of FCS global switches. Vice versa, FCS can receive data from SCS as global switches.

Note the following when using global switch data:

- SCS can read 256 bit data of FCS global switches.
- SCS link transmission global switch communication is interference-free communication. For the applications to use the received FCS data, the dedicated FB should be used. The input data from the dedicated FB cannot be used in the safety application logics.
- The global switches in FCS that can accept the SCS link transmission data are the global switches from %GS001 to %GS128. The switches from %GS129 are not available for SCS link transmission data.

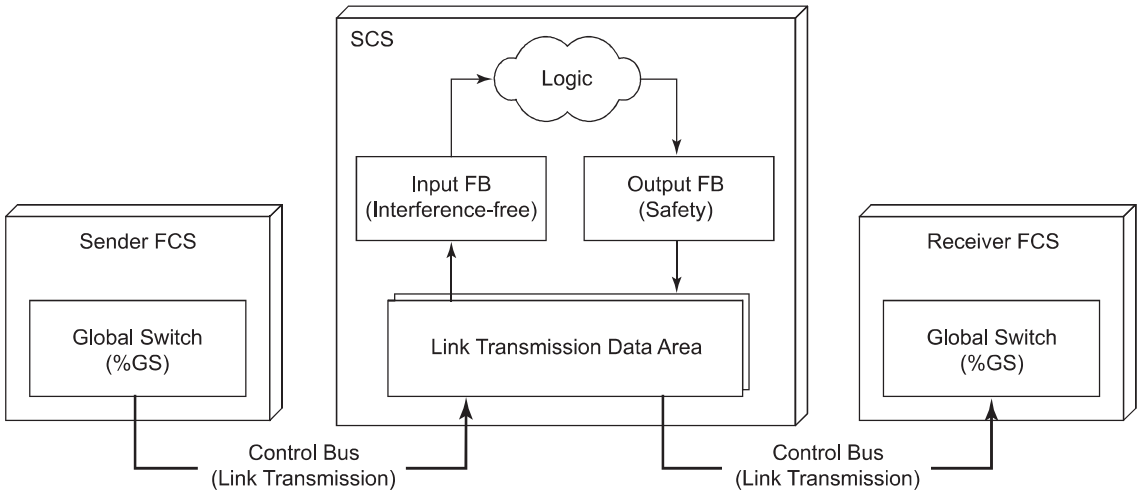


Figure A6.1-3 Data exchange between SCS and FCS through link transmission

SCS actions on communication error

When a communication error occurs or when the sender FCS stops, SCS will act as follows:

- Initiate a system alarm on the diagnosis error (alarm class 2).
- Set the statuses of the data received from the corresponding station to BAD.
- Use the fail-safe data values specified on the builder to replace the data values of input FBs.

When communication recovers from error, SCS will act as follows:

- Initiate a system alarm on the recovery.
- Set the statuses of the data received from the corresponding station to GOOD.
- Input FBs use the data values that are refreshed after recovery.

A6.2 Data structure and definition of the SCS link transmission

This section describes the overview of the data structure and necessary definition contents of the SCS link transmission.

Data structure of SCS link transmission

Data sent through SCS link transmission and data received from the stations are first stored in a dedicated data buffer.

When using SCS link transmission data in application logic, communication data is obtained using a dedicated input FB. Conversely, to send the result of application logic execution, the result of application logic should be input to a dedicated output FB.

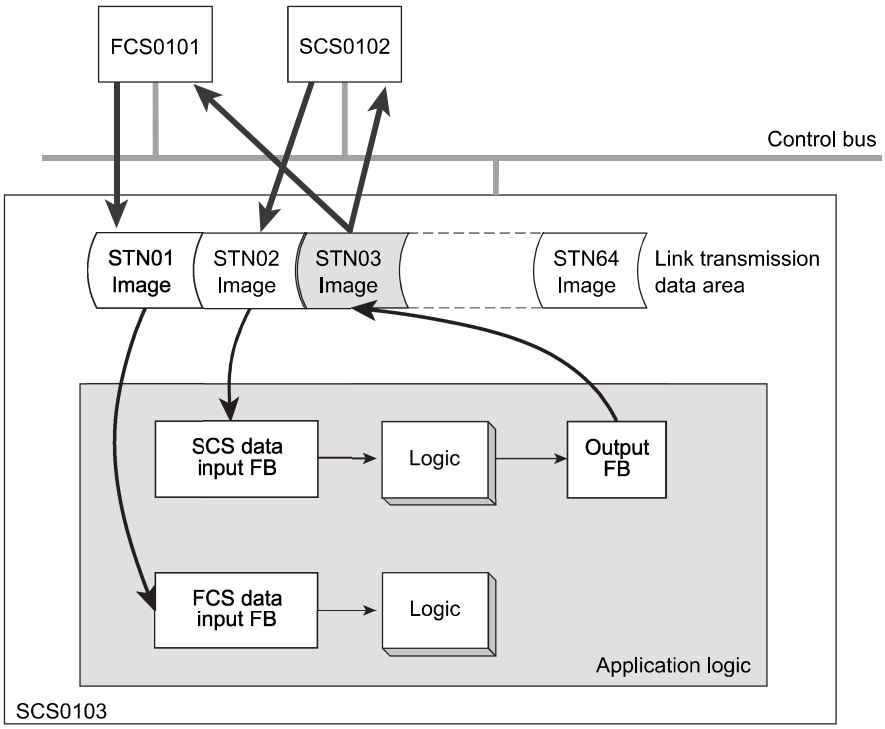


Figure A6.2-1 SCS link transmission dataflow

Receive data

Receive data of SCS link transmission consists of data value and data status. Data status in SCS link transmission does not indicate the quality of each data item, but rather gives status information regarding whether data was received normally. SCS determines data status based on the communication status and safety diagnosis result for each communication target station.

Both data value and data status can be referenced via input FB. Separate input FBs dedicated to each communicating station type (SCS/FCS) are provided.

Send data

Send data of SCS link transmission has data value only and no data status. There is only one type of output FB, regardless of whether the send destination is SCS or FCS.

Function blocks for SCS link transmission

In order for application logic to handle SCS link transmission data, the following function blocks are provided for each communicating station type.

Table A6.2-1 Function blocks related to SCS link transmission

FB type	Processing by the function block	Remark
LTRCV	Inputs link transmission data from other SCSs	Safety
LTSND	Outputs link transmission data from local SCS	
LTFCS	Inputs link transmission data sent from FCS (global switch)	Interference-free
SYS_FORCE_LT	Manages forcing of SCS Link Transmission	Safety system FB
SYS_LTSTS	Indicates SCS Link Transmission reception status	

SEE ALSO For more information about each FB, refer to:

- 6.7, “LTSND (link transmission data output)” in POU Reference Manual (IM 32P03B20-01EN)
- 6.8, “LTRCV (safety link transmission data input)” in POU Reference Manual (IM 32P03B20-01EN)
- 8.5, “LTFCS (interference-free link transmission data input)” in POU Reference Manual (IM 32P03B20-01EN)
- 11.3, “SYS_FORCE_LT (SCS link transmission lock status monitor)” in POU Reference Manual (IM 32P03B20-01EN)
- 11.6, “SYS_LTSTS (SCS link transmission reception status monitor)” in POU Reference Manual (IM 32P03B20-01EN)

Definition of send data

SCS link transmission send should be defined in SCS Link Transmission Builder and also by creating the application logic using the output FB of SCS link transmission.

Definition of SCS link transmission send

To send SCS link transmission data from an SCS to other stations, permit sending via link transmission in the Self Station tab of SCS Link Transmission Builder.

TIP At all SCSs in the domain where it is permitted to receive SCS link transmission from the station for which sending is defined, the application regarding receive data can be changed freely, and such changes do not affect other stations.

Wiring of send data

To send correct data, define an output FB in the application logic, and perform wiring definition for the local station data using SCS Link Transmission Builder.

IMPORTANT

If data with no wiring definition at the sending station is referenced at the receiving side station, data status will be GOOD and data value will be FALSE.

Definition of receive data

SCS link transmission receive should be defined in SCS Link Transmission Builder and also by creating the application logic using the input FB of SCS link transmission.

Definition of SCS link transmission receive

To receive SCS link transmission data from other stations, permit receiving via link transmission in the Self station tab of SCS Link Transmission Builder.

Data received from reception target stations are defined in the Other Stations tab of the SCS link transmission definition.

If the transmission source station type is SCS, it will be a safety communication and thus the following items must be defined. If the transmission source is FCS, it cannot be set.

- Reception Timeout (Reception interval timeout value): OUTT
- Transmission Timeout (Transmission delay timeout value): DLYT
- Pre-Alarm (Pre-alarm setting value): PALT

OUTT (reception interval timeout value) setting

The reception interval is the interval at which SCS receives the data. Specify the reception interval timeout value (OUTT) for each communication partner station. This value can be set between 3 and 30 seconds. OUTT is calculated by the following formula. However, if the calculation result is 3 seconds or less, set a value of between 3 and 30 seconds.

OUTT= (Scan period of sender SCS or receiver SCS whichever longer) x 8

If normal data cannot be received within this reception interval timeout value, a communication error will occur and the fail-safe values will be used to replace the communication data values.

Inter-SCS transmission delay time and reception interval

Inter-SCS transmission delay time is the elapsed time after the sending side SCS transmits the data until the receiving side SCS receives the data. The normal range is defined by DLYT (transmission delay timeout value). If the inter-SCS transmission delay time is outside the normal range, the received communication frame is ignored.

The transmission delay time is affected not only by the delay in the communication path but also by the difference in scan period settings of the SCS application logic execution function at the sending side and receiving side.

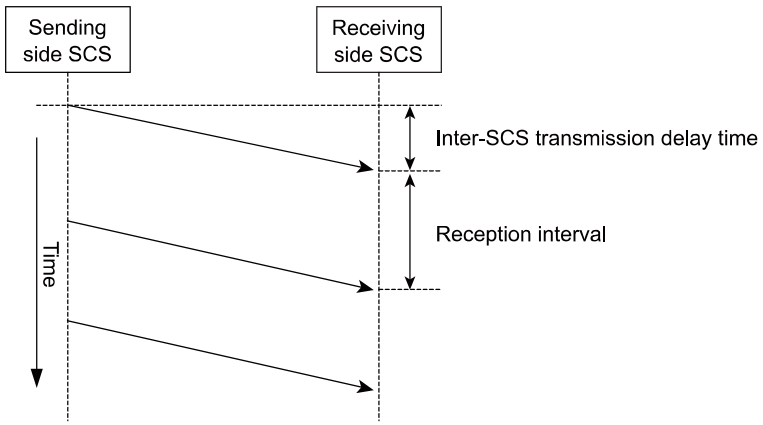


Figure A6.2-2 Inter-SCS transmission delay time and reception interval

A temporary transmission delay error can be detected by monitoring OUTT (reception interval timeout value). Set DLYT to detect a constant transmission delay error.

DLYT (transmission delay timeout value) and PALT (pre-alarm setting value) settings

- DLYT
  Specify the transmission delay timeout value (DLYT) for each communication partner station.

  DLYT can be set to 0 seconds or between 3 and 30 seconds. When DLYT is set to 0, the inter-SCS transmission delay check is disabled.

A communication error will occur if a delay outside the normal range occurs, that is, if the state where the “inter-SCS transmission delay time exceeds DLYT” continues longer than the time specified by OUTT. As a result, the fail-safe values will be used to replace the communication data values.

- PALT
  Specify the pre-alarm setting value (PALT) for each communication partner station. If it is necessary to detect transmission delay before the inter-SCS transmission delay time reaches the DLYT, specify this value. Diagnostic information message is not generated.

  PALT can be set to 0 seconds or between 3 and 29 seconds. When PALT is set to 0, the pre-alarm is not output.

  A pre-alarm will occur if the inter-SCS transmission delay time exceeds the time specified by PALT and if the state continues longer than the period specified by OUTT. By using a system function block of SYS_LTSTS, you can notify the application of the occurrence of pre-alarm.
- Relationship between DLYT and PALT
  PALT check is performed unless PALT is set to 0. Pre-alarms are detected even if DLYT is set to 0. To activate the pre-alarm while the DLYT is not set to 0, set 0 <PALT <DLYT.

IMPORTANT

If both PALT and DLYT are set to 0, the receive data of SCS link transmission cannot be used for safety purposes.

SEE ALSO

For more information about DLYT calculation method when the SCS system program release number is R2.03.51 or earlier on the sending or receiving end of SCS link transmission, refer to:

“■ Specification changes made in SCS system program (Release number R2.03.51)” in Appendix 3.2, “The major changes in R2” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Wiring of receive data

To use the receive data of SCS link transmission in application logic, define an input FB according to the station type, and then perform wiring definition of data for each receiving side station in SCS Link Transmission Builder.
During wiring definition, the input value at error occurrence should also be defined.

IMPORTANT

If wiring of the receive data from a nonexistent station is defined, the data status will always be BAD and the data value will be the input value at error occurrence.

Precaution for engineering

This section describes precautions and important issues in using SCS link transmission.

Purpose of SCS link transmission

The following figure illustrates the relationship between SCS link transmission and binding of inter-SCS safety communication for data exchange among SCSs.

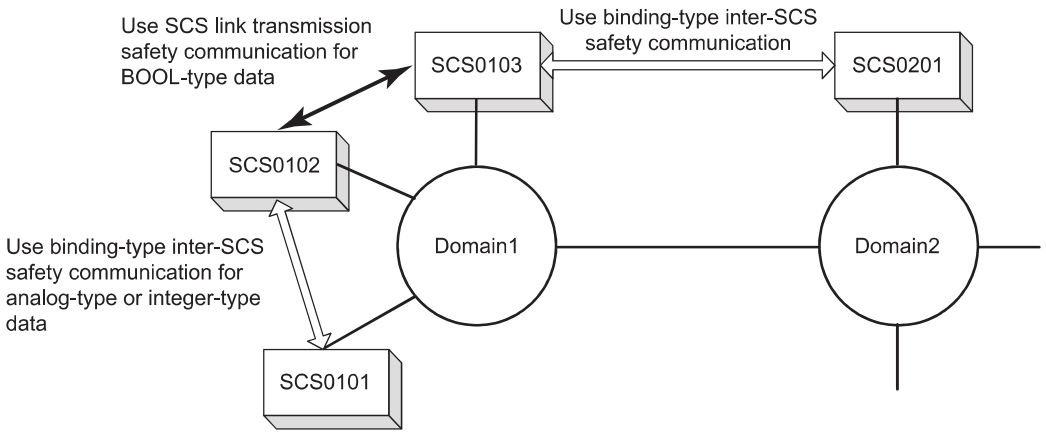


Figure A6.2-3 Relationship with Inter-SCS Safety Communication

The BOOL type data exchange among SCSs in the same domain is recommended to go through the SCS link transmission safety communication. Although the amount of data that can be communicated is limited, use of SCS link transmission safety communication enables communication with more stations and achieves higher performance, compared to when inter-SCS safety communication is used.

For analog-type or integer-type data exchange in the same domain and for inter-SCS data exchange across domains, use binding-type inter-SCS safety communication.

The following table shows the scope of communication and the relationship of communication data types and communication methods.

Table A6.2-2 Communication data types and communication methods

Scope	Data type	Communication Method	Remark
Inter-SCS in the same domain	BOOL	SCS link transmission safety communication	Can communicate with FCS (SCS global switch communication: Interference-free) Can be changed online
	Analog, integer	Binding-type inter-SCS safety communication	Cannot change the binding online
Inter-SCS across domains	BOOL, analog	Binding-type inter-SCS safety communication	Cannot change the binding online

Communication with FCS through the Inter-station Data Link Block (ADL)

FCS can read from SCS mapping blocks or write to SCS mapping blocks through the inter-station data link block (ADL). However, data exchange through SCS link transmission does not require the mapping blocks used by data exchange through inter-station data link block (ADL). Consider using SCS link transmission for SCSs exchange data of BOOL type in one domain.

The following cautions need to be noted when reading or writing for data exchange:

- When writing from FCS to SCS through the inter-station data link block (ADL), the periodic writing is restricted. However, periodic writing is possible through SCS link transmission.
- Tag names cannot be assigned for the Input/Output function block of SCS link transmission. For reading the SCS data transmitted through SCS link transmission on HIS, the transmitted data should be linked to the BOOL type internal variables by the application logics and assigned the tag names to the linked variables.

Other notices

- When the receiver station accesses data that is not assigned on the sender station, the data value will show FALSE and the data status will show GOOD.
- Builder cannot check the consistency of the data assigned on the sender station and on the receiver station for data exchange, so the assignment of the communication data on both sides must be checked by the communication test.
- By the setting of "Link Transmission Receiving Station" of SCS link transmission, the receiver stations can be limited so as to prevent the performance declination. Other stations with which no communication is required should not be specified as "Receive."
- The SCS system program for SCS that uses SCS link transmission must be R1.03.00 or later.

  The FCS system program for FCS that is the target of SCS link transmission global switch communication must be R3.08.50 or later.

SEE ALSO For more information about DLYT (transmission delay timeout value) calculation method when the SCS system program release number of either the sending or receiving end of SCS link transmission safety communication is R2.03.51 or earlier, refer to:

"■ Specification changes made in SCS system program (Release number R2.03.51)" in Appendix 3.2, "The major changes in R2" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

A6.3 SCS link transmission definition

The communication data for SCS Link Transmission can be defined on SCS Link Transmission Builder. This section explains how to define the SCS Link Transmission and how to use the SCS Link Transmission Builder.

SEE ALSO For more information about overview of definitions for SCS link transmission, refer to:

A6.1, “Overview of the SCS link transmission” on page A6-2

SCS link transmission configuration procedure

SCS Link Transmission Builder and Dictionary View are used to configure SCS Link Transmission definitions.

1. On Dictionary View, define the variable names for the SCS Link Transmission I/O FBs used for SCS Link Transmission.
2. On SCS Link Transmission Builder, define receptions and transmissions between local and other stations.
   The communicated data through SCS Link Transmission is represented by the bit number.
3. On the SCS Link Transmission Builder, define the relations of the bit numbers of each station and the variable names of the SCS Link Transmission I/O FBs.

Main features of SCS Link Transmission Builder

On the SCS Link Transmission Builder, the variables to be received and to be transmitted through SCS Link Transmission can be assigned and their connections with SCS Link Transmission I/O FBs can be wired.

Through wiring these elements, bit numbers of each station are associated with the variable names of SCS link transmission I/O FBs. The SCS Link Transmission I/O FBs that can be assigned to the bit numbers of SCS Link Transmission vary with the station type of the destined stations.

The station types of the destined Other Stations are:

- SCS
- FCS, GSGW, and APCS
  Other Stations such as FCS, GSGW, and APCS are referred as FCS.

Start SCS Link Transmission Builder

1. Choose [Engineering] from [Tools] menu of SCS Manager.
   The Engineering Launcher menu appears.
2. Click [SCS Link Transmission Builder].
   The SCS Link Transmission Builder starts.

SCS Link Transmission Builder window

In the left pane of SCS Link Transmission Builder window, the following contents are listed. After selecting content from the list, the corresponding details will be displayed in the right pane.

- SCS Link Transmission Definition
- Data Wiring Definition
- Data Wiring View

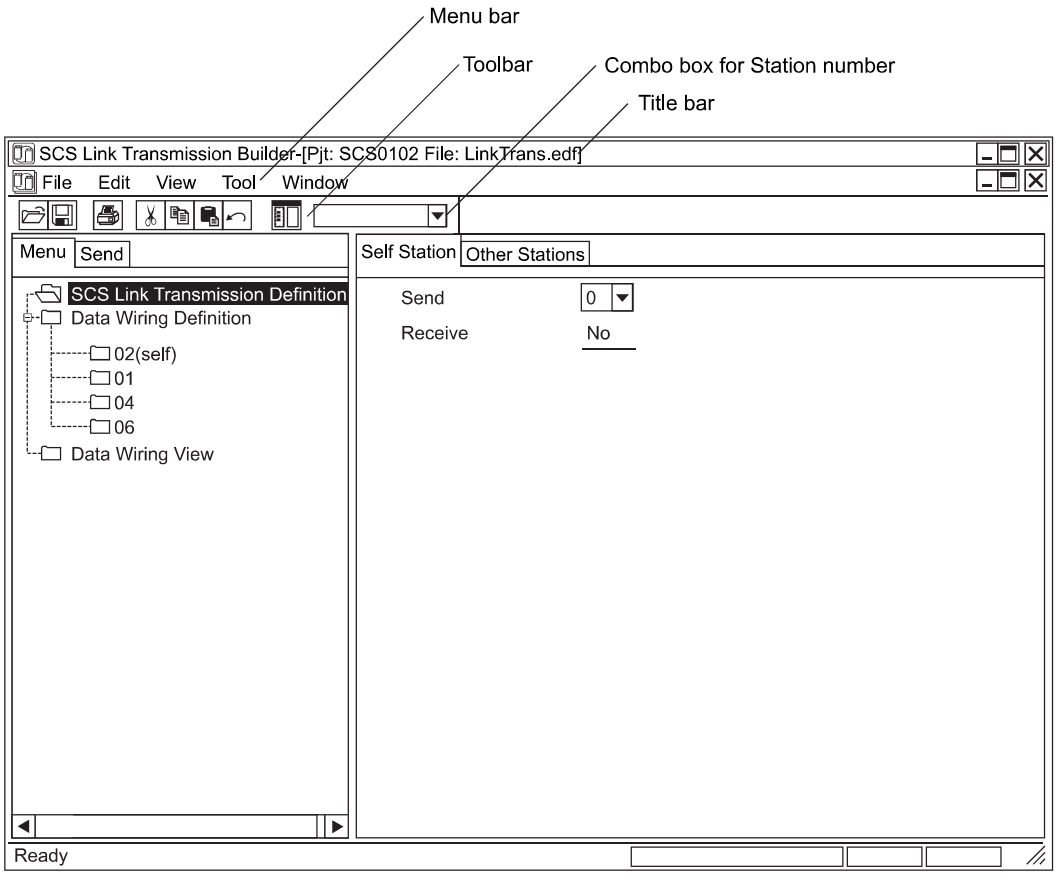


Figure A6.3-1 SCS Link Transmission Builder - SCS Link Transmission Definition - "Self Station" Tab

Self Station tab of SCS link transmission definition

On this tab, the data reception and transmission of the local station can be defined.

Send

Whether to send data from the local station can be defined. If you want to send data from the local station, choose [1: Yes], otherwise choose [0: No]. When [1: Yes] is chosen, the related wirings on the local station need to be defined. The initial setting is "No."

IMPORTANT

When "No" is chosen for Send, the previously defined wiring information will be removed at the moment of switching tabs.

Receive

Whether to receive data from other stations can be defined. If you want to receive data from other stations, choose [1: Yes], otherwise choose [0: No]. When [1: Yes] is chosen, the related settings on "Other Stations" tab need to be defined. The initial setting is "No."

IMPORTANT

When "No" is chosen for Receive, the previously defined wiring information will be removed at the moment of switching tabs.

Other Stations tab of SCS Link Transmission Definition

When Receive is set to [Yes] on "Self Station" tab of SCS Link Transmission Definition, the station type, the reception interval timeout (OUTT), the transmission delay timeout (DLYT), and the pre-alarm setting value (PALT) need to be defined for each station.

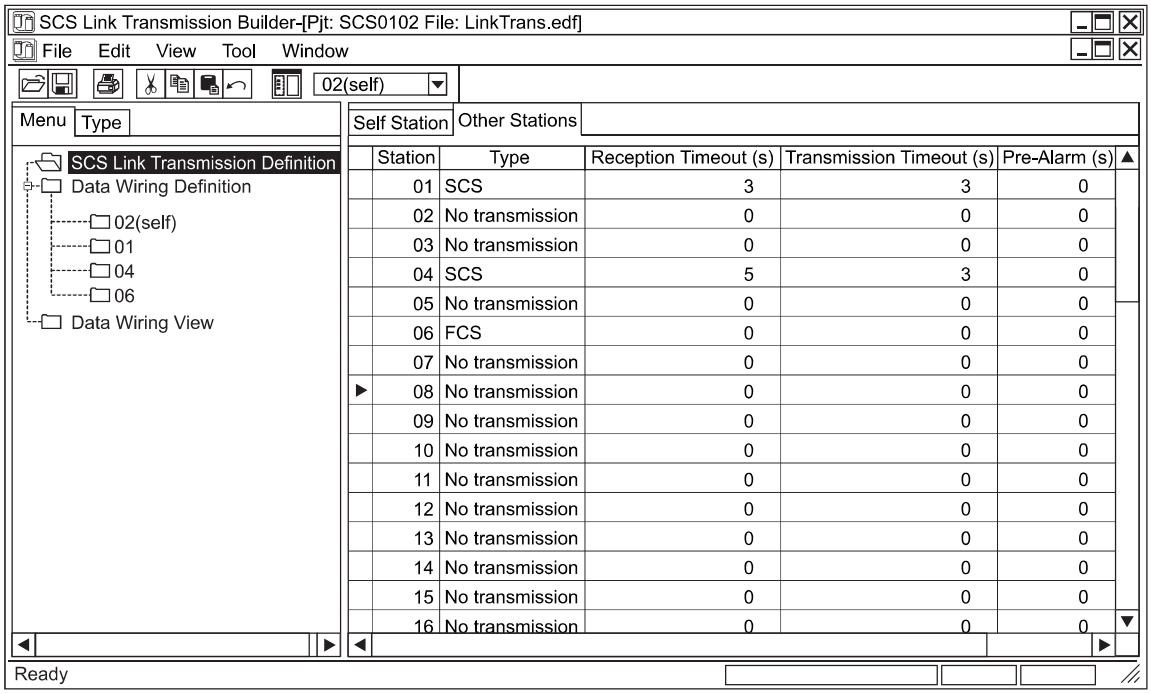


Figure A6.3-2 Other Stations tab of SCS Link Transmission Definition on SCS Link Transmission Builder

Type

The numbers in the "Station" column at left side are the station numbers. The type needs to be set according to each station number. For receiving the SCS Link Transmission data, the type should be set to [1: SCS], while for receiving the global switches of FCS, the type should be set to [2: FCS]. [0: No transmission] can also be set if not receiving data from that station.

IMPORTANT

- The type for the local station should not be set. If you set it, an error will occur during build operation.
- When "No transmission" is set for Type, the previously defined wiring information of that station will be removed at the moment of switching tabs.

Reception Timeout (Reception interval timeout value)

The reception timeout should be set to a time between 3 and 30 seconds. This setting is required for the SCS type only. The initial setting is 3 seconds.

Transmission Timeout (Inter-SCS transmission delay timeout value)

The transmission timeout, i.e. the limited time from transmission to reception should be set to a time between 3 and 30 seconds. This setting is required for the SCS "Type" only. The initial setting is 3 seconds.

If the inter-SCS transmission delay check is not required, "0" should be set. However, if "0" is set, the received data cannot be used for Safety loop logic.

Pre-Alarm (Pre-Alarm setting value)

The pre-alarm can be initiated prior to transmission timeout alarm. The time for initiating the pre-alarm can be set to 0 or from 3 to 29 seconds. This setting is required for the SCS type only. The pre-alarm setting value should be set if you need to detect transmission delay before the delay reaches the transmission delay timeout value (DLYT). The initial setting is "0".

SEE ALSO For more information about defining incoming data for SCS link transmission, refer to:

A6.2, “Data structure and definition of the SCS link transmission” on page A6-5

For more information about precautions regarding the setting times for SCS link transmission, refer to:

“■ Precaution for engineering” on page A6-8

Data Wiring Definition

Wiring details for both "Self Station" and "Other Stations" need to be defined.
The Data Wiring Definition of the tree view in the left pane and the tab in the right pane show the following station numbers.

- The station number of the Self Station When the setting of Send in the "Self Station" tab of SCS Link Transmission Builder is set to "Yes."
- The station numbers of the other stations When the setting of Receive in the "Self Station" tab of SCS Link Transmission Builder is set to "Yes" and the setting of Type in the "Other Stations" tab of SCS Link Transmission Builder is set to "SCS" or "FCS."

Do the following to switch the tabs from "Self Station" and "Other stations."

- Choose a station number in the tree view in the left pane.
- Select a station number in the combo box for selecting the station on the toolbar.

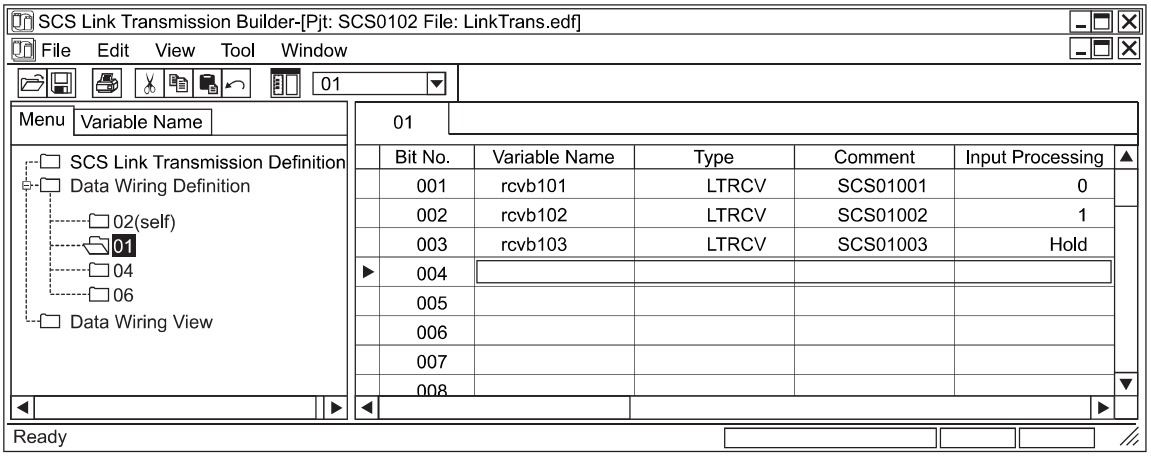


Figure A6.3-3 Other Stations tab of Data Wiring Definition on SCS Link Transmission Builder (SCS)

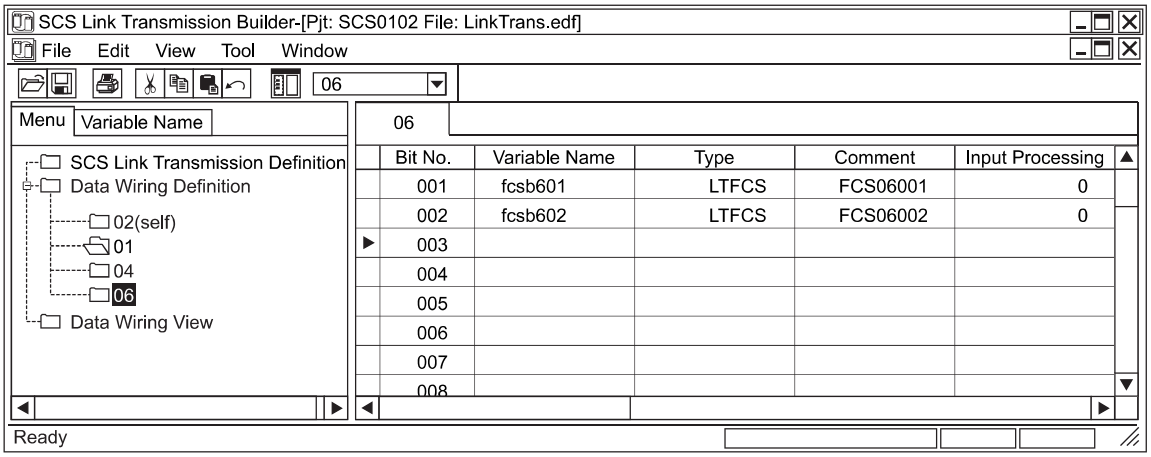


Figure A6.3-4 Other Stations tab of Data Wiring Definition on SCS Link Transmission Builder (FCS)

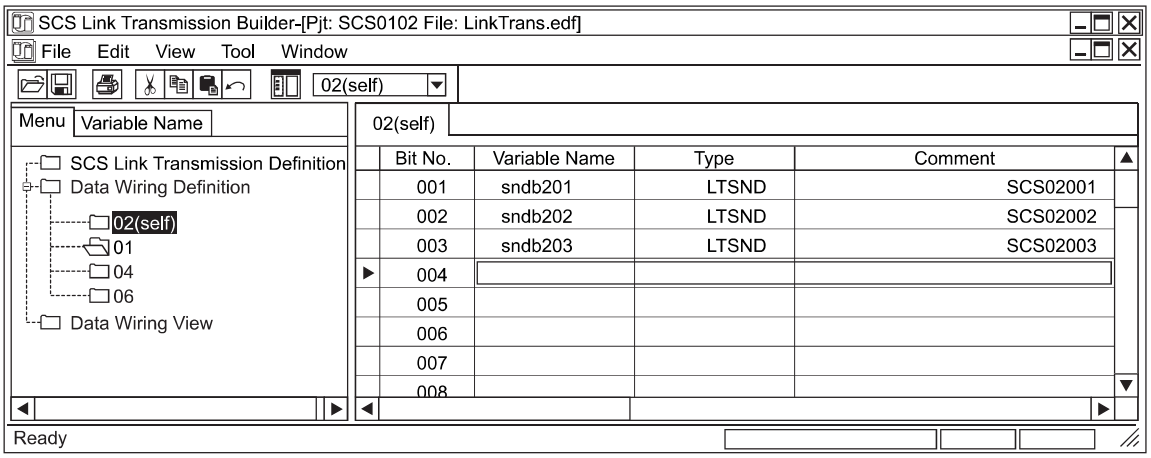


Figure A6.3-5 Self Station tab of Data Wiring Definition on SCS Link Transmission Builder

Bit No. (Bit number)

Shows the bit numbers in the SCS link transmission data area used for SCS Link Transmission. This number is not editable.

For SCS, the bit numbers are in the range of 001 to 128. For FCS, the range is 001 to 256.

Variable Name

Do any of the followings to set the instance name of SCS Link Transmission input/output FB to each variable name.

- Enter the variable name directly.
- Double-click a variable name displayed in the "Variable Name" tab in the left pane.
- Drag a variable name from Dictionary View and drop it into the Variable Name field.

A variable name can contain up to 69 single-byte characters.

To globally identify an internal variable that has been declared as a local variable, affix an @ character and scope name to the variable.

For accessing the internal variable of a user-defined function block, the user-defined function block itself should be assigned with an instance name on Dictionary View. Then the variable name becomes "<Instance Name>.<Internal Variable Name>." The variable can be accessed through two nests.

SCS Link Transmission Builder checks the following items:

- The variable name consists only of alphanumeric characters and "@", "." or "_". If any other character is used, an error will occur.
- The variable name begins with an alphabetic character or "_," otherwise, an error will occur.
- If the number of nests is three or more, an error will occur.
  For example, the variable name FB01.VAR3@PROG1 (Internal variable VAR3 of a user-defined function block instance FB01 in PROG1) has one nest; the instance "FB01.FB02.VAR3" (Internal variable VAR3 of a user-defined function block instance FB02 used in the user-defined function block instance FB01) has two nests.

  The selectable variables vary with the station types. The SCS Link Transmission I/O FBs for the variables corresponding to the station types are as follows:

Table A6.3-1 Station types and SCS Link Transmission I/O FBs

Station Type	SCS Link Transmission I/O FB
Self Station	LTSND (Link Transmission Data Output FB)
Other Station (SCS)	LTRCV (Safety Link Transmission Data Input FB)
Other Station (FCS)	LTFCS (Interference-free Link Transmission Data Input FB)

When setting a variable name from Dictionary View, the procedure is as follows.

Drag a variable name from Dictionary View and then drop it into the Variable Name field of Link Transmission Builder. Variable names can be specified for Link Transmission Builder. When dragging multiple variable names, they will be dropped from the beginning field. The existing variable names in the fields will be overwritten.

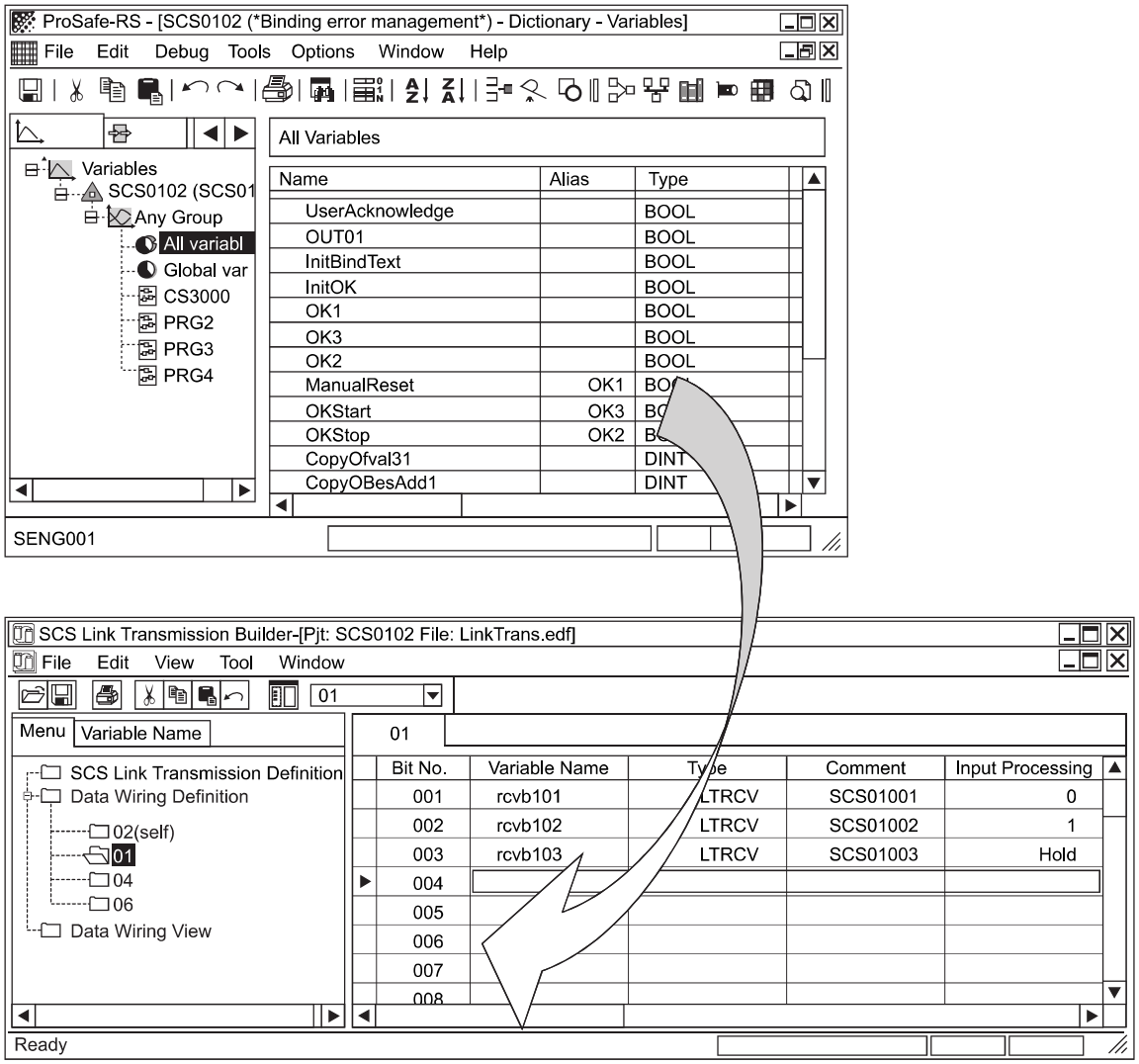


Figure A6.3-6 Drag and drop from Dictionary view

Type

Displays the SCS Link Transmission I/O FB types corresponding to the station type. This item is not editable.

Comment

Displays the comment of the variable. This item is not editable.

Input processing at fault

When a data's status becomes BAD, a predefined value can be set to the logic data. This is valid only when "Other Stations" is selected.

The input value to be set to the data at error occurrence is selectable from the following options, [0],[1] or [2]. The initial setting is 0.

Table A6.3-2 Input processing at fault

Option	Setting Value	Description
0	0	Set the input data to 0 when the input becomes error.
1	1	Set the input data to 1 when the input becomes error.
2	Hold	Hold the current value when the input becomes error.

Wiring View

Shows the list of Data Wiring Definition.

In this window, the wiring definitions are displayed with the format where the Self-Station is placed at the first and followed by Other Stations sorted by bit numbers. All data of the local station and up to 1000 data of the other stations can be displayed. This window is not editable.

Double-clicking a variable name, the Data Wiring Definition window regarding the variable will be displayed.

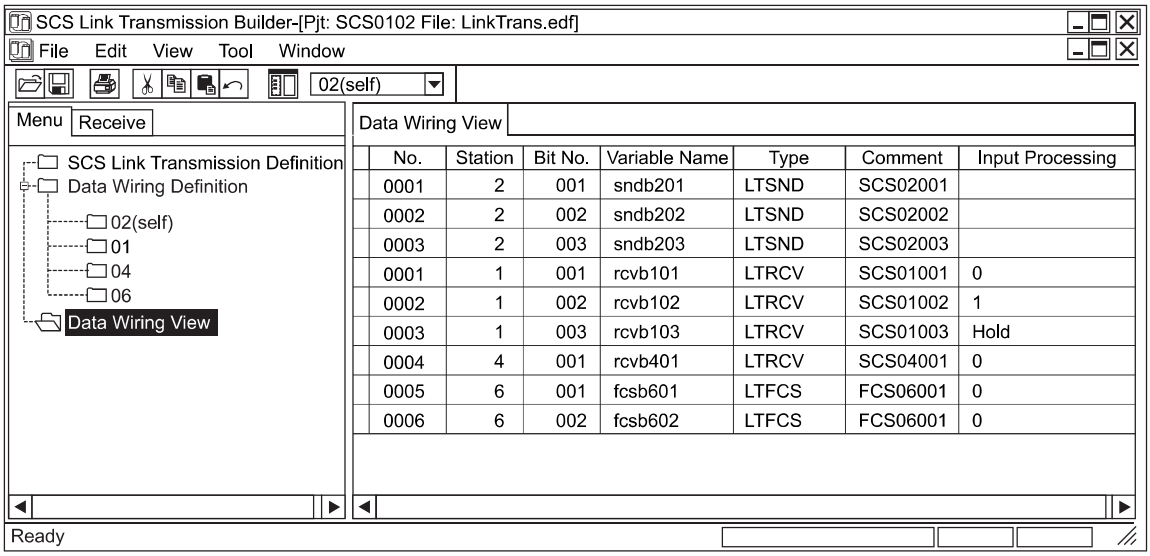


Figure A6.3-7 Data Wiring View on SCS Link Transmission Builder

Notes on reusing data defined by SCS Link Transmission Builder

In the following operation, the settings for the SCS Link Transmission Definition and the settings for wiring must be edited.

- Importing the 'data that was set to Station A for Link Transmission' to Station B
- In the SCS Project Properties dialog box, changing the station number of the SCS project from A to B

Notes for importing data and notes for changing station number are the same. Notes for importing SCS Project are given below.

The status of the imported data after SCS Link Transmission Builder saves them is as follows:

- The content of the SCS Link Transmission Definition settings is the exported data from Station A.
- The data for 'Self Station' tab in the Wiring Definition settings exported from Station A is automatically set to the 'Self Station' tab data for Station B. The contents of other stations remain unchanged.

IMPORTANT

Even if the exported SCS Project has a different Station type (SCS or FCS) in the Link Transmission Definition settings from the importing SCS Project, only the message meaning 'The data being edited will be lost. OK?' appears. Note that no dialog box to confirm the change in the Station type will appear.

An example of exporting data from Station A (SCS0101) and importing it to Station B (SCS0102) is shown below.

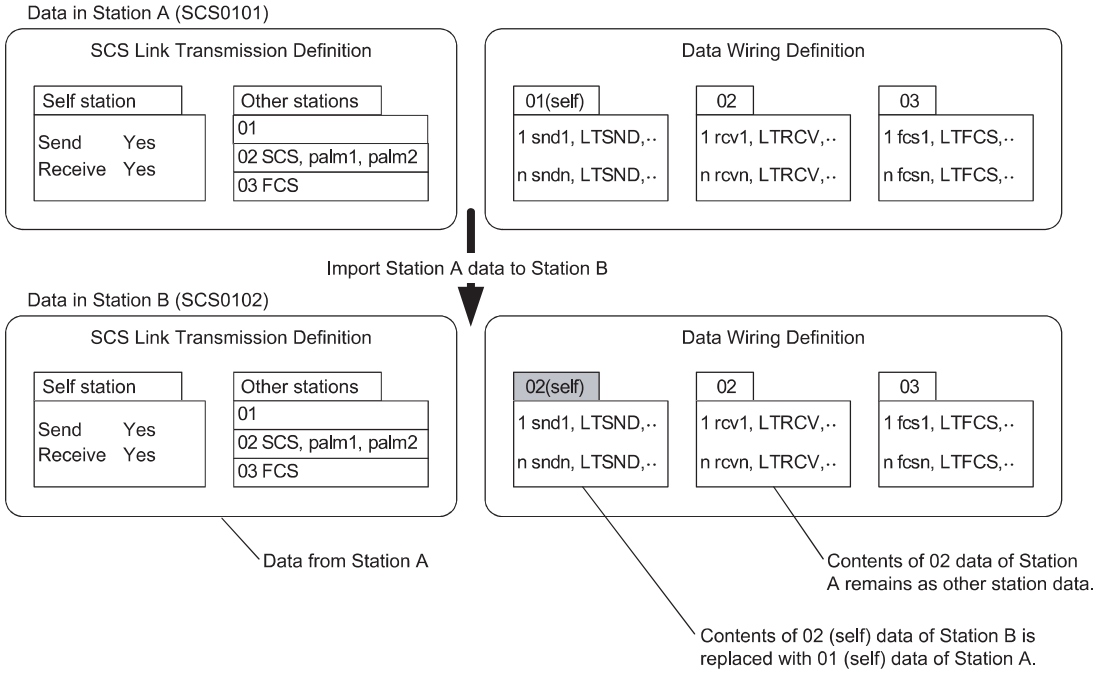


Figure A6.3-8 Example of importing Station A (SCS0101) Data to Station B (SCS0102)

As shown in the previous figure, the "Self Station" tab data of Station B (SCS0102) is replaced with the "Self Station" data in Wiring Definition settings of Station A (SCS0101).

If the Link Transmission Definition settings and Wiring Definition settings with Station B are made in Station A, the Link Transmission Definition settings and Wiring Definition settings in Station B will remain as "Other Station" data after the import.

If one station number is defined as both "Self Station" and "Other Station" an error is raised at a build. To avoid this, follow the steps below.

If the old Station B data is not needed,

1. After importing the Station A data to Station B, delete the Station B ("02" in the example) that is defined as "Other Station" in the SCS Link Transmission Definition settings of Station B and save the changes.
2. In the Dictionary View, delete related variables.
3. Edit the contents of the SCS Link Transmission Definition settings and Wiring Definition settings.

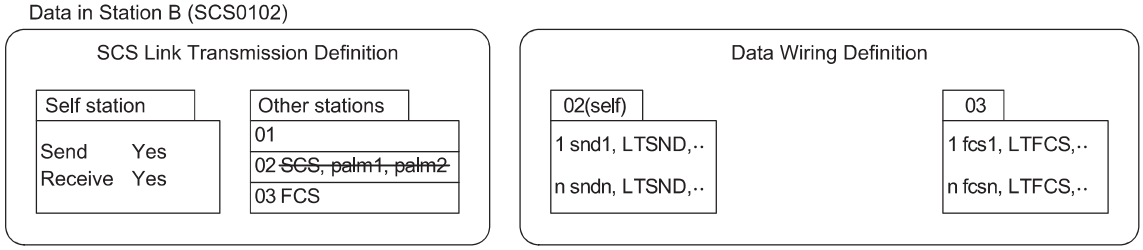


Figure A6.3-9 Case where the old Station B data is not needed

If the old Station B data needs to be saved,

1. After importing the Station A data to Station B, define a new station ("04" in the example) to move the Station B data that was defined as Other station ("02" in the example) in SCS Link Transmission settings to.

2. In Wiring Definition settings, copy the Station B data and paste it to the newly defined station.

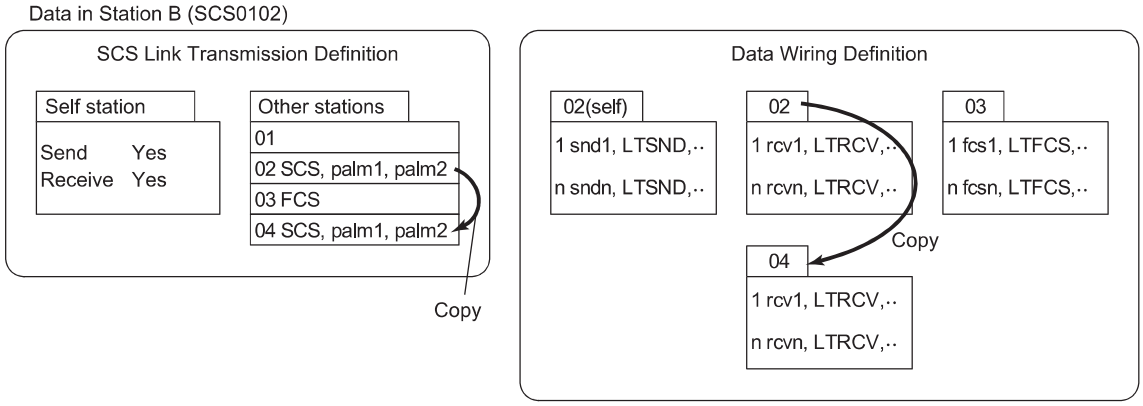


Figure A6.3-10 Data transfer when Station B data needs to be saved

3. In the SCS Link Transmission Definition settings, delete the Station B that is defined as Other station ("02" in the example) and then save the changes.
4. Edit the related variables in the Dictionary View if necessary.
5. Edit the contents of the SCS Link Transmission Definition settings and Wiring Definition settings.

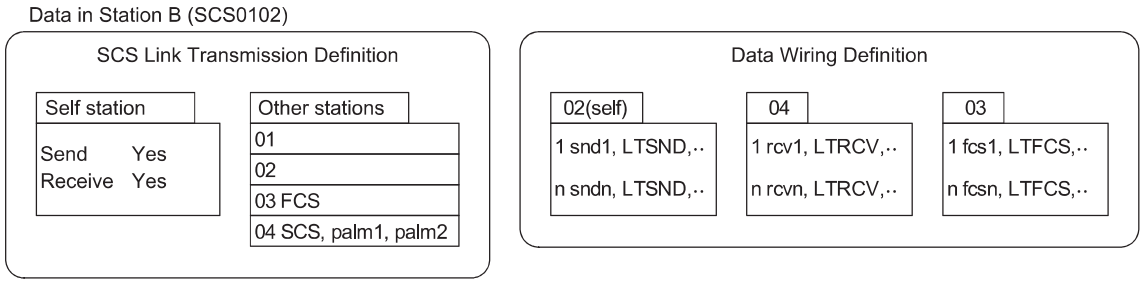


Figure A6.3-11 Structure when the old Station B data needs to be saved

A6.4 Actions taken for SCS link transmission when SCS is unsteady

This section explains the actions taken for SCS link transmission safety communication when the SCS is unsteady, as well as the operation at a SCS link transmission error occurrence.

SEE ALSO For more information about behavior of SCS global switch communication when the SCS is unsteady, refer to:

A6.5, “SCS global switch communication” on page A6-24

SCS link transmission safety communication during SCS startup

During SCS startup, SCS link transmission safety communication is processed in the following manner.

Start of reception

When the SCS is started, reception of SCS link transmission starts.

Start of sending and status of data

Even when the SCS is started, if the output enable operation is not performed, SCS link transmission data will not be sent. In this case, logical data of the receiving side link transmission data area will be the input value at error occurrence specified in [Input Processing at Fault] item of Data Wiring Definition in SCS Link Transmission builder (FALSE if specified as HOLD). The data status will be BAD.

When the output enable operation is performed at the sending side SCS, sending of data starts and logical data of the receiving side SCS's link transmission data area will be the value sent by the sending side SCS, and the data status will be GOOD.

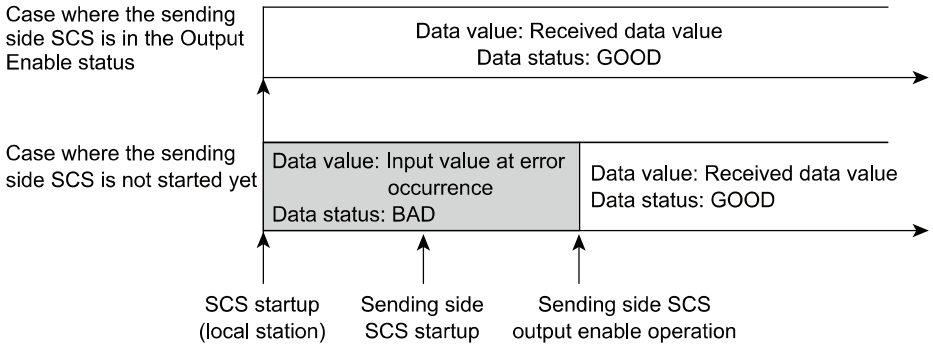


Figure A6.4-1 SCS link transmission safety communication receive data during SCS startup

TIP After the output enable operation is performed, sending of SCS link transmission will not be placed in the Output Disable status until the SCS is stopped.

Notification of errors and recovery during SCS startup

During the SCS startup, errors related to SCS Link Transmission are handled as follows:

- During the SCS startup, no diagnostic information message on SCS Link Transmission errors will be sent. After the error status during the startup turns to normal, diagnostic information message on errors will be sent at the error occurrence.
- No diagnostic information message notifying recovery from errors of SCS Link Transmission that occurred during the SCS startup will be sent.

Diagnosis of SCS link transmission safety communication

During inter-SCS link transmission safety communication, the following diagnoses are performed.

- The receiving side SCS checks if correct data is received within the reception interval timeout value (OUTT). If a timeout occurs, it is judged that a communication error has occurred. Until then, the last normal value is retained.
- In addition to the setting data, the sending side SCS appends data to guarantee communication quality and sends the data to the communicating SCS. The receiving side SCS performs various verifications to confirm validity of data sent by the sending side SCS. If the result of verification indicates abnormality, it is judged that a communication error has occurred.

Processing upon SCS link transmission safety communication error

When the result of SCS link transmission safety communication diagnoses indicates an error, the following processing takes place.

Receive data/data status

- Logical data of the link transmission data area received will be set according to the specified input value at error occurrence defined in the Data Wiring definition of SCS Link Transmission Builder.
- The data status will be BAD.

The data and data status above are output from the LTRCV function block.

Notification of communication error

A diagnostic information message indicating "Diagnostic Error" will be sent from each receiving station where a communication error has occurred. However, no diagnostic information message notifying errors related to SCS Link Transmission will be sent during the SCS start-up.

SEE ALSO For more information about diagnostic information messages, refer to:

Message Number 4133 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)

Processing upon recovery from SCS link transmission safety communication error

After the cause of communication error is removed and receive data from the SCS becomes normal, the error condition recovers automatically. If latching the data at communication error is necessary, write the data latching logic in application logic.

Receive data/data status

- Logical data of the link transmission data area received will be the value sent by the sending side SCS.
- The data status will be GOOD.

The data and data status above are output from the LTRCV function block.

Notification of recovery from communication error

A diagnostic information message indicating "Recovery from Diagnostic Error" will be sent from each receiving station where a communication error has been recovered. However, no diagnostic information message related to SCS Link Transmission notifying the recovery from the errors that occurred during the SCS startup will be sent.

SEE ALSO For more information about diagnostic information messages, refer to:

Message Number 4134 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)

SCS link transmission during switching of CPU control right

Switching the control right of a dual-redundant CPU module does not affect the receive data.

SCS link transmission during error at one side of control bus

An occurrence of error at one side of control bus does not affect the receive data.

A6.5 SCS global switch communication

By using SCS global switch communication of the SCS link transmission function, data can be sent and received between a CENTUM station (FCS, APCS, and GSGW, hereafter collectively referred to as FCS) and an SCS.

A6.5.1 Referencing FCS data from SCS

When sending of global switch value to other stations is permitted at an FCS, values set from %GS001 to %GS256 at the FCS can be received at an SCS as BOOL-type data.

Referencing FCS data

The LTFCS function block is used to reference FCS %GS data. LTFCS is an interference-free function block. It cannot be used for safety loop.

Data referenced with the LTFCS function block is defined by wiring the link transmission data area and LTFCS function block in SCS Link Transmission Builder.

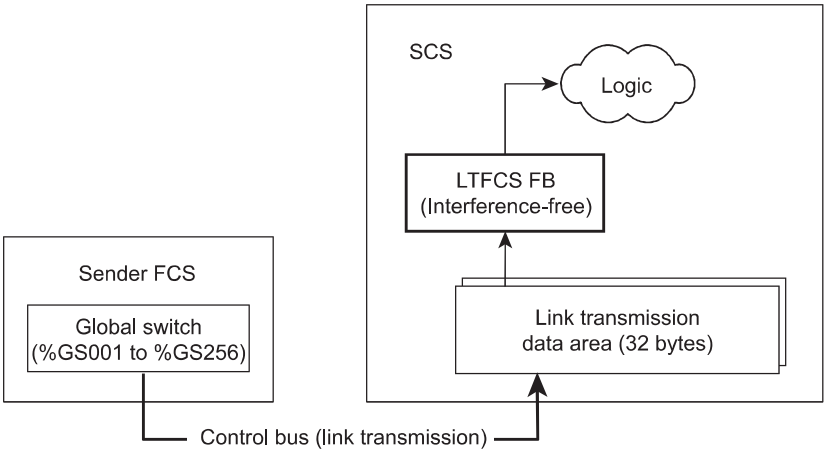


Figure A6.5.1-1 Referencing FCS data

Data check using CENTUM

- For data set to an SCS from an FCS, check global switch data of the FCS.
- To check the data received at an SCS from CENTUM stations, connect BOOL data to GSV parameter of the LTFCS function block and give a tag name to the BOOL data.
- To check the status of data received at an SCS from CENTUM stations, connect BOOL data to STS parameter of the LTFCS function block and give a tag name to the BOOL data.

Diagnosis of communication error

The communication status with an FCS is checked at an SCS. Regardless of the scan period of SCS application logic, if data update from the FCS stops for 3 seconds, the SCS judges that a communication error has occurred and starts the input processing at fault. Possible causes of communication error are shown below.

- The sending side FCS failed.
- Control bus failed on both bus 1 and bus 2.

Processing upon communication error

If a SCS global switch communication error, including the sending side FCS stop, has occurred, the SCS starts the input processing at fault.

Receive data/data status

- Logical data of the link transmission data area received by the SCS will be set depending on the input value at error occurrence defined on the Data Wiring definition of SCS Link Transmission Builder.

- The data status will be BAD.

The data and data status above are output from the LTFCS function block.

Notification of communication error

A diagnostic information message indicating "Diagnostic Error" will be sent from the SCS. However, no diagnostic information message notifying errors related to SCS Link Transmission will be sent during the SCS startup.

SEE ALSO For more information about diagnostic information messages, refer to:

Message Number 4133 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)

Processing upon communication error recovery

After the cause of communication error is removed and the receive data from the FCS becomes normal, the error condition recovers automatically. If latching the data at communication error is necessary, write the data latching logic in application logic.

Receive data/data status

- Logical data of the link transmission data area received by the SCS will be the %GS value sent by the FCS.
- The data status will be GOOD.

The data and data status above are output from the LTFCS function block.

Notification of recovery from communication error

A diagnostic information message indicating "Recovery from Diagnostic Error" will be sent from the SCS. However, no diagnostic information message related to SCS Link Transmission notifying the recovery from the errors those occurred during the SCS startup will be sent.

SEE ALSO For more information about diagnostic information messages, refer to:

Message Number 4134 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)

A6.5.2 Data setting from SCS to FCS

If reception of global switch values from other stations is permitted at an FCS, data from the link transmission data area of an SCS can be received by the FCS as global switch data %GS001 to %GS128. The data received at FCS from %GS129 to %GS256 are meaningless and thus should not be referenced on the FCS side.

FCS data setting

The LTSND function block is used for setting data to an FCS. Input the BOOL-type data to be sent to the LTSND function block, and perform wiring between the LTSND function block and link transmission data area in SCS Link transmission builder.

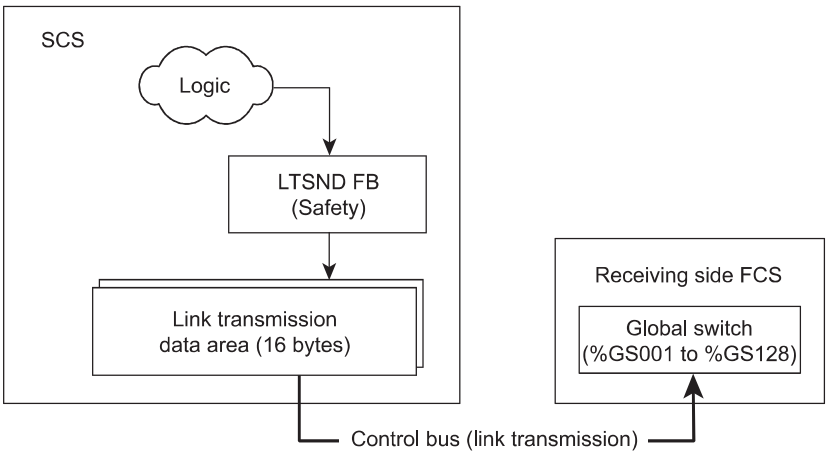


Figure A6.5.2-1 FCS data setting

SEE ALSO For more information about flow of engineering procedures, refer to:

"■ SCS link transmission" on page B7-32

For more information about engineering functions required for engineering, refer to:

A6.3, "SCS link transmission definition" on page A6-11

For more information about precautions regarding FCS data setting, refer to:

A6.1, "Overview of the SCS link transmission" on page A6-2

When SCS is in the Output Disable status

When the data sending side SCS is in the Output Disable status, %GS of the FCS is set to 0 and the data status will be BAD.

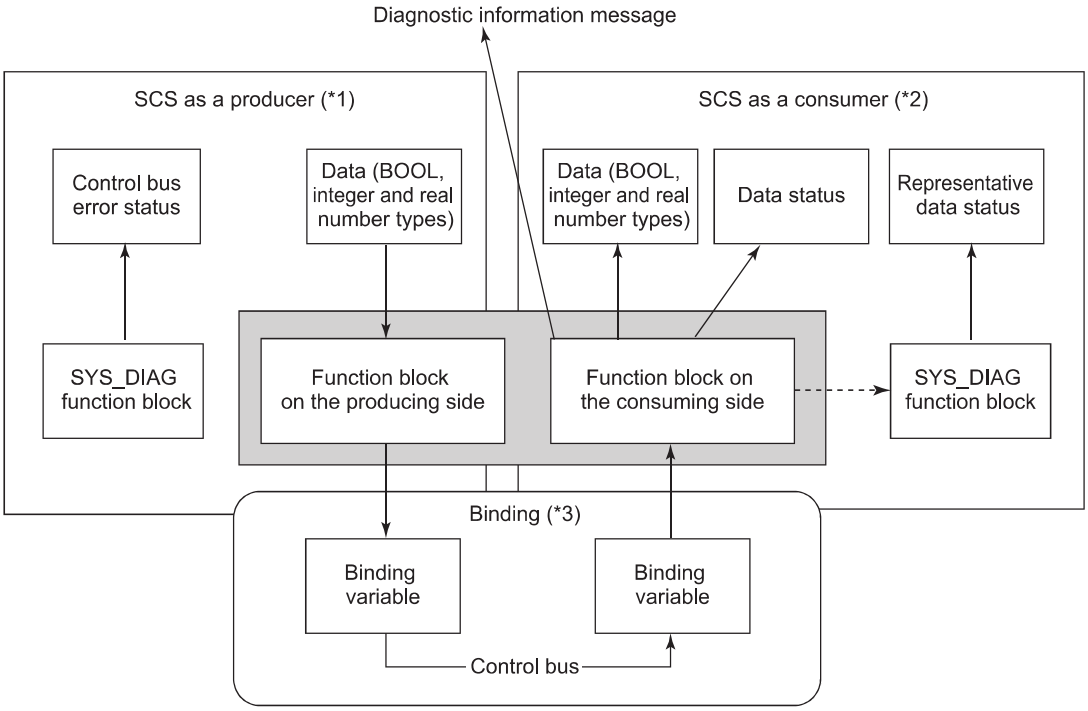
After the SCS output enable operation is performed, data specified in SCS Link Transmission Builder will be set to %GS and the data status will change to GOOD.

A7. Inter-SCS safety communication

An SCS is able to perform safety communication with other SCSs in the same domain as well as in different domains. This means that the user can create a safety-loop covering two SCSs.

Structure of Inter-SCS safety communication function

The following figure shows an overview of Inter-SCS safety communication.



*1: An SCS that creates and sends a binding variable
*2: An SCS that receives and reads the binding variable
*3: A mechanism for passing a binding variable of the SCS on the producing side to the SCS on the consuming side

Figure A7-1 Overview of inter-SCS safety communication

Outline of the inter-SCS safety communication

In ProSafe-RS, it is possible to perform the Inter-SCS safety communication in the same control bus domain or in different control bus domains. The inter-SCS safety communication is a one-way communication of one-to-one variable between SCSs. The inter-SCS communication can be used to build the safety loop between SCSs.

To perform the Inter-SCS safety communication, the application logic using the dedicated FB is generated in each SCS of the sender and the receiver. Variables called binding variable are used to bind each variable of the sender and the receiver.

The following example explains the inter-SCS safety communication which sets BOOL variable X to variable Y.

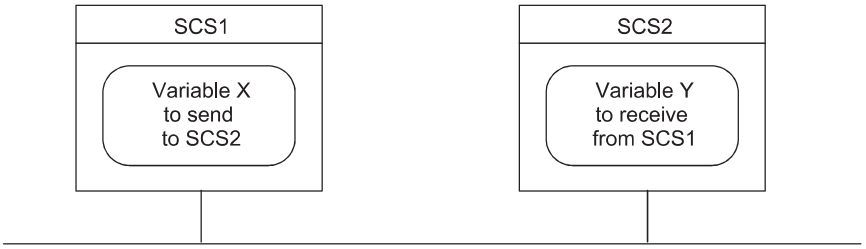


Figure A7-2 An example of a project

Generate FB (PROD_B, PROD_I, PROD_R) for communication on the sender side (the producer) in SCS, and FB (CONS_B, CONS_I, CONS_R) for communication on the receiver side (the consumer) in SCS in order to implement this Inter-SCS safety communication. To connect the sender and the receiver, define the binding variables ("P0101001" and "C0101001" in the figure shown below) for each side.

The binding variables in pairs are connected in Binding List View.

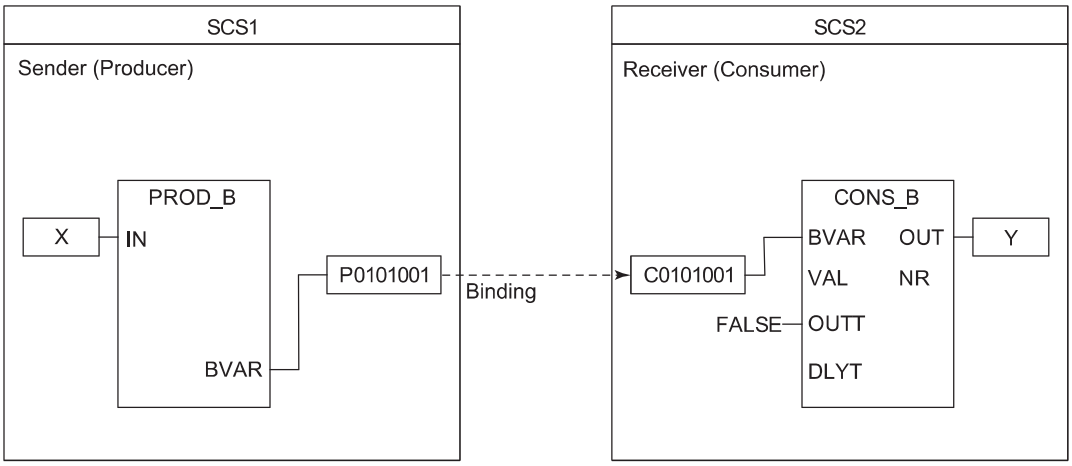


Figure A7-3 Inter-SCS communication application

The following status indicates how the Inter-SCS safety communication is performed.

- Control bus fault status indicating whether or not the SCS (the producer, the consumer) is communicable.
- Data status and Representative data status showing that data can be received normally (the consumer)
- Diagnostic information message about communication error and recovery (the consumer)

Several data sent in the same scan timing from the producer are certainly received in the same scan timing in the consumer.

SEE ALSO For more information about how to define inter-SCS communication, refer to:

A7.1, "Inter-SCS safety communication definition" on page A7-12

Mechanism of inter-SCS safety communication

Inter-SCS safety communication is achieved by function blocks dedicated for inter-SCS safety communication. The function block on the producing side sends setting data as well as data for guaranteeing communication quality to the communicating SCS via the control bus. The communication path can be between SCSs in the same domain or SCSs in different domains. In a configuration with CENTUM integration, inter-SCS safety communication can be performed while CENTUM devices are connected to the same control bus. The function block on the consuming side performs various tests on received data to check the validity and only outputs data whose quality can be guaranteed. If data is judged to be incorrect as a result of

these tests, the fail-safe value preset on the consuming side is output. Make sure to create an application logic to be used when data is not correct.

IMPORTANT

The output enable operation is required in order for the SCS on the producing side to perform transmission. The function block on the consuming side outputs the specified fail-safe values and communication status (parameter NR) becomes abnormal (FALSE) until the output enable operation is performed.

SEE ALSO

For more information about BOOL-type data reception, refer to:

6.4, “CONS_B (inter-SCS safety communication BOOL-type data consumer)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about DINT-type data reception, refer to:

6.5, “CONS_I (inter-SCS safety communication INTEGER-type data consumer)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about REAL-type data reception, refer to:

6.6, “CONS_R (inter-SCS safety communication REAL-type data consumer)” in POU Reference Manual (IM 32P03B20-01EN)

Operation when launching inter-SCS safety communication

- The function block on the consuming side outputs the fail-safe values predefined in the function block, until the SCS on the producing side starts sending data and the function block on the consuming side is ready to correctly receive the data sent by the SCS on the producing side. The communication status (parameter NR) remains abnormal (FALSE) during this period.
- When you start up the SCS on the producing side and perform the output enable operation, inter-SCS safety communication starts sending data. Once the sent data is successfully received by the SCS on the consuming side, the function block on the consuming side will output the received data and the communication status will change to normal (TRUE).

Operations at inter-SCS safety communication errors

If a communication error occurs during inter-SCS safety communication, the following operations are performed.

- The fail-safe value preset on the function block for inter-SCS safety communication on the consuming side is output.
- The communication status (parameter NR) becomes abnormal (FALSE).
- A diagnostic information message notifying about the error is output.

The following operations are performed if the system recovers from a communication error.

- The data value received from the producing side is output from the function block on the consuming side.
- The communication status (parameter NR) becomes normal (TRUE).
- A diagnostic information message notifying about the recovery is output.

The following table shows the operations that are performed for each error status.

Table A7-1 Operations at communication errors

Status	Output on the consuming side	Remarks
The SCS on the producing side has stopped	The previous value is retained after the communication stops. After the reception interval timeout period is exceeded, the fail-safe value is output.	Start up the SCS on the producing side and perform the output enable operation to restore communication.
An error has occurred in the communication path and communication has stopped for a long period	Same as above. The data value is output when the communication is resumed.	-
An error has occurred in the communication path and communication has stopped temporarily	The previous value is retained while the communication is stopped. The data value is output when the communication is resumed.	This applies when communication is resumed within the reception interval timeout period
An error has occurred in the communication path and the contents of the communication have been destroyed	The previous value is maintained as long as the communication data is corrupted. The data value is output when correct data is received.	The fail-safe value is output if the communication data is corrupted for longer than the reception interval timeout time.
There is a delay in the communication path and communication is very slow	The fail-safe value is output if the communication is delayed more than the transmission delay timeout period. The data value is output when the communication is resumed. The transmission delay is not checked if the transmission delay timeout value is set to 0.	-
Erroneous engineering is performed.	The fail-safe value is output and a diagnostic information message is output.	When a wrong binding variable name is used.

Precaution for engineering

This section describes precautions and important issues in using the Inter-SCS safety communication.

Communicable extent

Safety communication that guarantees the safety of SIL3 or SIL2 for the SCS used is possible between the SCSs in Vnet/IP domains and the V-net domains. Even if control communication and open communication coexist on the Vnet/IP network, safety of SIL3 or SIL2 is guaranteed.

SEE ALSO For more information about precautions when SCS in V-net is included in the route of inter-SCS safety communication, refer to:

Appendix 4.2, “Inter-SCS safety communication in a V net domain” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Inter-SCS safety communication capacity

The number of data handled in Inter-SCS safety communication is as follows:

- The maximum number of data that one SCS can send is up to 200.
- The maximum number of data that one SCS can receive is up to 200.

The number of binding connections in each SCS should be 16 or less. This number is a total of connections from both sender and receiver.

- Connections on the sender side
  This is the number of all consumer binding groups that are mapped to all binding groups defined as producers on the local SCS.

- Connections on the receiver side
  This is the number of all binding groups that are defined as consumers on the local SCS.

The following figure shows how to calculate the number of binding connections.

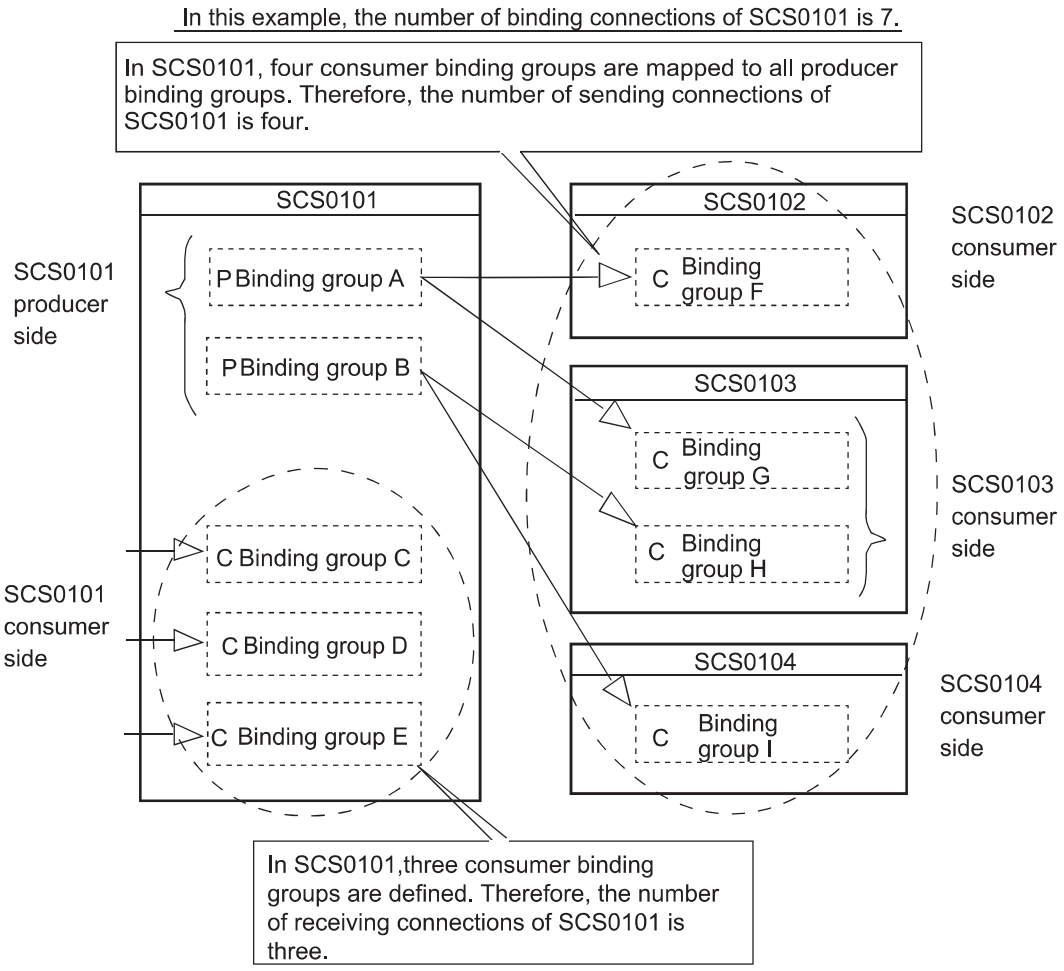


Figure A7-4 Calculating the number of binding connections

SEE ALSO For more information about range in which inter-SCS safety communication is possible, refer to:

- "● Communicable extent" on page A7-4
- Appendix 4.2, "Inter-SCS safety communication in a V net domain" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)
- "■ Inter-SCS safety communication in systems in which a V net domain and a Vnet/IP domain are connected" in Appendix 4.4, "System expansion with V net router connection" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

● Important issues to consider

- When an error occurs in Inter-SCS safety communication, a diagnostic information message is output and the fail-safe value (VAL) is set to the output of FB (OUT) for communication on the consumer. You need to design so that a proper value is set to VAL of the consumer communication FB while considering the system operations.
- The FB that is used in Inter-SCS safety communication does not have a latch function. Therefore, the value of the binding variable is output when returning from the error. You need to make the latch function in the application if necessary, in order to control the error condition and he release from the error condition by using the application.

- The above-mentioned error will be automatically recovered. A diagnostic information message is output at the recovery. The output of FB for communication on the consumer is also automatically recovered to the received data from the output value at the occurrence of an error.

IMPORTANT

- Value of a binding variable on the producer side of the Inter-SCS safety communication must not be set in two or more locations.
- Changing the binding list online causes an error at the builder.
- If you use inter-SCS safety communication, SCS projects on the consumer side and the producer side must be upgraded at the same time. If either of the SCS projects is opened by using upgraded SCS Manager, the opened SCS project is upgraded. The SCS project on the other SCS must also be upgraded by opening it with SCS Manager with the same software release number. If the revisions of the SCS projects do not match, a build error will occur.
- The software release number must be the same between all the SENGs which is for engineering SCS projects in the RS project, and SENGs which is for engineering SCSs that perform inter-SCS safety communication each other. Also, you must upgrade the revision of SCS projects that perform inter-SCS safety communication.
- Inter-SCS safety communication bindings cannot be changed online. Changing bindings (for example, adding inter-SCS safety communication or changing the SCS with which you are communicating) requires an offline download of the SCS on both the producer and consumer sides. For details, see the following “CAUTION” section.

CAUTION

- The logic for inter-SCS safety communication and the wiring of inter-SCS safety communication FB can only be changed online. For example, only the input wiring for communication FB on the producer side (see wiring A in the following figure) or the output wiring for communication FB on the consumer side (see wiring B in the following figure) can be changed. Do not make online changes for the wiring between the communication FB on the producer side and the communication FB on the consumer side. If this wiring is changed online, an error occurs in the communication FB on the consumer side, and then a fail-safe value is generated.

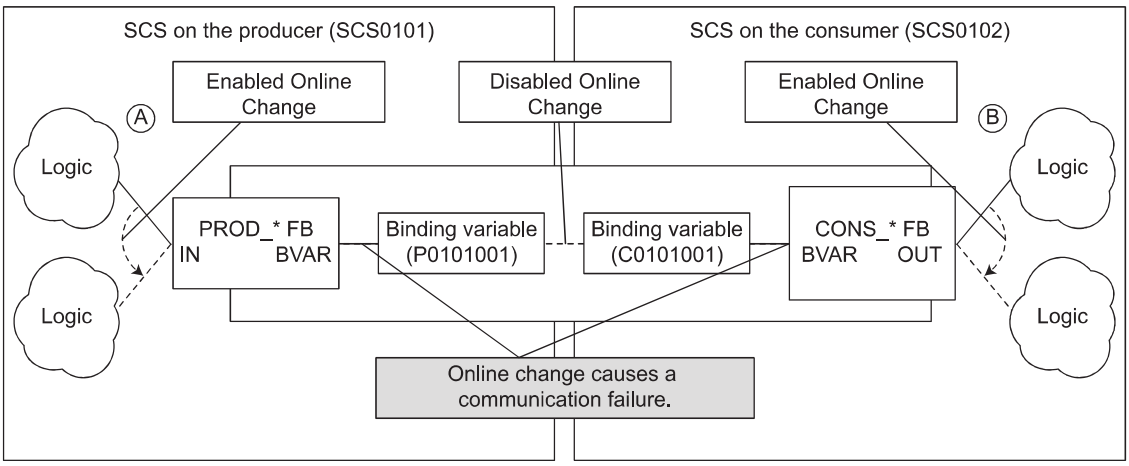


Figure A7-5 Wiring of Inter-SCS safety communication is changed online

- If the producer binding group is changed, you need to perform offline download of the group on the producer SCS as well as on every consumer SCS that references the changed binding groups. You must perform offline download irrespective of the changed contents. For example, when a variable is deleted from the binding group on the producer SCS, offline downloading is necessary on the consumer SCS even if this variable is not referenced by any consumer SCS.
- When making a wide-area connection via CGW or WAC routers, you must consider whether inter-SCS safety communication through the wide-area network is really necessary. Especially, when using a satellite connection, which is sensitive to the weather, as an inter-exchange channel, you must pay attentions because a trip may easily occur in inter-SCS safety communication. When the wide-area network does not have high performance or reliability, inter-SCS safety communication will be delayed. Then, the inter-SCS safety communication will time out due to this delay, and there will be a possible occurrence of a false trip.

  Moreover, when performing inter-SCS safety communication through WAC routers, you must set an appropriate bandwidth limit on the System View so that the inter-SCS safety communication is always given priority.
- You must use the Inter-SCS Communication Lock Window to perform lock operation on inter-SCS safety communication. If you lock the binding variables directly from the Multi-Language Editor or Dictionary, an error occurs in the consumer FBs that receive locked variables and fail-safe values are output. This may cause a false trip depending on the application.

- As a general rule, FBs for inter-SCS safety communication should be used after creating instances with names by using the Dictionary. If instance names are not assigned to inter-SCS safety communication FBs, inter-SCS safety communication is performed normally. However, the instance names that are displayed on the Inter-SCS Communication Lock Window and in system alarm messages are automatically assigned by SCS Manager.

- You must connect inter-SCS safety communication FBs and bind variables directly. If you insert any variables, function blocks, or parameters between them, forcing and monitoring cannot be performed.

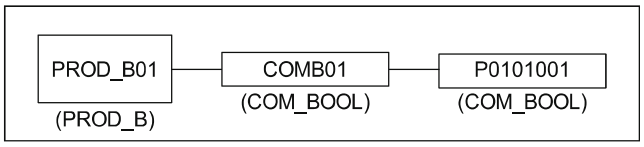


Figure A7-6 Example where FB and variable are not directly connected

- Do not use inter-SCS safety communication FBs as parameters of function blocks. If you use inter-SCS safety communication FBs as parameters, they are not displayed on the Inter-SCS Window. Also, forcing cannot be performed.

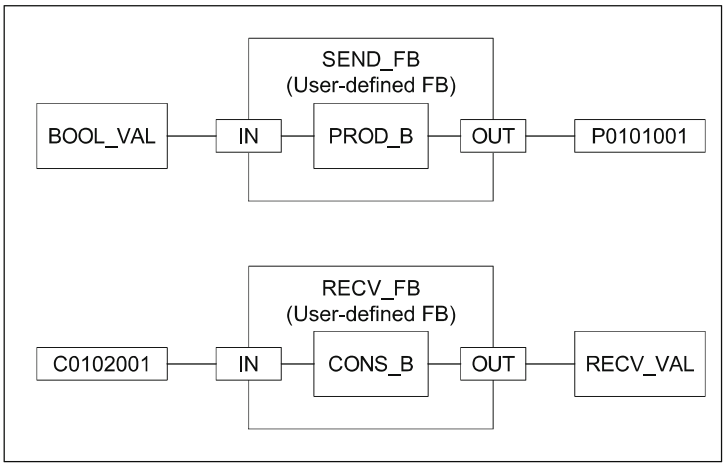


Figure A7-7 Example where Inter-SCS safety communication FBs are used as parameters

- Note that when multiple binding variables are connected to a single producer FB, if you perform forcing by selecting a line corresponding to a binding variable on the Inter-SCS Communication Lock Window, the values of all binding variables that are connected to the same producer FB will be changed. You must be careful.

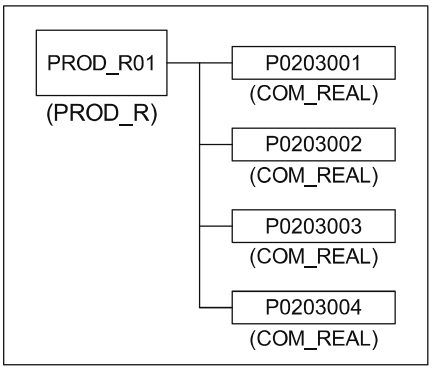


Figure A7-8 Example of multiple binding variables connected to a single producer FB

Inter-SCS Safety Communication FB — All FB

Station	L	D	Variable	Variable Type	Instance	FB Type	Logical Value	Physical Value	Variable Comment
SCS0203			P0203001	COM_REAL	PROD_R01	PROD_R	TRUE	TRUE	
			P0203002	COM_REAL	PROD_R01	PROD_R	TRUE	TRUE	
			P0203003	COM_REAL	PROD_R01	PROD_R	TRUE	TRUE	
			P0203004	COM_REAL	PROD_R01	PROD_R	TRUE	TRUE	
SCS0201			C0201001.v C0201001.sts	COM_DINT	CONS_I01	CONS_I	TRUE GOOD	TRUE GOOD	
			C0201001.v C0201001.sts	COM_DINT	CONS_I02	CONS_I	TRUE GOOD	TRUE GOOD	
			C0201001.v C0201001.sts	COM_DINT	CONS_I03	CONS_I	TRUE GOOD	TRUE GOOD	

Figure A7-9 Example of the display on the Inter-SCS Communication Lock window (multiple binding variables connected to a single FB)

- The SCS system program of the SCS that performs inter-SCS safety communication must be R1.01.30 or later on both the producer and consumer sides.

  If Vnet/IP is used for the route of the Inter-SCS safety communication, the SCS system programs on the SCSs must be R1.02 or later on both the producer and consumer sides.

SEE ALSO For more information about how to upgrade the revision of SCS project, refer to:

C4.2.2, “Upgrading an SCS project” in Installation Guide (IM 32P01C50-01EN)

For more information about DLYT (transmission delay timeout value) calculation method when the SCS system program release number of either the producer side or the consumer side of inter-SCS safety communication is R2.03.51 or earlier, refer to:

“■ Specification changes made in SCS system program (Release number R2.03.51)” in Appendix 3.2, “The major changes in R2” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Inter-SCS safety communication timeout settings

There are two timeout settings for monitoring intervals for Inter-SCS safety communication. One is the reception interval timeout value (OUTT) and the other is the transmission delay timeout value (DLYT).

A temporary “transmission delay error” is detectable by OUTT. Set DLYT to detect a constant "transmission delay error."

- Reception Interval Timeout Value (OUTT)
  Intervals to receive data are checked in the CONS_* FB for communication on the consumer. When a data reception interval exceeds the timeout value (OUTT), a communication error occurs and then a fail safe-value (VAL) is output.
- Transmission Delay Timeout Value (DLYT)
  This is the checking of the time taken between the transmission of data by producer FB(PROD_*), and the reception of the data by consumer FB(CONS_*). This time is called Inter-FB transmission delay time. When the time exceeds the timeout value (DLYT) of CONS_* and that situation continues for the time of OUTT, a communication error occurs and a fail safe value (VAL) is output.
- Setting the Reception Interval Timeout Value (OUTT)
  OUTT accepts a setting of between 3 and 30 seconds. Ensure that you set a value equal to or higher than the value obtained using the following formula. If the result of the calculation is less than 3 seconds, set OUTT to 3 seconds or more.

  In case of executing the inter-SCS safety communication through WAC routers, if the calculated OUTT is less than 10 seconds, set OUTT as 10 seconds.

  OUTT = (select the longer scan period of either the producer or the consumer) x 8 + (Additional Delay)

Table A7-2 Additional delays by network configuration

Network configuration	Additional Delay
V net	No BCV/CGW used: 0 s Via BCV/CGW: number of BCVs used x 1 s + number of pairs of CGWs used x 2 s
Vnet/IP	Within a Vnet/IP domain: 0 s Between Vnet/IP domains (no WAN): 0 s (regardless of the number of Layer 3 switches) Between Vnet/IP domains (with WAN): 1 s (regardless of the number of Layer 3 switches) Between Vnet/IP domains connected via WAC routers (with WAN): 1.3 s (*1)
If a Vnet/IP domain and a V net domain are connected	V net delay (above) + Vnet/IP delay (above) + number of V net routers x 1 s

*1: When the revisions of two SCSs for inter-SCS safety communication is earlier than R2.03.59, perform either of the following:
- Install the SNTP server for each domain connected with the WAC routers to synchronize the time.
- If the SNTP server cannot be added, add 5 seconds to the additional delay of OUTT.

- Setting the Transmission Delay Timeout Value (DLYT)
  DLYT accepts a setting of between 3 and 30 seconds. Ensure that you set a value equal to or higher than the value obtained using the following formula. If the result of the calculation is less than 3 seconds, set DLYT to 3 seconds or more.

  DLYT= (scan period of the producer) + (scan period of the consumer) + (Additional Delay)

Table A7-3 Additional delays by network configuration

Network configuration	Additional Delay
V net	No BCV/CGW used: 300 ms Via BCV/CGW: number of BCVs used x 1.3 s + number of pairs of CGWs used x 2.3 s
Vnet/IP	Within a Vnet/IP domain: 300 ms Between Vnet/IP domains (no WAN): 300 ms (regardless of the number of Layer 3 switches) Between Vnet/IP domains (with WAN): 1.3 s (regardless of the number of Layer 3 switches) Between Vnet/IP domains connected via WAC routers (with WAN): 1.3 s + Transmission delay of WAN
If a Vnet/IP domain and a V net domain are connected	V net delay (above) + Vnet/IP delay (above) + number of V net routers x 1.3 s

IMPORTANT

If DLYT is set to 0 second and the Inter-FB transmission delay check is bypassed, the received data in the corresponding inter-SCS safety communications cannot be used for the purpose of safety.

- When the result of the calculation is OUTT < DLYT, OUTT should be changed to DLYT.
- The timeout times of the Inter-SCS Safety Communication must be taken into account to calculate the system reaction time depending on the safety engineering concept.

SEE ALSO

For more information about settings for the communication timeout in inter-SCS safety communication, refer to:

6., “Function blocks for inter-SCS communication (Safety FBs)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about DLYT (transmission delay timeout value) calculation method when the SCS system program release number of either the producer side or the consumer side of inter-SCS safety communication is R2.03.51 or earlier, refer to:

“■ Specification changes made in SCS system program (Release number R2.03.51)” in Appendix 3.2, “The major changes in R2” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

A7.1 Inter-SCS safety communication definition

With ProSafe-RS, it is possible to exchange data between SCSs. This section provides an overview of inter-SCS safety communication definition and engineering tasks, and explains the setting rules.

Overview of Inter-SCS safety communication definition

In order to implement inter-SCS safety communication, binding variables and inter-SCS communication function blocks are used to create application logics. BOOL-type, DINT-type and REAL-type data are grouped for each communicating SCS. Binding variables here stand for the identifiers that bind the SCS variables of sender and receiver.

The variables are defined in Dictionary View of SCS Manager.

The association among variables communicated is defined in Binding List View.

A variable that creates (sends) data is called a variable on the producing end and a variable that reads (receives) data is called a variable on the consuming end.

SEE ALSO For more information about details on Dictionary View which defines variables, refer to:

"Dictionary View" in "Workbench" in the Workbench User's Guide

For more information about details on Binding List View which links two variables between SCSs, refer to:

"External bindings" in "Variable Bindings" in "Link Architecture View" in "Workbench" in the Workbench User's Guide

Overview of engineering tasks when defining Inter-SCS safety communication

The following figure shows the overall scheme of applications for inter-SCS safety communication.

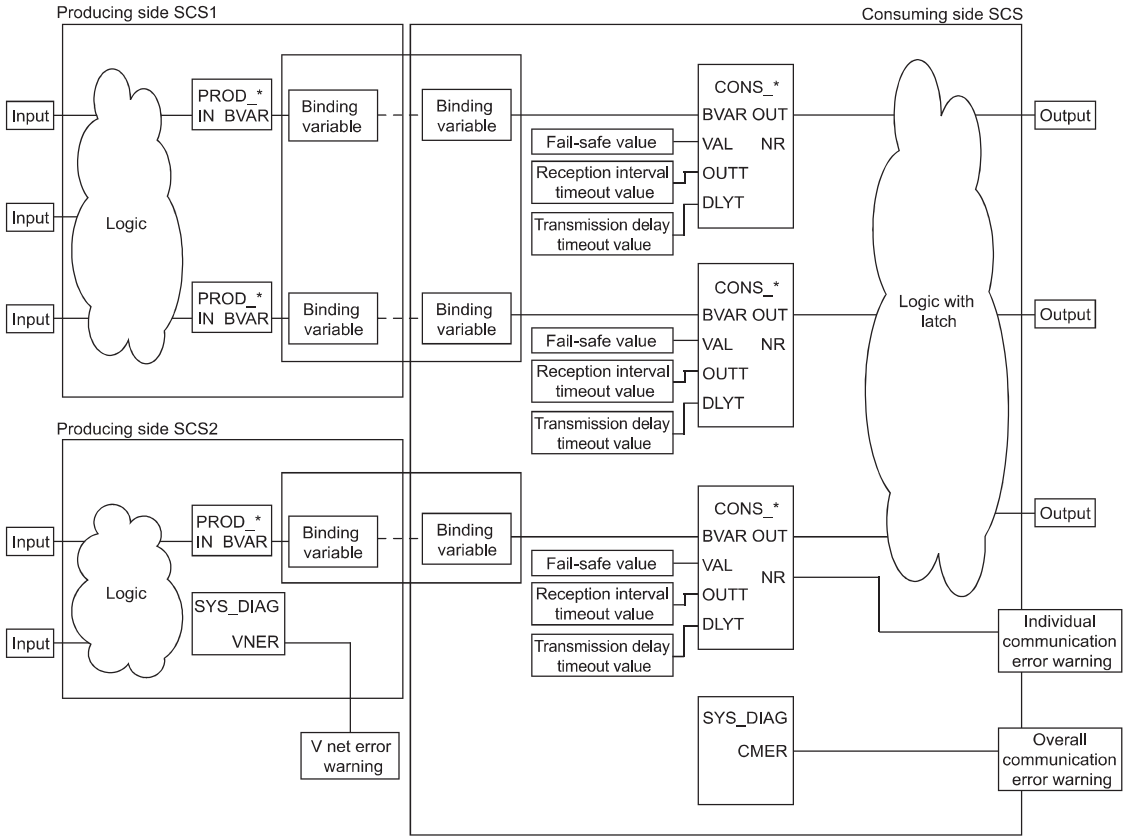


Figure A7.1-1 Overall scheme of applications

In order to communicate data between SCSs, group and define data in SCSs on the producing side and consuming side respectively. This section provides an overview of the engineering tasks.

Producing side

- Prepare an FB (PROD_B, PROD_I or PROD_R, hereinafter referred to as PROD_*) for inter-SCS safety communication for the producing side and a corresponding binding variable for each data.
- Define a global variable for the binding variable. Make sure to observe the naming rules for binding variables.
- Connect the variable to be sent with the input of the PROD_* and bind the output of the PROD_* with the binding variable.
- Make binding settings for the binding variable.
- Do not connect more than one output for PROD_* to one binding variable.
- It is recommended to describe information of the consuming side as the comment for the binding variable.
- Assign a binding group for each SCS on the consuming side.
- An error of V net communication can be output by using a SYS_DIAG. When engineering, VNER parameter of SYS_DIAG can be used for outputting the alarms.

SEE ALSO For more information about rules for naming binding variables, refer to:

"■ Binding variable" on page A7-15

Recommended guideline for engineering

For maintenance of Inter-SCS safety communication, it is recommended that the information on connection with the consume side should be written as a comment at the producer side in a program sheet.

Consuming side

- Prepare a binding variable, a corresponding FB (CONS_B, CONS_I or CONS_R, hereinafter referred to as CONS_*) for inter-SCS safety communication for the consuming side and a corresponding internal variable for each data.
- Define a global variable for the binding variable. Make sure to observe the naming rules for binding variables.
- Set a fail-safe value to be output in case the communication cannot be established or a communication error occurs and a timeout value (reception interval timeout value and transmission delay timeout value) for judging that a communication error has occurred for each data.
- Make binding settings for the binding variable.
- Assign a binding group for each SCS on the producing side.
- The communication status can be output. When engineering, NR output parameter of CONS_* for each data can be used for outputting the alarms. CMER output parameter of SYS_DIAG for the entire data can be used for outputting the alarms.

IMPORTANT

It is recommended to create a mechanism to latch requests in the logic related to inter-SCS safety communication on the consuming side.

SEE ALSO

For more information about precautions when using an SCS of an SCS system program number earlier than R2.03, refer to:

Appendix 4., “Compatibility between Revisions and Cautionary Notes for Upgrading” in Installation for ProSafe-RS R3 (IM 32Q01C50-31E)

A7.2 Combination of communication data and FBs for Inter-SCS safety communication

Use the following combinations of FBs for inter-SCS safety communications according to the type of data to be communicated.

Table A7.2-1 Combination of data types and FBs for Inter-SCS safety communication

Communicated data type	FB for inter-SCS safety communication on the producing side	FB for inter-SCS safety communication on the consuming side	Type of binding variable
BOOL-type	PROD_B	CONS_B	COM_BOOL
Integer-type (DINT)	PROD_I	CONS_I	COM_DINT
Real-number-type (REAL)	PROD_R	CONS_R	COM_REAL

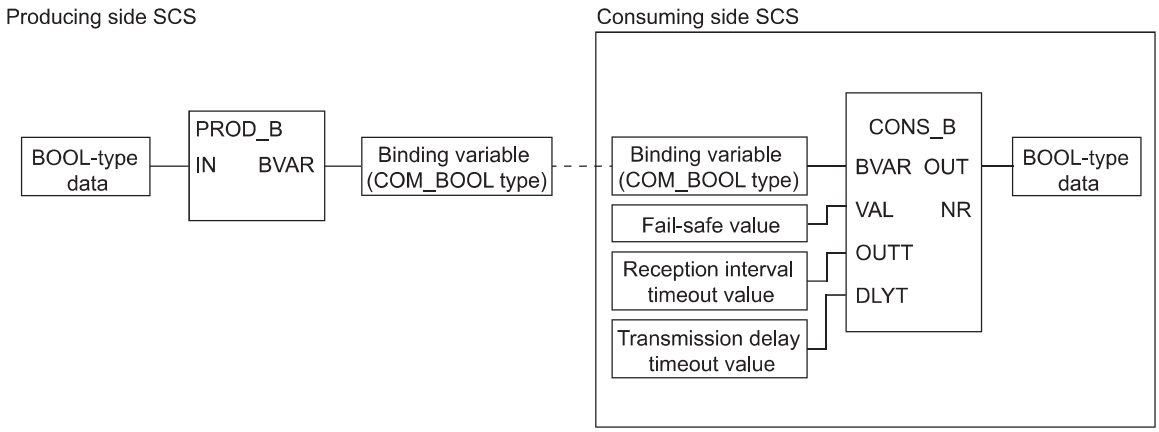


Figure A7.2-1 Combination of communication data, FBs for Inter-SCS safety communication and binding variables

In the case of an FB for inter-SCS safety communication on the consuming side, make sure to specify fail-safe value and timeout values (reception interval timeout value and transmission delay timeout value) in addition to a binding variable.

SEE ALSO For more information about details on the function blocks for inter-SCS safety communication, refer to:

6., “Function blocks for inter-SCS communication (Safety FBs)” in POU Reference Manual (IM 32P03B20-01EN)

Binding variable

There are particular rules for naming binding variables. Moreover, there are rules for binding to multiple SCSs on the consuming side for communication among SCSs.

Use the Binding List View to make settings for the binding variables.

Binding variable naming rules

- Name of binding variable on the producing side
  A character string in the form of Pddssxxx (dd represents the domain number of producing-side SCS, ss represents the station number of producing-side SCS, and xxx represents a 3-digit integer). "P" must be in upper case and "dd," "ss" and "xxx" must be 7 digits including 0, as in 0101001.
- Name of binding variable on the consuming side

The same as the binding variable name on the producing side, except that "P" is replaced with "C" (upper case).

- A "producing variable" is a binding variable starting with "P" and a "consuming variable" is a binding variable starting with "C." The numerical values for the binding variable names must be matched.

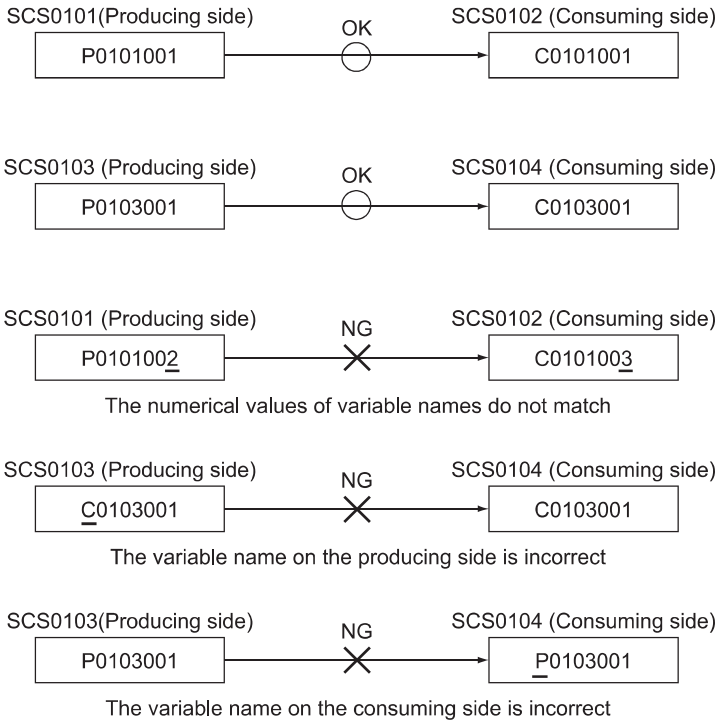


Figure A7.2-2 Binding variable naming rules

Binding rules

- It is possible to bind one binding variable on the producing side with multiple binding variables on the consuming side. In effect, this is equivalent to defining multiple 1 to 1 communications.

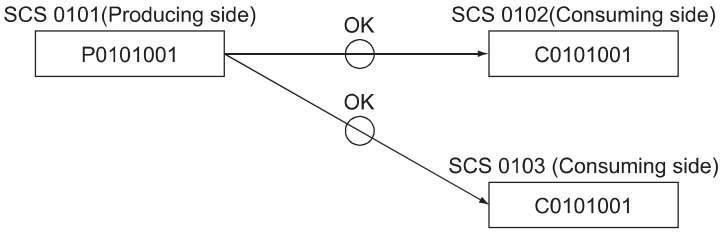


Figure A7.2-3 One binding variable on the producing side and multiple binding variables on the consuming side

- In the case of bi-directional binding, it is necessary to use different variable names. Several 1 to 1 communications are defined in this case as well.

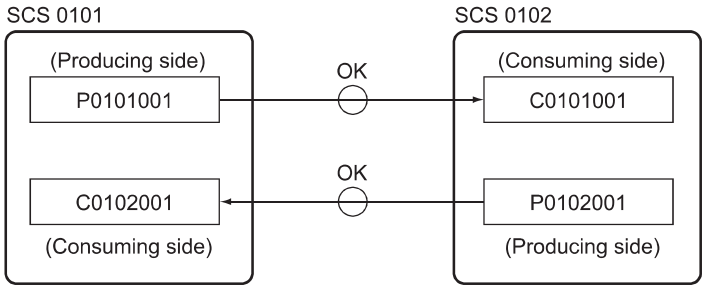


Figure A7.2-4 Use of different binding variables in bi-directional communication

Binding settings

The following items should be set for binding variables in the Binding List View.

Table A7.2-2 Binding setting items

Item	Setting Value	Remarks
Producing variable	Pddssxxx (dd: domain number, ss: station number, xxx: 3-digit integer)	The producing variable and consuming variable must have the same value of "ddssxxx."
Consuming variable	Cddssxxx (dd: domain number, ss: station number, xxx: 3-digit integer)	
Network	ETCP	Automatically set when [Producing variable] and [Consuming variable] are specified.
Communication error behavior	Use last value issued from binding	
Binding parameters	-	
Binding error variables	None	-

Setting binding groups

Create one binding group for each SCS communicating on the producing side and consuming side.

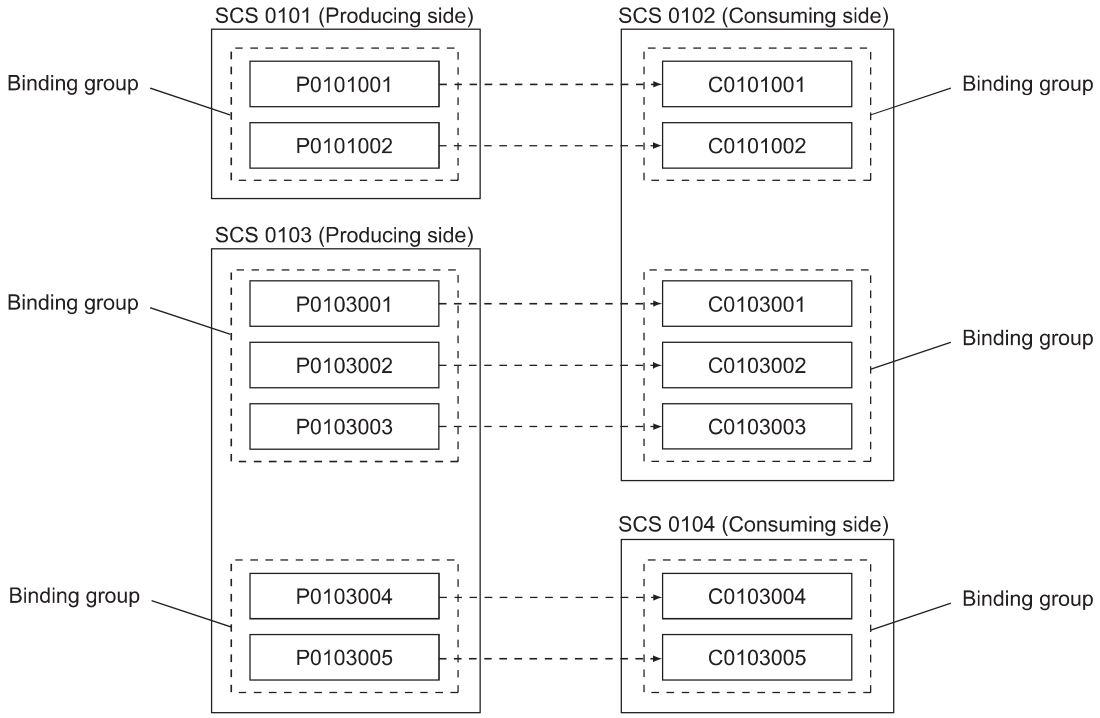


Figure A7.2-5 Binding groups

It is possible to send data from one producing side SCS to multiple consuming side SCSs. In this case, define one group on the producing side SCS for each consuming side SCS.

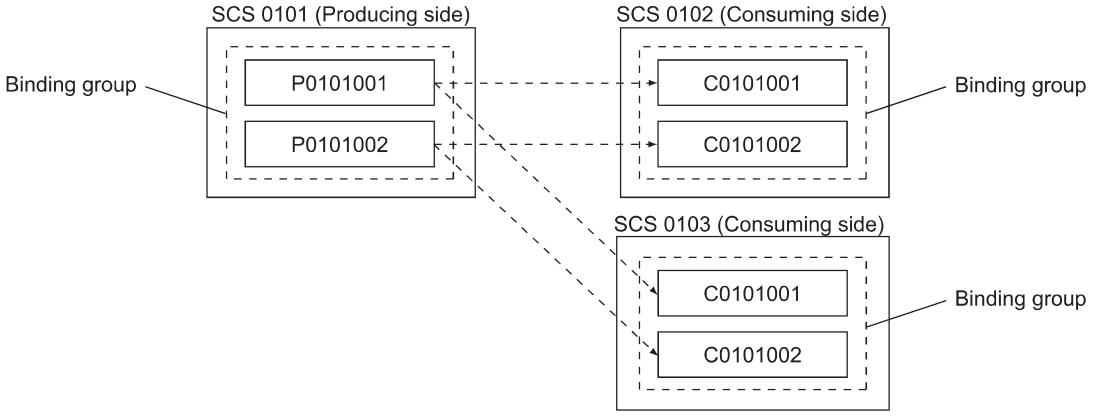


Figure A7.2-6 Relationship between one producing side SCS and multiple consuming side SCSs

When sending data between the producing side SCS and consuming side SCS bi-directionally, prepare binding variables for both the producing and consuming sides. Prepare binding groups as well for both the producing and consuming sides.

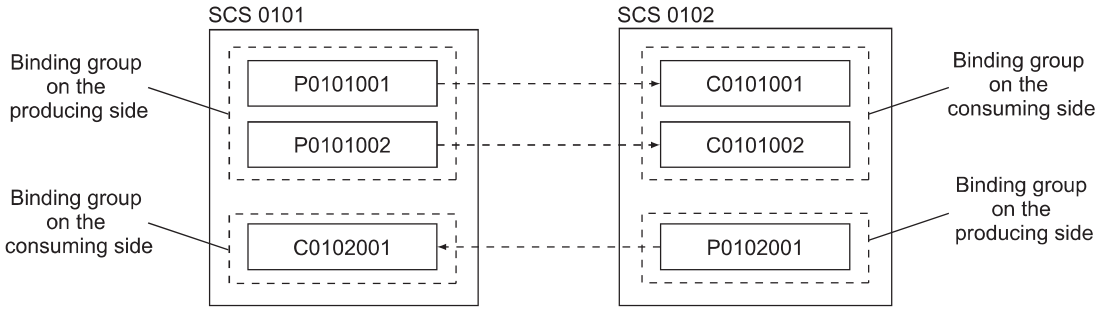


Figure A7.2-7 Bi-directional binding

SEE ALSO For more information about how to configure binding groups, refer to:

"External bindings" in "Variable Bindings" in "Link Architecture View" in "Workbench" in the Workbench User's Guide

A8. SOER functions and how to use them

This section describes functions of the SOER.

The SOER (Sequence of Events Recorder) is for recording and analyzing events detected by SCS. In ProSafe-RS, the SOER is used for the user to analyze the cause of a trip based on the event information detected right before and after the trip.

The user provides definition related to the SOER on SENG. The definition is downloaded to the CPU and the DI module of SCS. The event collected and saved by SCS is uploaded to the SOE viewer on SENG or HIS.

SEE ALSO

For more information about engineering for SOER, refer to:

A8.5, “SOER collection definition” on page A8-12

For more information about host interface, refer to:

C1., “Overview of SOE OPC Interface” on page C1-1

For more information about SOE viewer, refer to:

I4.3, “SOE Viewer” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

A8.1 Overview of SOER

With a SOER, changes in analog inputs/outputs, discrete inputs/outputs and application logics can be collected/saved as event information. Collected event information is displayed in the SOE Viewer. Moreover, a function to synchronize to the standard time is provided in order to maintain the accuracy of the time stamps attached to the events.

ProSafe-RS SOER

Configuration

The SOER function of ProSafe-RS can be used for a minimum system configuration, i.e., one SENG and one SCS.

Event collection

- The SOER function of ProSafe-RS can collect changes of not only discrete inputs (DI) but also discrete outputs (DO) as event information.
- Analog input values can also be collected as event information.
- By creating FBs for SOER, changes of analog output values and application logics can be collected as event information. By doing so, changes of communication data with other SCSs can also be recorded.

Event saving

- You do not need to prepare a dedicated PC for saving events or keep the power supply to an SENG on at all times, because event information is saved in the SCS.
- The maximum number of event information records that can be saved in an SCS is 15000. You can be sure that users are successfully notified of particularly important event information, i.e., records acquired before and after a trip signal was generated, by separating the storage location.

SOE Viewer

- Event information saved in an SCS can be read by the SOE Viewer function in an SENG via the control bus.
- SOE Viewer allows filtering the event information so that only the information the user wants to see is shown.
- SOE Viewer can display diagnostic information messages as well.

Relationship among the SOER functions

The following figure illustrates a structure of functions related to SOER.

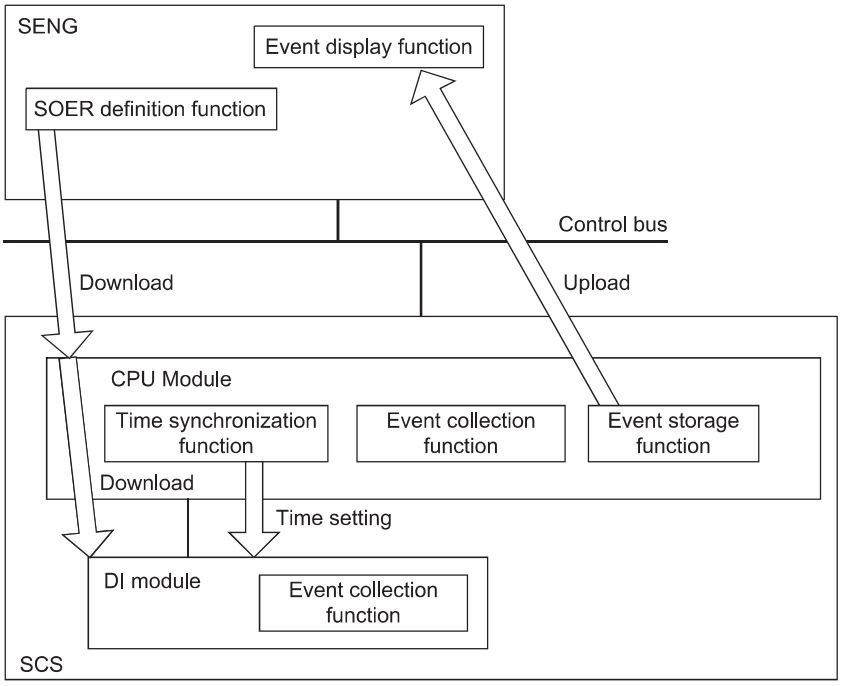


Figure A8.1-1 Relationship between SCS and SENG

The user defines items related to SOER on an SENG. The defined information is downloaded to the CPU of an SCS as well as to discrete input modules in the system. The event information collected/saved in the SCS is uploaded to SOE Viewer in the SENG or HIS.

With SCSs connected to the V net, IRIG-B time synchronization can be selected.

With SCSs connected to the Vnet/IP, time synchronization is implemented based on the Vnet/IP time.

A8.2 Event collection

An SCS allows saving specified discrete inputs, discrete outputs, analog I/O, and variable data of application logics as event information.

Event targets

An SCS can save the following data as event information by user specification.

Events related to discrete inputs (DI) are collected by the input modules; other events are collected by the CPU.

Events of discrete inputs (DI)

- Discrete input modules detect changes in the input signals input to each channel (FALSE to TRUE or TRUE to FALSE) and collect events.
- Users can specify whether or not to collect SOE event information for each channel.
- If discrete input modules are placed in redundant configuration, the active module collects events.
- The comment text attached to the variable corresponding to each DI channel is added to the event. The text can contain a character string of up to 32 single-byte characters, or 16 double-byte characters. The user needs to define the variables corresponding to the contact inputs on the Workbench Dictionary View as the comments so as to identify the whereabouts of the occurred events.

Events of discrete outputs (DO)

- The CPU detects changes in the output value set to a discrete output module and collects events.
- Users can specify whether or not to collect SOE event information for each channel.
- If the output channel is abnormal (data status is BAD), the events will not be gathered.
- Each event is attached with a comment text assigned as a variable to the contact output (a character string of up to 32 single-byte characters or 16 double-byte characters). The user needs to define the variables corresponding to the contact outputs on the Workbench Dictionary View as the comments so as to identify the events.

Events of analog inputs (AI)

- The ANLG_S function block outputs alarms by judging analog input values, and it is able to collect events by making appropriate application. It performs magnitude correlation comparison of set values and analog output values (OUT) and collects events by using a change in OUT as a trigger.
- Events are collected when the SOER input terminal is set to TRUE.
- At event collection, a character string set to the ID input (a character string of up to 32 single-byte characters or 16 double-byte characters) is stored along with the event data.

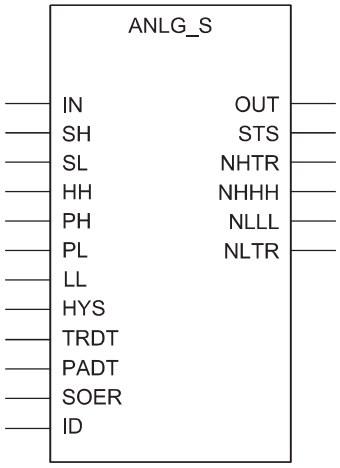


Figure A8.2-1 ANLG_S function block

An ANLG_S function block collects events when the following outputs change their status from FALSE to TRUE, or from TRUE to FALSE:

- NHTR (HI trip flag)
- NHHH (HI pre-alarm flag)
- NLLL (LO pre-alarm flag)
- NLTR (LO trip flag)

When the event occurred can be checked in the ID field of the SOE Viewer.

Table A8.2-1 ANLG_S event IDs

ID in SOE Viewer	Event generation timing
EVT_TRUE	When an alarm recovered (when output status change from FALSE to TRUE).
EVT_FALSE	When an alarm generated (when output status change from TRUE to FALSE).

Events of application logic variables

An SCS collects values of internal variables defined in an application logic as events by connecting them to function blocks dedicated to the SOER function. Variables of the BOOL, integer or real number types can be collected. At event collection, a character string specified in the ID input (a character string of up to 32 single-byte characters) is stored along with the event data.

Use SOE_R to collect analog output events. In IN, enter an output variable. In TRIG, enter a signal that specifies the event collection timing.

The following function blocks are dedicated to the SOER function. Note that events from function blocks are treated as trip signals if TRIP_OFF or TRIP_ON is specified for TRP.

- SOE_B (BOOL type) function block
  SOE_B is a function block used to collect BOOL-type data as events. It collects events if there is a difference between the input value (IN) and the previous value at the execution timing of the function block. The default value of the previous value is 0.

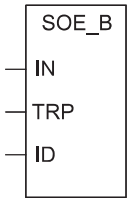


Figure A8.2-2 SOE_B function block

- SOE_I (integer type) function block
  SOE_I is a function block used to collect integer-type data as events. It collects events if the value of TRIG, an input terminal, changes at the execution timing of the function block.



Figure A8.2-3 SOE_I function block

- SOE_R (real number type) function block
  SOE_R is a function block used to collect real number-type data as events. It collects events if the value of TRIG, an input terminal, changes at the execution timing of the function block.

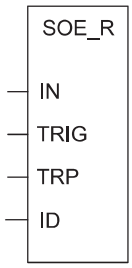


Figure A8.2-4 SOE_R function block

When the event occurred can be checked in the ID field of the SOE Viewer.

Table A8.2-2 Event IDs of dedicated SOE function blocks

FB type	ID in SOE Viewer	Event generation timing
SOE_B	EVT_TRUE	When the status of IN input changed from FALSE to TRUE.
	EVT_FALSE	When the status of IN input changed from TRUE to FALSE.
SOE_I SOE_R	EVT_TRUE	When the status of TRIG input changed from FALSE to TRUE.
	EVT_FALSE	When the status of TRIG input changed from TRUE to FALSE.

Event time

Event information records include a time stamp indicating when the event occurred. The event generation time varies depending on the event type (object).

Table A8.2-3 Event time

Object	Time information of event
Discrete input (DI)	The current time of a discrete input (DI) module at event generation is recorded.
Discrete output (DO)	The current SCS time is stamped to the signal right before outputting it through the output module.
Variable	The current time of the SCS right before the execution timing of a function block is recorded.

Recording of occurrence times of DI module-related events

After an occurrence of channel failure, such as open or short circuit, if you check the SOE Viewer to view a diagnostic information message, you will find that the channel error is displayed after the ON/OFF event of the applicable channel. This means that the time of event occurrence does not match the time of the message. This is because the event and the message are generated by different modules: the DI module generates events and the CPU module generates diagnostic information messages.

When an event occurs, event information is generated based on the DI module time at the occurrence. On the other hand, diagnostic information messages for channel errors, etc., are generated during I/O refresh processing of the CPU module based on the error information received from the DI module, in accordance with the time information acquired at the start of each scan period.

A8.3 Event storage

Event information is stored in the SOER event information storage memory of an SCS. There are two types of files in which event information can be stored: an event log file and trip signal files. An event log file stores the latest event information. In the trip signal file, events before and after each trip signal are saved.

Saving event data

- An SCS saves event data using two types of files: an event log file, which stores event information in the order of data collection, and trip signal files, which store events generated before and after the trip signal specified by the user. There are two trip signal files.
- Event information saved in an SCS is not deleted when read by an SENG and HIS. It is thus possible to reference the information from multiple SOE Viewers.

Flow of event storage

The figure below illustrates the flow according to which event information is stored in an SCS.

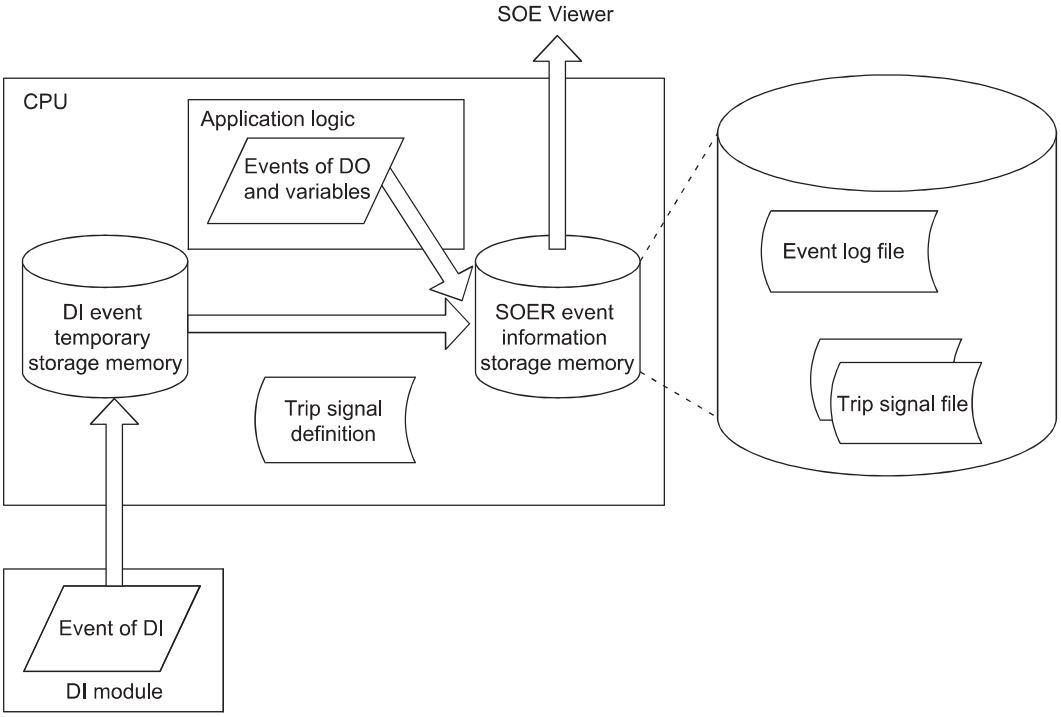


Figure A8.3-1 Flow of data in event information storage

Since event information from a discrete input (DI) module is automatically stored in the DI event temporary storage memory of the CPU, both the DI event in this memory and event information collected in the application logic are stored in the SOER event information storage memory.

Specification of event log files

- An event log file stores the latest event information and one event log file is saved per SCS.
- Up to 15,000 events can be saved in the event log file.
- If the number of events saved exceeds the maximum number, events are deleted and overwritten by new events from the oldest one.

- Whenever an SCS has saved 12,000 events in the event log file, it sends a diagnostic information message to prompt the user to upload to the SENG.

Trip signal

- Trip signals are particularly important events in the plant. Since they are key events when engineers attempt to analyze the causes of tripping, they must be securely stored in the SCS together with the events generated before and after them.
- Either ON edge or OFF edge can be specified as the trip signal. However, both edges can be specified as ignored.
- Users can specify trip signals in input/output definitions or in function blocks for SOE. There is no restriction on the number of trip signals that can be specified, but it is necessary to examine trip signal settings thoroughly in order to record useful event information.

Specification of trip signal files

Trip signal files store events generated before and after a trip signal specified by the user.

- An SCS stores events generated before and after the trip signal in a trip signal file.
- A trip signal file stores 1500 events in total: the last 500 events generated before tripping including the trip signal and the 1000 events generated after tripping.
- Up to two trip signal files can be stored in the SCS. Even when more trip signals occur, no more trip signal file is created. If a trip signal file is created, you need to upload and initialize the trip signal file from SENG immediately.
- Trip signal files are not automatically initialized by the system. The files can be initialized only through operation from SENG.
- If two trips occur in a short period of time, the data in the two trip signal files may overlap.
- If less than 500 events are collected prior to a trip event, the number of the events before the trip event is less than 500.
- If the number of events is less than 1000 after 30 minutes has passed since the trip event occurred, the file will be closed anyway with less events.
- An SCS sends a diagnostic information message when saving of a trip signal file is completed.

SEE ALSO For more information about initializing the trip signal file, refer to:

I4.2.5, “Initialization of tripping information” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Initialization of trip signal files

Trip signal files can be initialized only via initialization operation from the SENG. After you have uploaded events from the SOE Viewer on the SENG, initialize the trip signal files using the Message Cache Tool of the SENG.

- Up to two trip signal files can be initialized with a single operation.
- Initialization operation is also valid while events are being stored.

A8.4 Management of event information when SCS is unsteady

This section explains the management of event information in the following cases of unsteadiness.

- A power failure occurs in the SCS
- During startup of the SCS
- I/O variables are locked

If a power failure occurs in an SCS, event information is saved in NVRAM (nonvolatile RAM). The SCS restores the event information at startup; it is thus possible to check the event information before the SCS was stopped.

Protection of event information at power failure

Generally, event information is stored in the main memory of an SCS. If a power failure occurs in the CPU, the data saved in the main memory is lost. Therefore, the SCS saves the most recent events recorded immediately before the power failure to NVRAM (nonvolatile RAM). Although not all of the events can be protected, it is possible to analyze events that occurred immediately before the power failure by protecting them in this way.

Table A8.4-1 Protection of event information at power failure

File type	Specifications at power failure occurrence (*1)
Event log file	The most recent 1000 events recorded immediately before the power failure are protected.
Trip signal file	Upon completion of collection, the trip signal files are saved to NVRAM (nonvolatile RAM) (up to 1500 events x 2 files). If the files have been fully saved prior to the power failure, all events are safe. If the power failure occurred before the files are fully saved, the events are lost. (*2)

*1: The same operations apply to offline download.
*2: If the most recent events are not saved, refer to the event log file.

SCS startup operation

An SCS restores the event information that was saved before it was stopped when it starts up at restarting or after offline download.

Lock status by the forcing function

If I/O variables are locked by the forcing function, event collection is performed in the following ways when the values of the I/O variables change.

Table A8.4-2 Event collection operation in the locked status

Object	Event collection operation
Discrete input (DI)	Since events are collected by a discrete input module, events are collected based on the actual values input to the module regardless of the lock status. Events are not collected if the value of the discrete input is changed by the forcing function.
Discrete output (DO) (*1) Analog input (AI)	Since events are collected by an application logic, events are collected with the changed value if the values of I/O variables are changed by the forcing function.

*1: In order to collect events, it is necessary that the DO modules are operating normally and the data status of the output channels are GOOD.

SEE ALSO For more information about SOE event collection when switching module control rights, refer to:

A8.6.1, “Redundant configuration in SCS” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

A8.5 SOER collection definition

The SOER collection definition defines which events to collect.

By using SOE Viewer, it is possible to analyze collected events and save them in files. This section explains the types of targets for which events can be collected.

SEE ALSO For more information about SOE viewer details, refer to:

I4.3, “SOE Viewer” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Definition of event collection objects

The setting method of event collection definition varies depending on the object. Events can be collected either from a discrete AIO/DIO module or an application logic.

Objects of event collection

The following types of events can be collected for SCSs.

- Signal changes of discrete input modules
  It is possible to collect events from discrete input modules according to the changes of data input from individual channels. Specify whether or not to collect events for each channel.
- Signal changes of discrete output data
  It is possible to collect events according to the changes of data output to individual discrete output channels. Specify whether or not to collect events for each channel.
- Alarms on Analog input data and Recovery
  It is possible to collect events by comparing the output values with the settings of alarm level set to the analog input block.
- Variation of Analog output data
  It is possible to collect events based on the variation of output variable. Take the settings of the output variable into SOE_R, and specify the conditions of event generation.
- Changes of internal variable of an application logic
  It is possible to collect events according to the changes of an internal variable of an application logic. Specify the object internal variable and conditions of event generation.

Event collection definition for Discrete Input/Output modules

For each channel of a discrete input/output module, you can specify whether to perform SOER collection by setting an I/O parameter. Events are collected when the channel signal of the discrete input/output module changes.

SEE ALSO For more information about I/O parameter setting items for modules, refer to:

Appendix 1.2, “Settings for modules” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about I/O parameter setting items for channels, refer to:

Appendix 1.3, “Settings for channel items” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Event collection definition for application logic

Events generated at input from an analog input and signal change in an application logic can be collected. To collect events, add a function block that can collect events in a program or a function block. There are the following four types of function blocks that can collect events according to the target data type.

Table A8.5-1 Function Blocks that can collect data

Data type	Function block	Description
BOOL	SOE_B	Records BOOL-type data values as events when a specified trigger value changes
DINT	SOE_I	Records DINT-type data values as events when a specified trigger value changes
REAL	SOE_R	Records REAL-type data values as events when a specified trigger value changes
IO_REAL	ANLG_S	Used for SOER on analog input. If an alarm is raised as the result of a data value exceeding the limit and the status continues for a specified period of time, the alarm status is recorded.
	ANLGI	Used for SOER on analog input. Records data values as events when the data value gets outside the specified range.
	HSDTR	Records IO_REAL-type data values as events when an alarm occurs and upon recovery.
	GASDTR	

TIP

It is necessary to append a character string to the ID terminal of a function block in order to identify events. The character string must be up to 32 characters.

SEE ALSO

For more information about details on the function blocks of SOE, refer to:

8., “Interference-free function blocks” in POU Reference Manual (IM 32P03B20-01EN)

For more information about details on the analog input function blocks with data status, refer to:

5.7, “ANLG_S (analog input function block with data status)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about details on the analog input function blocks, refer to:

5.8, “ANLGI (analog input)” in POU Reference Manual (IM 32P03B20-01EN)

Event collection of application logic

The following figure shows an example of an application with FBs for the SOE event collection.

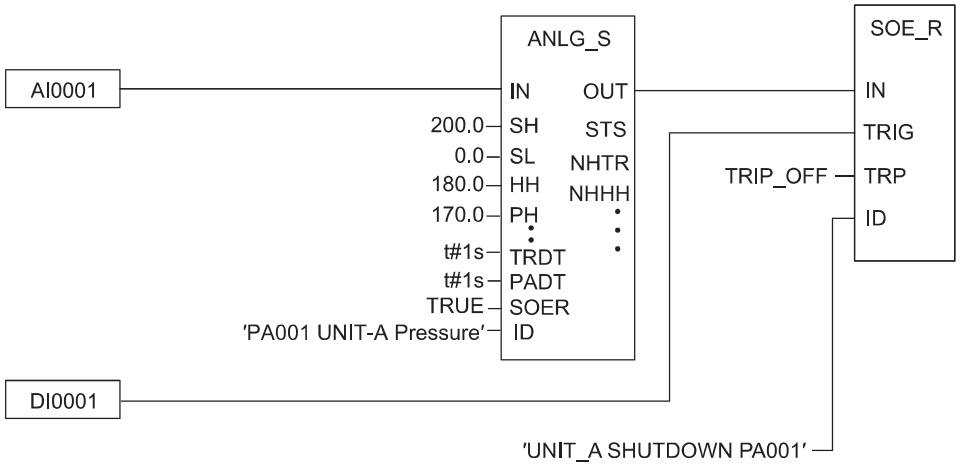


Figure A8.5-1 Example of application with FBs for SOE event collection

In the figure, the "SOE_R" FB collects the output value (OUT) of the "ANLG_S" FB together with the character string "UNIT_A SHUTDOWN PA001" when DI0001 changes value. The SOER of the "ANLG_S" is set to TRUE, so that the "ANLG_S" FB collects the alarm status with the character string "PA001 UNIT-A Pressure" when alarm of the FB occurs.

Precautions for creating an application

- Comment(s) is added to the DI events and DO events. Comments are bound with I/O variables wired to its channel. (Max. 32 characters) The user should set character strings that can identify events for the I/O variables.
- For the function block (ANLG_S/ANLGI/SOE_*) used for acquiring events on variables in application logic, specify the number of characters (max. 32 characters) for comments added to events. Comments are used to identify events.
- For acquiring analog output value (AO) as events, specify the 'value set to output variable' in SOE_R also. Specify the timing of acquiring events as a trigger signal in application.

A9. HART communication

Analog I/O module with HART communication (hereinafter called HART modules) on ProSafe-RS allows Plant Resource Manager (PRM) to control the HART communication devices connected to input and output on SCS. Also, HART modules allow PRM to conduct Partial Stroke Test (hereinafter called PST) on HART-supported valve positioner equipped with the PST function.

The HART modules on ProSafe-RS are interference-free and have no impact on the safety functions on SCS.

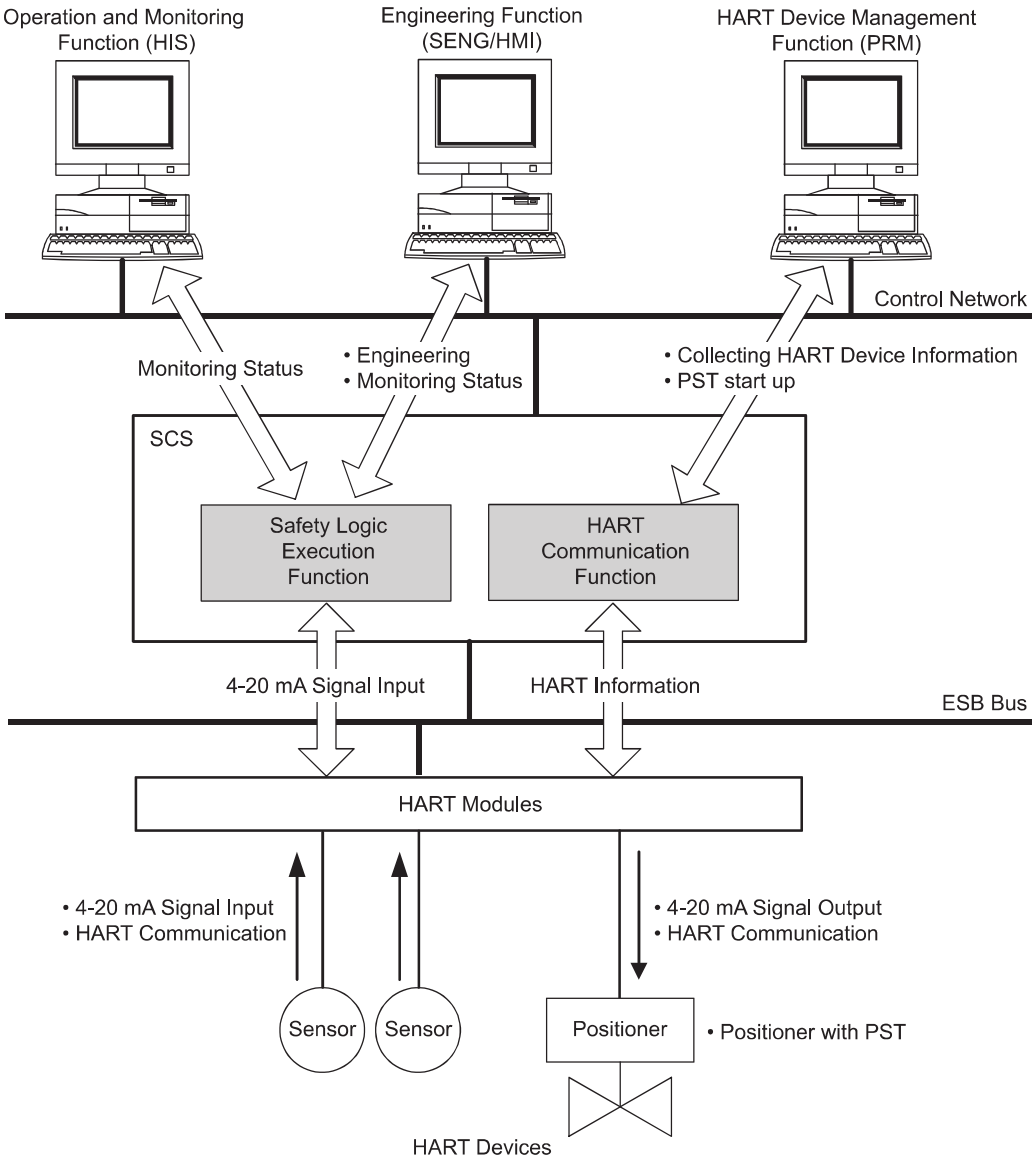


Figure A9-1 HART Communication function

A9.1 Description

This section introduces input and output modules supporting HART communication functions and provides precautions to perform HART communications.

AI/AO modules for HART Communication function

The following table shows the AI/AO modules for HART communication available to ProSafe-RS.

Table A9.1-1 AI/AO modules for HART Communication function

Module	Model	Description	Remark
Analog input module (Current input)	SAI143-H/ L1AI143-H	16 channel; 4 to 20 mA, Isolated	HART communication function
Analog output module (Current output)	SAI533-H/ L1AI533-H	8 channel; 4 to 20 mA, Isolated	HART communication function
Analog digital I/O module	S2MMM843	AI/AO/DI/DO 16 channel, module isolation	

One HART device is connectable for each channel of these modules. Each channel is equipped with a power supply function to the HART device.

As analog input modules and analog output modules have only one HART modem for each module, only one HART device can communicate at a time through a single module.

For the analog digital I/O module, one HART device can be connected to each channel. As the analog digital I/O module has one HART modem for each channel, multiple HART devices can communicate at a time through a single module. For one analog digital I/O module, a maximum of 16 HART devices for AI or 8 for AO can be connected.

SEE ALSO For more information about HART communication function specific to N-IO, refer to:

A9.3, “HART communication function specific to N-IO” on page A9-6

ProSafe-RS software setting items

Among the valve positioners equipped with the HART communication function, there are types capable of HART communication even during the output of a shutdown (valve fully closed) (*1). If you set the Shutdown output value for the analog output module on ProSafe-RS in accordance with the specifications of the valve positioner, HART communications continue even after the valve is shutdown. To do so, set the following parameters for the analog output module on ProSafe-RS based on the specifications of the valve positioner.

- Shutdown output value
- Tight-shut output value
- Output value at fault

*1: For example, specifications of some HART-supported valve positioners are defined as: 14 mA or more: Full open; 5.6 mA or less: Full close; 3.8 mA or more: HART communications allowed. In this case, set 'Shutdown output value', 'Tight-shut output value', and 'Output Value at Fault' to 3.8 mA (within the range where HART communications are allowed and safety shutdown is guaranteed), and HART communications continue even after the valve is full-closed.

Precautions for using HART devices

There are certain precautions to be taken regarding any HART devices that you are using and to be observed during their use.

Precautions regarding HART devices

If HART devices (such as sensors, multiplexers, positioners, and handy terminals) are used in Safety loop, the devices must meet the requirements for the Safety loop (such as SIL certified: Self-diagnosable for HART circuit failure and capable of notifying it to external devices).

A failure in HART devices may affect field signals and cause errors such as false trip or no demand responding. If HART devices are incapable of notifying the errors, ProSafe-RS has no way to recognize them.

You must use devices not-constantly connected to the system such as a handy terminal only when the plant is shutdown or when maintenance work is being performed while no hazardous situation is created even if field signals are affected. If you have to use a handy terminal while the plant is in operation, make sure that the handy terminal works correctly and take the above mentioned risks into account.

Dealing with HART communication errors

If an error occurs in communication via a HART module between a HART communication device and PRM and there is nothing wrong in the communication route between the HART communication device and the HART module, the HART circuit inside the HART module may have failed. When an error occurs in the HART circuit, the control rights for the module are not switched, even if the HART module has a redundant configuration. In such cases, use the IOM Control Right Switching Tool to switch the control rights for the module and check whether communication is restored. If communication returns to normal as a result of switching the control rights, it is possible that the problem was caused by a HART circuit failure in the module on standby. In this case, ensure that the module is replaced.

SEE ALSO For more information about IOM Control Right Switching Tool, refer to:

I4.7, “IOM Control Right Switching Tool” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

A9.2 PST engineering

From a PC integrated with PRM in which PST supported Plugin Software (hereinafter called Plugin for PST) is installed, you can execute PST on the valve positioner that supports the Plugin. Operations for and configuration of the PST are performed from the Plugin for PST. Plugin for PST communicates with the valve positioner via HART communications protocol. The valve positioner executes PST based on the information from the Plugin for PST and stores the test results inside. You can refer to the stored result by Plugin for PST, so you can determine the status of the valve (normal/abnormal) based on the result.

To build such a PST environment, consideration must be given to the following:

- PRM Configuration
- PST Engineering

PRM Configuration

PRM configuration includes:

- Register devices connected to ProSafe-RS in PRM.
- Register the 'Plugin for PST' software in PRM.
- Set the handling manner of errors raised by ProSafe-RS (such as system or device alarms) (*1)
- Customize to distinguish SIS devices from DCS devices.

All engineering work for PRM is done on PRM. For details, see User's Manuals for PRM.

*1: Error handling here means setting parameters for PRM's Fault Notification functions (such as Device Patrol and Maintenance Alarms). PRM is an interference-free product including its error handling functions.

PST engineering

PST engineering includes the following parameter settings:

- Interval of PSTs
- Valve close level in PST (Percentage)
- Criteria for raising errors
- How to activate PST (Manual or Auto)
- If PST is automatically activated, how to notify errors (*1)

*1: If PST is automatically activated, available error notification methods are: sending alarms to HIS via PRM or using the output contacts equipped with the valve positioner. For the specifications of the output contacts on the valve positioner, see its specifications.

All the PST engineering work is done from Plugin for PST or Valve positioner. For details of the engineering work, see the User's Manuals for the Valve positioner.

Some Plugin for PST are capable of working in conjunction with PRM client. For details, see the User's Manuals for Plugin for PST.

Safety Integrity Level (SIL)-certified and PST-supported valve positioner is provided with a manual which describes precautions for conducting PSTs. Be sure to read the manual and follow the given procedures for conducting PSTs.

Precautions for building PST environment

The following must be observed when PST environment is built:

- Specifications of the valve positioner define that the shutdown output from ProSafe-RS has the highest priority (even in a PST).

- When an online change download is implemented with the configuration of the analog output module, the entirety of the analog digital I/O module, or the AO channel of the analog digital I/O module, ProSafe-RS is temporarily disconnected from HART communications. For this reason, do not perform online change download for said modules while using the Plugin for PST software (in other words, while conducting HART communication). If an online change download is performed and a HART communication error occurs, retry the operation of the Plugin for PST after recovery of the module.
- According to the manual for the valve positioner, setup the ProSafe-RS.

A9.3 HART communication function specific to N-IO

This section describes the HART communication function that is specific to N-IO.

I/O module for the HART communication function of N-IO

The following table shows I/O modules that are available in ProSafe-RS for N-IO for the HART communication function.

Table A9.3-1 I/O module for the HART communication function of N-IO

Module	Model	Basic functions	Remarks
Analog digital I/O module (16 channel, module isolation)	S2MMM843	16 channel, module isolation AI/AO: 4 to 20 mA DI/DO: 24 VDC	• Only AI/AO supports HART communication function • You can switch among AI/AO/DI/DO in each channel

The Analog digital I/O module can use a different signal category (AI/AO/DI/DO) for each channel. For the signal category is AI or AO, one HART device can be connected to one channel with a signal type of a current input (HART communication) or current output (HART communication). Each analog channel is equipped with a power supply function to the transmitter.

As the analog digital I/O module has one HART modem for each channel, multiple HART devices can communicate at a time through a single module. For one analog digital I/O module, a maximum of 16 HART devices for AI or 8 for AO can be connected.

A9.3.1 Status change notification function of HART devices

You can use the status change notification function of HART devices when using N-IO in SCSP3 of CENTUM integration environment. The functions are interference-free and have no impact on the safety functions on the SCS.

These functions are divided into two features: a function for detecting the change of status of a HART device (device status change detection function) and a function for notifying PRM of the detected information through HIS (device status change notification function).

The following figure shows the concept of the notification of the status change in HART devices.

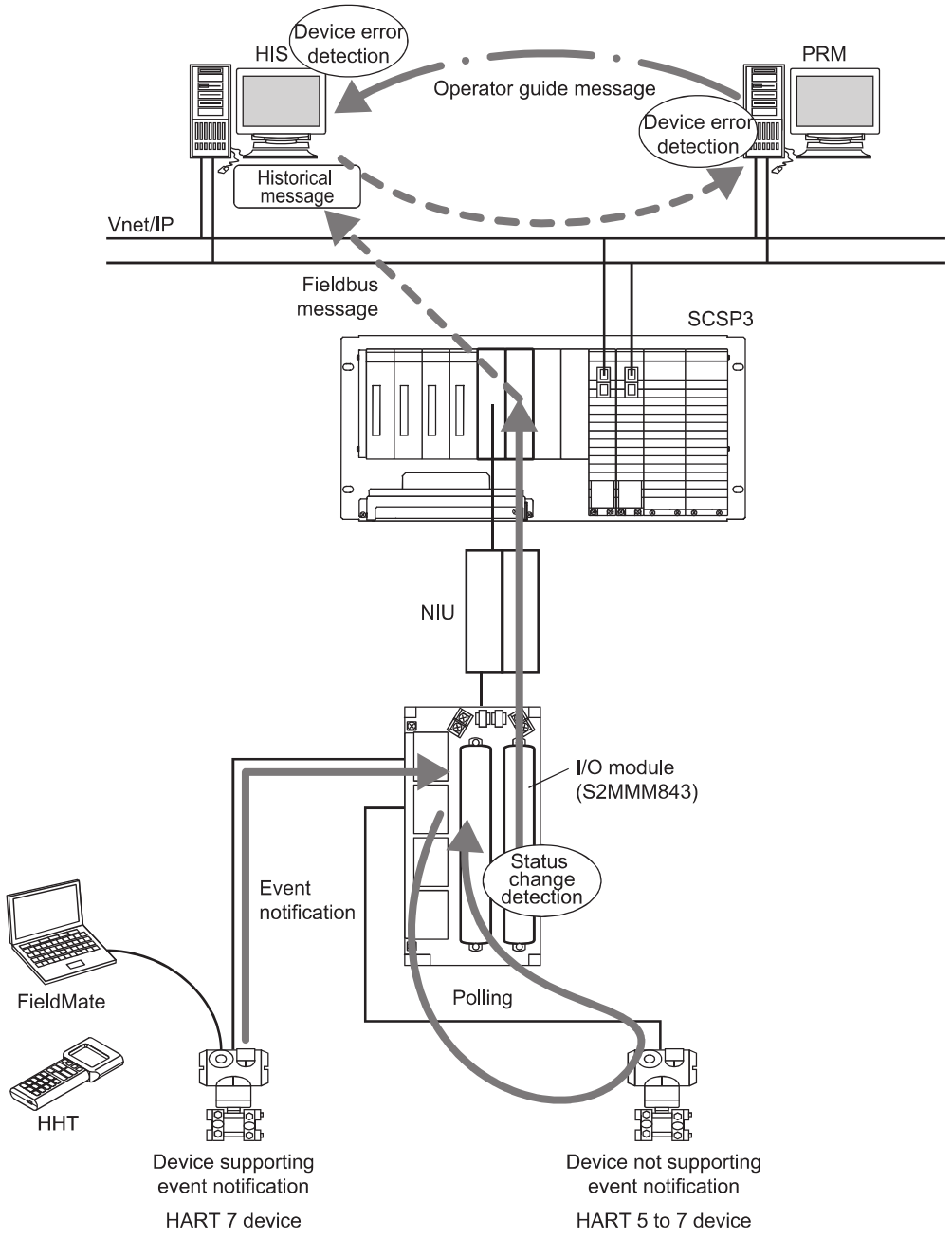


Figure A9.3.1-1 The concept of the notification of the status change in HART devices.

Device status change detection function

Analog digital I/O modules detect the status change in HART devices. The function is targeted for the signal category is AI or AO, and the channel with a signal type of current input (HART communication) or current output (HART communication).

The target models of the function are wired HART 5 to 7 devices.

There are two types of supported methods for transferring the status change:

- Event method: Receives events from HART 7 device.
- Polling method: Reads detailed information from HART devices at regular intervals and detects status change.

TIP

The I/O module identifies the target device and dynamically selects the transfer method.

I/O modules send the status change information of HART devices to the SCS.

SEE ALSO

For more information about precautions for the transfer method of the status change in HART devices, refer to:

A9.3.2, “Precautions for the transfer method of the status change in HART devices” on page A9-9

Device status change notification function

The SCS notifies the status change of HART devices, which is sent from I/O modules, to HIS as a fieldbus message.

HIS manages the fieldbus message as historical data and equalizes it with PRM.

PRM analyzes the fieldbus message that is received from HIS and updates the HART device status.

To notify the operators of the detected HART device failures or errors, configure operator guide messages in PRM.

A9.3.2 Precautions for the transfer method of the status change in HART devices

The following are transfer methods for the status change of HART devices:

- Event method
- Polling method

This section describes the precaution for each method.

Event method

The event method involves receiving events from HART devices.

The target of the event method is HART 7 devices where event notification is enabled.

I/O modules send a notification of the events received from HART devices to the SCS. The fieldbus message is sent from the SCS.

After a status change is detected in HART devices, it takes 4 to 5 seconds for the fieldbus message to be sent.

IMPORTANT

In the event method, a fieldbus message with the same content may be sent again if the following events occur after the first fieldbus message is sent.

- CPU control right switching
- IOM control right switching
- Recovery from HART communication error
- Recovery from power outage in N-IO nodes

Due to the resending function of HART devices, the detection of the status change in the device is not skipped.

Polling method

In the polling method, I/O modules read detailed information from HART devices at regular intervals and detect the status change.

The target of the polling method is HART 5 to 7 devices where the event method is not used.

I/O modules read the device status from HART devices once every 30 seconds. If the value changes from the previous reading, the I/O module sends a notification to the SCS. The fieldbus message is sent from the SCS.

After a status change is detected in HART devices, it takes 4 to 35 seconds for the fieldbus message to be sent.

IMPORTANT

In the polling method, the same fieldbus message will not be sent.

However, if the control right of the I/O module is switched before sending the status change, which is detected in the HART device to the controller, the notification for status change of the device may be skipped.

If the status change of the HART device is set back while the I/O module is reading the HART device information, the change is not detected.

B. CENTUM integration

The structure of a ProSafe-RS connected with CENTUM projects is called CENTUM Integration Configuration. This section describes the overview and the engineering procedure of CENTUM Integration Configuration.

B1. Overview of CENTUM integration

The CENTUM Integration Function of ProSafe-RS provides a communication interface for accessing SCS of ProSafe-RS from HIS and FCS of CENTUM VP or CS 3000 system (hereinafter referred to as "CENTUM") through control bus. By this function, you can operate and monitor SCS from HIS using the same interfaces (windows) for operating and monitoring FCS. You can also access SCS data from FCS using the same interface (tag names) used by an FCS to access other FCS.

CENTUM VP integrated system configuration

The structure that integrates ProSafe-RS with CENTUM VP is called CENTUM integration configuration. The role of each station in the CENTUM integration structure is as follows:

- SCS: Shuts down the plant safely if an error occurs in the plant.
- FCS: Performs process control.
- HIS: Provides user interfaces for accessing FCS and SCS data.

The following figure shows an example of the CENTUM integration structure. In the CENTUM integration structure, both SCS and FCS can be operated and monitored from HIS. It is also possible to access SCS data from FCS.

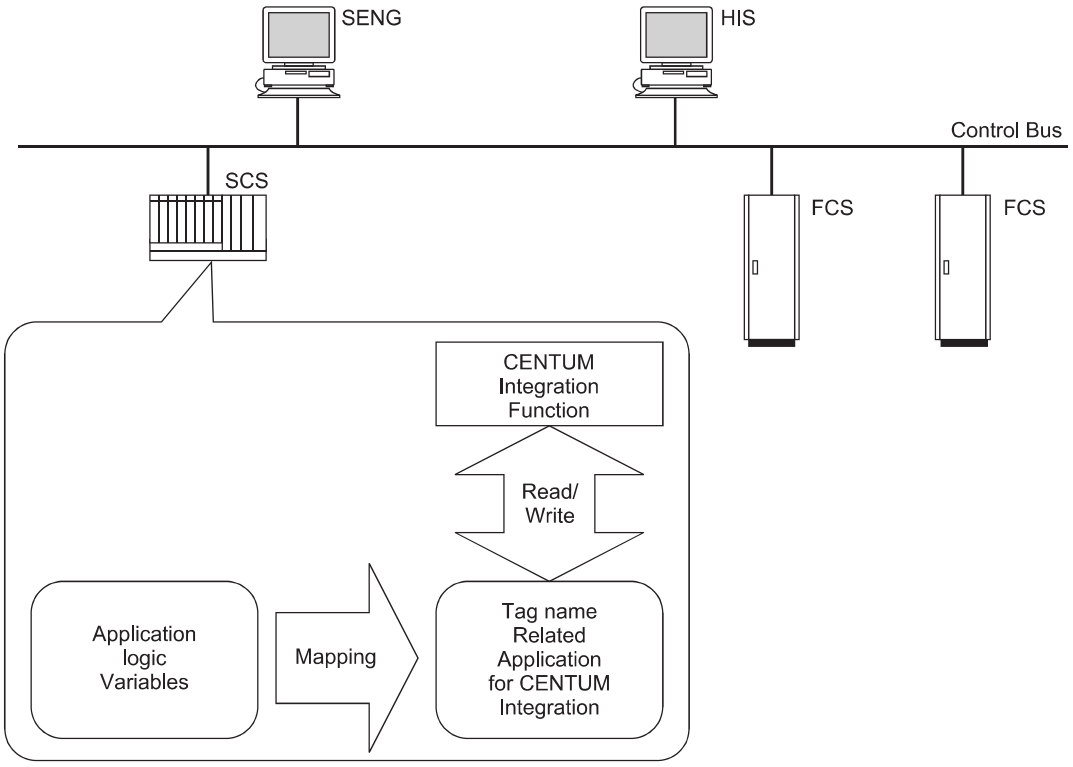


Figure B1-1 CENTUM integration function

Application logics and CENTUM elements

In the connection definitions for CENTUM integration, application logics and CENTUM elements are associated in the manner shown in the table below. Since tag names are defined for CENTUM elements, the user can monitor their statuses using the tag names.

Table B1-1 Correspondence between application logics and elements

Application logic		CENTUM element
Variable	Internal variable (BOOL)	%WB
	Internal variable (DINT)	%WB
	Internal variable (REAL)	%WB
	I/O variable (IO_BOOL)	%Z and %Y
	I/O variable (IO_REAL)	%WB
Function block	• Analog input FB with data status (ANLG_S), Analog input FB (ANLGI), Analog input FB for smoke and heat detectors (HSDTR), Analog input FB for gas and flame detectors (GASDTR) • Velocity limit alarm FB (VEL) • Override FBs (OVR_B, OVR_I, OVR_R, OVR_IB, OVR_IR) • Grouping override FB (GOV_B, GOV_IB) • Password FB (PASSWD) • Manual operation FB (MOB_11, MOB_21, MOB_RS, MOA)	%BL
	External communication FB (ECW_B, ECW_I and ECW_R)	%WB
	Subsystem communication I/O FB (SCI_B, SCI_I, SCI_R, SCO_B, SCO_I, SCO_R)	%WB
	Safety subsystem communication I/O FB (PSI_I, PSI_R, PNI_I, PNI_R)	%XB
	Annunciator FB (ANN, ANN_FUP)	%AN

Operation/monitoring using tag names

Operators can reference and set values of instances of application logics (function blocks defined as entities) using tag names from an HIS. It is also possible to reference and set data from data items of tag name.

Process alarm message transmission

CENTUM elements collect errors on the field side detected in an application logic and send process alarm messages to an HIS. Process alarm messages include messages sent by mapping blocks (%BL) and messages sent by annunciator elements (%AN).

A process alarm message is sent at the execution timing of a mapping block or annunciator element. The occurrence/recovery time stamp attached to the messages is the time at which the application logic is executed. If several messages are generated in one second from the same block and element, only the last two event messages are sent.

Software inputs/outputs

Two of the software inputs/outputs supported by FCSs, common switch and annunciator, are available for use in SCSs.

Table B1-2 Software inputs and outputs available in SCSs

Name	Support in SCS (*1)	Element
Common switches	Yes	%SW
Global switch	No	%GS
Annunciator	Yes	%AN
Printout message (with printing, Historical)	No	%PR
Printout message (without printing, Historical)	No	%PR

Continues on the next page

Table B1-2 Software inputs and outputs available in SCSs (Table continued)

Name	Support in SCS (*1)	Element
Operation guide message	No	%OG
Multimedia start message	No	%VM
Sequence message request	No	%RQ
Supervisory computer event message	No	%CP
Supervisory computer message output for PICOT	No	%M3
Signal event message	No	%EV
SFC/SEBOL return event message output	No	%RE

*1: Yes: Supported
No: Not supported

TIP

The sent and received data through SCS Link Transmission cannot be accessed from HIS as accessing a %GS element. For accessing from HIS, an internal variable should be placed in application logics. The examples below show how to connect the internal variable with SCS Link Transmission FB, and then define the variable with a tag name on the Tag Name builder.

- For accessing the value of a sent data, the data connected to the sending FB should be branched so as to connect to a variable.
- For accessing the value of a received data, the output parameter of the receiving FB for the data value should be connected with a variable.
- For accessing the data status of a received data, the output parameter of the receiving FB for the data status should be connected with a variable.

Common switches (Common switches for system)

Since common switches for the system reflect the internal status of an SCS, they can be used in the Graphic view of an HIS.

The following table shows a list of common switches for the system. Elements without a switch number cannot be used in the SCS. Tag names cannot be defined for SCS common switches. Also, you cannot set a value to the SCS common switches. You cannot use the value of SCS common switches in an application logic, either.

Table B1-3 Common switches for system

Switch number	Name	Description
%SW0001	Initial cold start	1: Fixed (to initial cold start)
%SW0002	Continuous start	0: Fixed (to initial cold start)
%SW0004	(Reserved)	Same as %SW0001
%SW0017	Right side CPU status	0: Normal 1: Abnormal
%SW0018	Left side CPU status	0: Normal 1: Abnormal
%SW0019	Fan status of the safety control unit	0: All normal 1: At least one is abnormal
%SW0020	CPU temperature status	0: All normal 1: At least one is abnormal
%SW0021	Power module status of the safety control unit	0: All normal 1: Either the left or right module is abnormal
%SW0022	Power supply module status of nodes (*1) (*2)	0: All normal 1: At least one is abnormal

Continues on the next page

Table B1-3 Common switches for system (Table continued)

Switch number	Name	Description
%SW0027	Right side CPU control status	1: Control 0: Other
%SW0028	Left side CPU control status	1: Control 0: Other
%SW0033 to 0042	Status of nodes 1 to 16 (*3)	0: Normal 1: Abnormal
%SW0065 to 0072	CPU idle time per minute (seconds)	0 to 60 seconds (8-bit integer)
%SW0073 to 0080	Communication load per second (%)	0 to 100% (8-bit integer)
%SW0097 to 0104	I/O module status of the safety control unit	0: Normal or no definition 1: Abnormal
%SW0105 to 0176	Status of I/O module (each of the 8 slots) of the 2nd to the 10th nodes (safety node units)	0: Normal or no definition 1: Abnormal
%SW0177 to 0208 (*4)	Status of input/output module (each of the 8 slots) of the 11th to the 14th nodes (I/O nodes)	0: Normal or no definition 1: Abnormal
%SW0225 to 0256	N-IO Node 1 to 32 status (*3)	0: Normal 1: Abnormal
%SW0289 to 0320	N-IO Node 1 to 32 diagnostic status (*3) (*5)	0: Normal 1: Abnormal
%SW0353	I/O module status of N-IO node 1, I/O unit 1, and slot 1	0: Normal or no definition 1: Abnormal
%SW0354	I/O module status of N-IO node 1, I/O unit 1, and slot 2	0: Normal or no definition 1: Abnormal
%SW0355 to 0364	I/O module status of N-IO node 1 and I/O units 2 to 6	0: Normal or no definition 1: Abnormal
%SW0365 to 0736	I/O module of N-IO nodes 2 to 32	0: Normal or no definition 1: Abnormal

*1: The power module status of the unit for optical ESB bus repeater module is excluded.
*2: When only SEC40x or L1EC40x is defined for FIO Node 1, the power status of FIO Node 1 is not reflected. Use %SW0021 together.
*3: 0 is set for undefined nodes.
*4: Applicable to SCSP2, SCSP3, and SCSL2.
*5: If temperature monitoring and input monitoring from external devices are all normal, the status is 0. The status is 1 if there is any error.

● Update interval

The SCS internal status is reflected in common switches for the system at the intervals of the scan period of the external communication function.

■ Overview of mapping blocks/mapping elements

In an CENTUM integration structure, mapping blocks/elements are created when users define tag names in Tag Builder in an SENG.

Mapping blocks/elements map function blocks and variables of an application logic and provide simple ways to interface with them via the tag names.

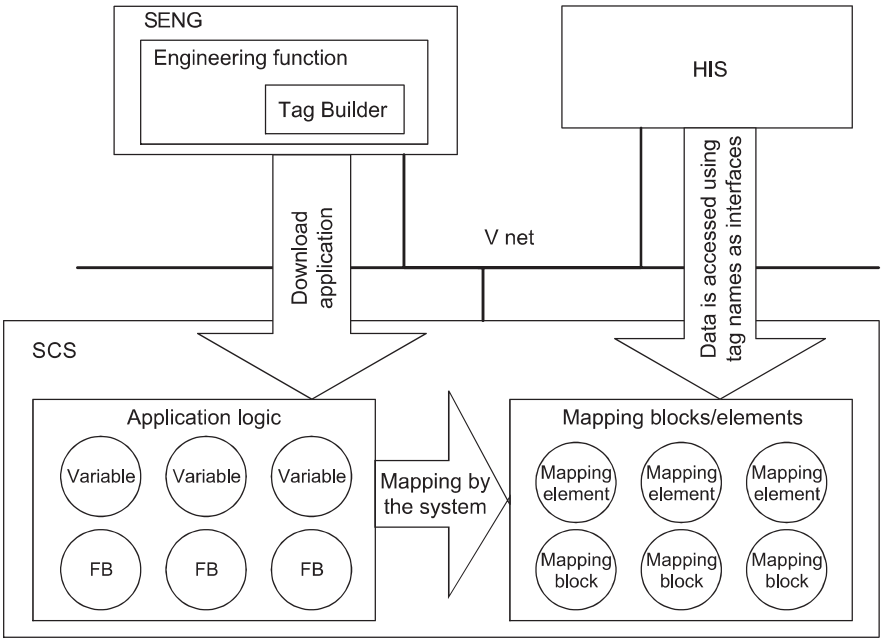


Figure B1-2 Mapping blocks/elements

Data reference via tag name interface

- By defining tag names in Tag Builder, it is possible to associate mapping elements with internal variables of BOOL, integer or real number type of an application logic and reference the data using the tag names.
- By defining tag names in Tag Builder, it is possible to associate mapping elements with I/O variables of an application logic and reference the data using the tag names.
- By defining tag names in Tag Builder, it is possible to associate mapping blocks/elements with function blocks of an application logic and reference the data using the tag names. For example, an ANLG_S function block can be associated with a mapping block, while an ANN function block can be associated with a mapping element. Specific function blocks are associated with mapping blocks.

SEE ALSO For more information about variables, elements, and FBs for which tag names can be defined, refer to:

"■ List of mapping blocks/mapping elements" on page B3-2

Data setting and alarm management by tag name interfaces

- Operations on mapping blocks/elements (without influencing application logics)
  It is possible to acknowledge process alarms and set operation marks (data item OPMK). If these operations are performed from an HIS, the data of the mapping blocks/elements changes, but this does not cause any changes to variables and function blocks of application logics.
- Operations on variables and function blocks of an application logic
  Operations on mapping blocks/elements are reflected in the corresponding application logic. The override operations, setting BOOL-type data with password, setting data with Manual Operation FB, setting data via tag name and so on operations can be performed.

Input/output terminals

No input/output terminals are used for mapping blocks/elements of an SCS. Mapping blocks/elements are used to exchange data with variables and function blocks of the corresponding application block, and not for connection between with mapping blocks/elements.

B2. Integration with CENTUM

The main purposes of integrating with CENTUM are as follows.

- To monitor the controlling status of SCS with an HIS
- To notify errors on the field side to operators via process alarm messages
- To set data to SCS
- To integrate system alarms

This chapter explains the SCS functions for integrating with CENTUM.

Functions in CENTUM integration structure

This section describes the functions of operating SCS from HIS or FCS in the CENTUM integration.

Monitoring and operation from HIS

- SCS data can be monitored and operated with tag names through the same interface as the one for FCS, which allows data reference with a faceplate and display of SCS data on a Graphic View.
- SCS data to be collected can be defined as a historical trend by HIS by specifying its tag name and data type, but not as a high-speed trend (1 sec).
- The occurrence/recovery of process alarm and annunciator messages that are detected by SCS can be monitored on the Process Alarm View of HIS.
- Diagnostic information messages issued at SCS can be monitored on the System Alarm View of HIS.
- SCS status can be shown on the SCS Status Display View of HIS.
- The values of the variables of the SCS application logic can be overridden by HIS. This is the function of fixing a variable of SCS application logic at the predefined value temporarily.
- Boolean variables of SCS application logic can be set to 1 or 0 by HIS with password authentication.

IMPORTANT

Incorrect usage of the dedicated alarm management software in HIS might result in the overlook or filtering out of important alarms critical to safety. Therefore when configuring alarms, it is important to ensure that critical alarms are always communicated to operators.

SEE ALSO

For more information about the software for managing the alarms, refer to:

B8.1.6, “Software for Managing the Alarms” on page B8-26

For more information about override, refer to:

7.1, “Override function blocks” in POU Reference Manual (IM 32P03B20-01EN)

For more information about data setting with password authentication, refer to:

11.11, “SYS_PSWD (password function blocks management)” in POU Reference Manual (IM 32P03B20-01EN)

Communication between FCS and SCS

- The variables of SCS application logic can be set from FCS by using Sequential Function Chart (SFC) blocks. The External Communication Function Block is used for SCS. In this case, the SCS data must be confirmed by reading the data back by FCS. This function does not affect the safety function of SCS.
- SCS data can be read by FCS using tag names and the FCS function of connecting between stations.
- From the Switch Instrument Block or the Motor Control Block, data can be set to the External Communication FB on the SCS using Inter-station Data Link Block (ADL). However, there are some precautions as following: Do not change frequently (every second) the MV in the Switch Instrument Block or Motor Control Block connected to SCS tags using ADL. If you use the three-position type Switch Instrument Block or the Motor Control Block on FCS, note the following:
  - Use enhanced Switch Instrument Block or Motor Control Block. Non-enhanced function blocks cannot connect with three-position type input and output via ADL.
  - In ADL connection, synchronization of open signal and close signal from/to three-position type input and output is not guaranteed. Both open signal and close signal from/to input and output can become ON (PERR status) at the same timing. Mask the PERR alarm using the answer-back inconsistency alarm mask in enhanced Switch Instrument Block or enhanced Motor Control Block for three-position type input and output.
  - For three-position type output, create a logic considering the behavior when both open signal and close signal turn ON at the same timing on the SCS side (which has the priority, for example).
  - When you change the MV in Switch Instrument Block or the Motor Control Block on FCS from 2 to 0, first change it from 2 to 1 then 1 to 0. This will prevent both the ON-open signal and ON-close signal from sending to SCS from FCS. Take enough time when the MV is 1 (twice the time taken in ADL communication period)

Limitations on the number of data setting requests via tag name interfaces

An SCS places priority to executing application logic function within the scan period. Data setting via tag name interface is processed on the basis of maximum 4 packets per second if the scan period is shorter than 250 ms, or one packet per one scan if the scan period is 250 ms or longer. Taking data congestion into consideration, up to 8 packets for setting data can be received and stored as they are generated, and processed internally in sequence at intervals of one scan period of application logic. This number of packets does not include communication via the Modbus slave connection function. If 8 unprocessed packets have accumulated in the SCS, and an additional packet is issued from HIS or FCS, a data setting error is generated.

SCS can process only one communication frame at one time in the order of reception, either from HIS/FCS or from Modbus.

Types and communication packet of data setting requests

The types and communication packet of data setting requests are as follows:

- Data setting requests from an associated faceplate and windows of HIS (one data operation constitutes one communication packet)
- Data setting via SEBOL all-data setting statements of SFC blocks of FCS (one all-data setting statement constitutes one communication packet. Up to 32 data items can be set per all-data setting statement.)

Operations and actions to be taken at error occurrence

The following are operations and actions to be taken if communications become congested and cannot be processed.

- If an error occurs as a result of a data setting request from HIS, the message "Communication error occurred" is displayed. If the reason is that data is set at the same timing as data setting from FCS, avoid the collision and perform data setting again.
- If an error occurs as a result of data setting via a SEBOL statement, an error is stored in the SEBOL error storage variable. A system alarm occurs if no error storage variable has been specified. If large amounts of data need to be set repeatedly with SEBOL statements, the system should be designed accordingly, for example by ensuring that data is set in a specific sequence and confirming that each processing is carried out correctly.

IMPORTANT

Do not set data periodically to SCS from control blocks such as PID or MLD, or from arithmetic/logic calculation blocks such as CALCU, using inter-station data link blocks (ADL) of FCS.

Error codes returned from SCS in CENTUM integration configuration

When you try to set data from CENTUM stations to an SCS on CENTUM Integration, the following error codes may be returned due to an application error.

Table B2-1 Error codes returned by SCS

Error code	Meaning (cause)	Action
0x5408	Setting request buffer in SCS is FULL.	Check the applications that periodically set data to SCS.
0x5409	The number of Setting requests exceeded SCS's capacity.	Check the applications that set a number of data to SCS.

Variable and Function Block to which a tag name can be assigned

In the CENTUM Integration Configuration, the variables or the function blocks of the SCS application logic need to have tag names to be accessed from HIS.

When a tag name is assigned with the tag name builder, a mapping block/element is created. These mapping blocks/elements are accessed from outside.

Tag names can be assigned to I/O variables, internal variables, and certain variables or function blocks including ANLG_S/ANLGI, VEL, HSDTR, GASDTR, OVR_* (Override FB), PASSWD (Password FB), ECW_* (External Communication FB), MOB_* (BOOL-Type Data Manual Operation FB), MOA (Analog-Type Data Manual Operation), SCS_*, SCI_*, SCO_* (Subsystem Communication I/O FB), PSI_I, PSI_R, PNI_I, PNI_R (Safety Subsystem Communication I/O FB), and ANN/ANN_FUP.

SEE ALSO For more information about variables for which tag names can be defined, refer to:

B7.1.5, “Defining tag names” on page B7-12

Engineering procedure of CENTUM integration configuration

In the CENTUM Integration Configuration, engineering needs to be performed by using both the SENG functions and the CENTUM system builders. The following figure shows the engineering procedure in the CENTUM Integration Configuration.

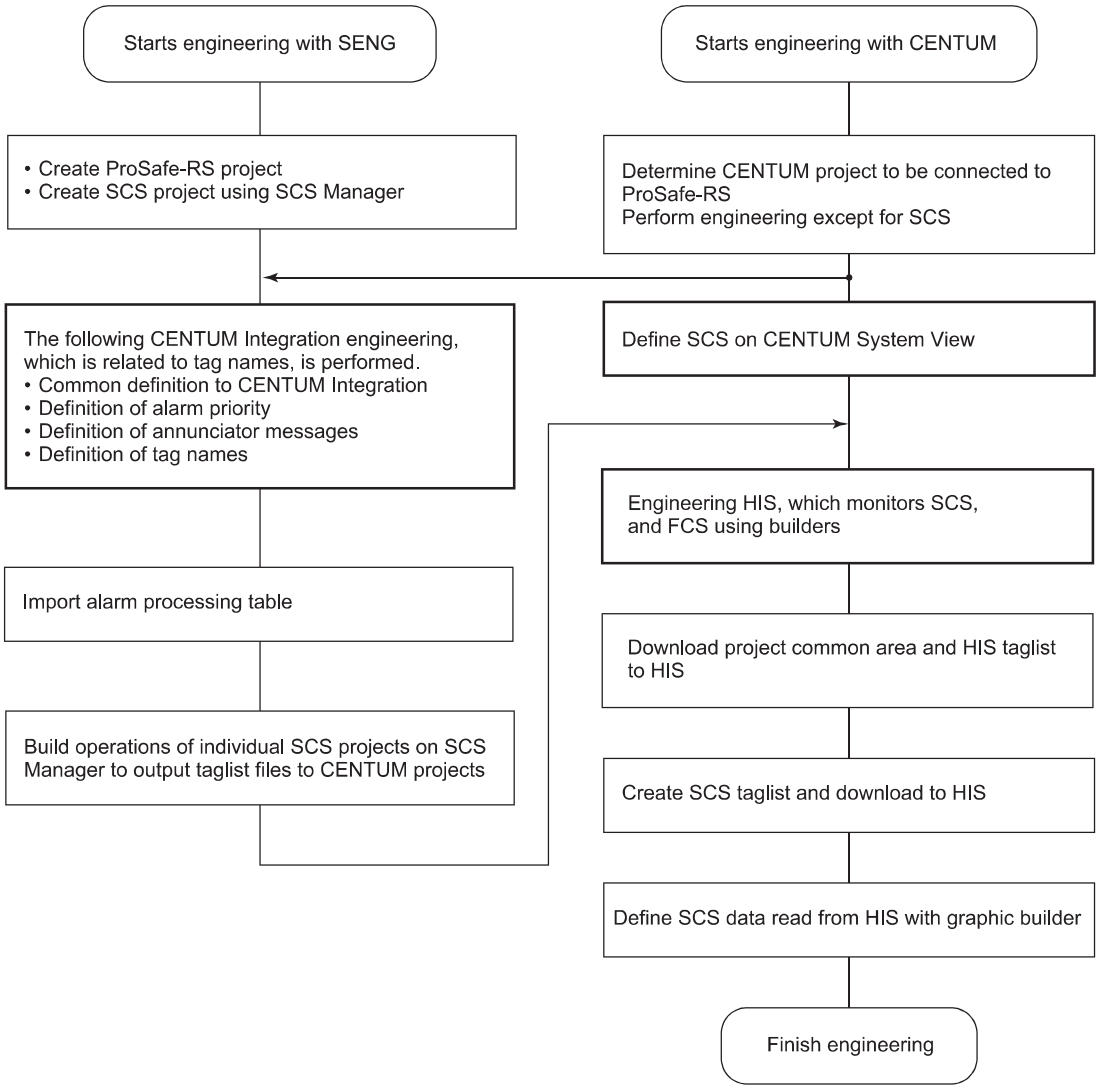


Figure B2-1 Engineering of CENTUM Integration

The following are the engineering items performed by SENG and CENTUM.

Table B2-2 Engineering with SENG

Engineering	Details	Builder to be used
Common definition of CENTUM Integration	Defines the top folder of the CENTUM project for CENTUM Integration	SCS Project Properties
Definition of alarm priority	Defines the handling of SCS process alarms in SCS, which appear on HIS	Alarm Priority Builder
Definition of alarm processing table	Import the alarm processing table, which defined on CENTUM	Alarm processing Builder
Definition of annunciator messages	Defines the contents of process alarms, which appear on HIS	Tag Name Builder (*1)
Definition of tag names	Allows CENTUM to access the variables of application logic by assigning tag names	Tag Name Builder (*1)

*1: In the engineering with iDefine, you can also use iDefine.

Table B2-3 Engineering with CENTUM

Engineering	Description	Builder to be used
Definition of SCS	Defines the SCS as one station of CENTUM projects for connecting SCS project and CENTUM project	System View
Generation of SCS Taglist	Connects the SCS project and CENTUM project. The SCS project is included in the CENTUM project	System View
Definition of SCS data reference from HIS	Creates a Graphic View shown on HIS	Graphic Builder

Perform other engineering for HIS, which includes the trend definition and the operation mark definition for the operation and monitoring function of HIS, and data settings of SCS from FCS as necessary.

Even if SCS project and CENTUM project are disconnected, you can define SCS using the builders for CENTUM. You can also edit the tag name-related application programs and create a database of SCS mapping blocks/elements using the SCS Manager without connecting to the project. However, duplication check for tag names using System View or creating database for operating and monitoring mapping blocks/elements from HIS is not possible if SCS project and CENTUM project are disconnected.

SEE ALSO

For more information about engineering for integration with CENTUM, refer to:

B7., “Engineering for CENTUM integration” on page B7-1

For more information about SCS properties, refer to:

B7.1.1, “Setting of SCS project property” on page B7-4

For more information about Alarm Priority Builder, refer to:

B7.1.2, “Defining alarm priorities” on page B7-5

For more information about Tag name builder, refer to:

B7.1.5, “Defining tag names” on page B7-12

For more information about security operations, refer to:

“■ Security of SCS” in C7., “Offline download to the target SCS” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Relationship between projects

An SCS project is held by the ProSafe-RS system. An RS project, which includes one or more SCS projects, is the unit handled by the SCS Maintenance Support Tool for SCS Status Overview. A CENTUM project is held by the CENTUM system. SCS projects can be connected with CENTUM projects.

When an SCS project is connected with a CENTUM project, SCS is regarded as one station in the CENTUM project. The following figure shows the relationship between projects. It shows, from the top to the bottom, the station structure, projects, and the display on the SCS Maintenance Support Tool, the SCS Manager, and the System View.

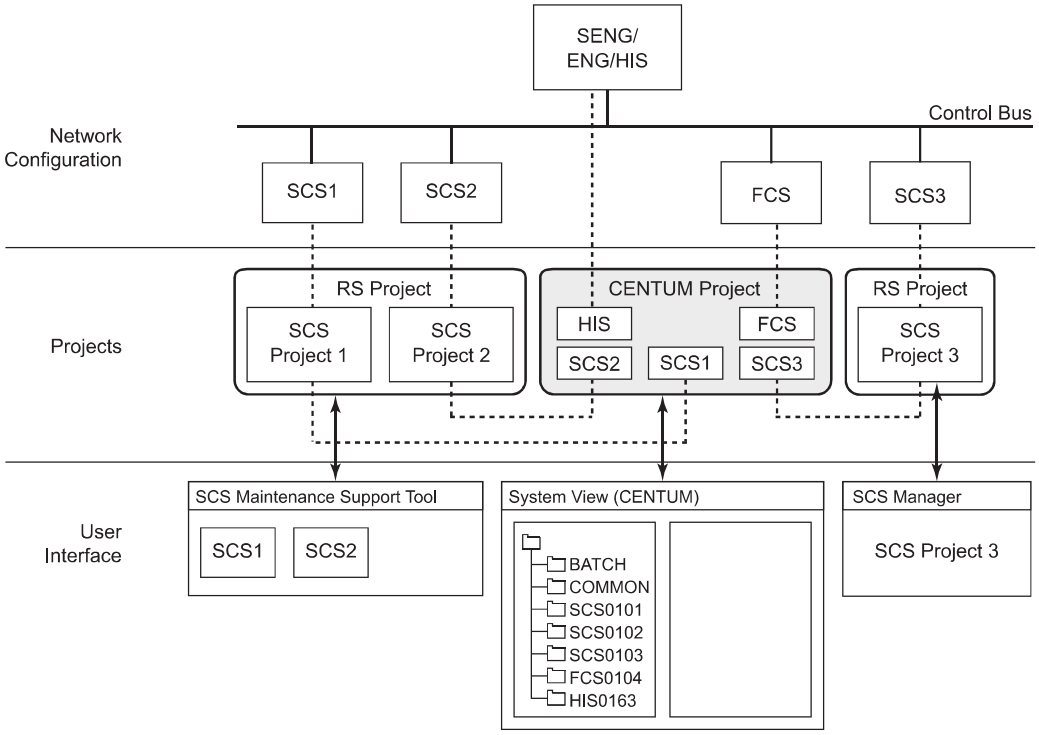


Figure B2-2 Relationship between RS projects, SCS projects, and CENTUM projects

Rules in folder configuration

An RS project and a CENTUM project must be placed in separate folders so that they do not overlap. These two projects can be placed in the same PC or different PCs.

Relationship with tag name generation

HISs and FCSs can access SCS data using tag names. In order to do so, define a list of tag names to be accessed in ProSafe-RS and pass the tag list to CENTUM.

- The SCS engineering functions on the ProSafe-RS output the SCS tag list to the communication folder of the CENTUM project.
- The CENTUM engineering functions on the CENTUM are then able to generate a HIS tag list based on the passed SCS tag list.

B3. Tag name interfaces for CENTUM

Mapping blocks and mapping elements are created when you define tag names for function blocks and variables in an application logic in Tag Name Builder. They allow accessing data using the tag names from an HIS and FCS.

B3.1 Overview of tag name interfaces

In this chapter, the following items regarding tag name interface for CENTUM will be explained.

- Types of mapping blocks and mapping elements for the FBs and variables
- Data size of mapping elements
- Common data items of mapping blocks and mapping elements
- Process alarms

List of mapping blocks/mapping elements

For keeping consistency with the data types of variables and the types of function blocks in the application logics, the types of mapping blocks and mapping elements will be automatically determined on Tag Name Builder according to the data types of variables and the types of function blocks in the application logics.

The table below lists mapping blocks/elements.

Table B3.1-1 Mapping blocks/elements

Classification	Description	Application logic definition		Mapping block/element	
		Classification	Type name	Type	Type name/ element name
Internal Variable	BOOL type	Internal variable	BOOL	Mapping element	%WB
	Integer-type (32-bit)	Internal variable	DINT	Mapping element	%WB
	Real number-type (32-bit)	Internal variable	REAL	Mapping element	%WB
I/O variable	Discrete (FIO)	I/O structure	IO_BOOL	Mapping element	%Z
	Discrete (N-IO)	I/O structure	IO_BOOL	Mapping element	%Y
	Analog	I/O structure	IO_REAL	Mapping element	%WB
Data setting from external device	Data setting (BOOL)	FB	ECW_B	Mapping element	%WB
	Data setting (integer)	FB	ECW_I	Mapping element	%WB
	Data setting (real number)	FB	ECW_R	Mapping element	%WB
Analog input	Analog input FB with data status	FB	ANLG_S	Mapping block	S_ANLG_S
	Analog input indication	FB	ANLGI	Mapping block	S_ANLGI
	Analog input for smoke and heat detectors	FB	HSDTR	Mapping block	S_HSDTR
	Analog input for gas and flame detectors	FB	GASDTR	Mapping block	S_GASDTR
Velocity limit	Velocity limit alarm	FB	VEL	Mapping block	S_VEL

Continues on the next page

Table B3.1-1 Mapping blocks/elements (Table continued)

Classification	Description	Application logic definition		Mapping block/element	
		Classification	Type name	Type	Type name/ element name
Annunciator	Annunciator	FB	ANN	Mapping element	%AN
	First-up alarm annunciator	FB	ANN_FUP	Mapping element	%AN
	Annunciators with tag names	FB	ANN	Mapping element	%AN
Override from HIS	Override (BOOL)	FB	OVR_B	Mapping block	S_OVR_B
	Override (integer)	FB	OVR_I	Mapping block	S_OVR_I
	Override (real number)	FB	OVR_R	Mapping block	S_OVR_R
	Override (discrete)	FB	OVR_IB	Mapping block	S_OVR_IB
	Override (analog)	FB	OVR_IR	Mapping block	S_OVR_IR
	Grouping override (BOOL)	FB	GOV_B	Mapping block	S_GOV_B
	Grouping override (discrete)	FB	GOV_IB	Mapping block	S_GOV_IB
Manual operation	BOOL-type data manual operation FB with two-position answerback	FB	MOB_11	Mapping block	S_MOB_11
	BOOL-type data manual operation FB with three-position answerback	FB	MOB_21	Mapping block	S_MOB_21
	Auto-reset BOOL-type data manual operation	FB	MOB_RS	Mapping block	S_MOB_RS
	Analog-type data manual operation	FB	MOA	Mapping block	S_MOA
Password	Password entry	FB	PASSWD	Mapping block	S_PASSWD
Subsystem communication I/O	Subsystem communication input (BOOL)	FB	SCI_B	Mapping element	%WB
	Subsystem communication input (integer)	FB	SCI_I	Mapping element	%WB
	Subsystem communication input (real number)	FB	SCI_R	Mapping element	%WB
	Subsystem communication output (BOOL)	FB	SCO_B	Mapping element	%WB
	Subsystem communication output (integer)	FB	SCO_I	Mapping element	%WB
	Subsystem communication output (real number)	FB	SCO_R	Mapping element	%WB

Continues on the next page

Table B3.1-1 Mapping blocks/elements (Table continued)

Classification	Description	Application logic definition		Mapping block/element	
		Classification	Type name	Type	Type name/ element name
Safety subsystem communication I/O	Integer-type fire and gas communication input	FB	PSI_I	Mapping element	%XB
	Real-type fire and gas communication input	FB	PSI_R	Mapping element	%XB
	Integer-type PROFINET communication input	FB	PNI_I	Mapping element	%XB
	Real-type PROFINET communication input	FB	PNI_R	Mapping element	%XB

Size of memory used by communication inputs/outputs

The mapping elements corresponding to BOOL-type, DINT-type, REAL-type and IO_REAL-type variables and ECW_B, ECW_I, ECW_R, and subsystem communication I/O function blocks of an application logic are communication I/O (%WB). The mapping elements corresponding to safety subsystem communication I/O function blocks are safety communication I/O (%XB). The following table shows the maximum number of data items that can be mapped and the size of memory used by communication I/O.

Table B3.1-2 Size of memory used by communication inputs/outputs

Description in application logic	Mapping element	Size used	Maximum number of data items that can be mapped
BOOL-type variable	%WB	1 bit	3200 data items in total
ECW_B FB	%WB	1 bit	
DINT-type variable	%WB	2 words	900 data items in total
REAL-type variable	%WB	2 words	
IO_REAL-type variable	%WB	2 words	
ECW_I FB	%WB	2 words	
ECW_R FB	%WB	2 words	
SCI_B (FB)	%WB	1 bit	Up to 2000 data items in total regardless of the size of an FB (1 bit or 2 words)
SCI_I (FB)	%WB	2 words	
SCI_R (FB)	%WB	2 words	
SCO_B (FB)	%WB	1 bit	
SCO_I (FB)	%WB	2 words	
SCO_R (FB)	%WB	2 words	
PSI_I (FB)	%XB	2 words	2000 data items in total
PSI_R (FB)	%XB	2 words	
PNI_I (FB)	%XB	2 words	
PNI_R (FB)	%XB	2 words	

List of data items of mapping blocks/mapping elements

Each mapping block/mapping element has the following data items. See the explanation of each mapping block/mapping element for a detailed explanation of each data item.

Table B3.1-3 List of data items of mapping elements (1/2)

Data item	FB (*1)								
	Internal variable			I/O variable		External communication FB			Annunciator
	BOOL	DINT	REAL	IO_BOOL	IO_REAL	ECW_B	ECW_I	ECW_R	ANN/ANN_FUP
ALRM									Yes
AOFS									Yes
PV	Yes			Yes		Yes			Yes
PVI32		Yes					Yes		
PVU32									
PVF32			Yes		Yes			Yes	
PVI16									
PVU16									
OPMK	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
UAID									Yes

*1: Yes: The data item exists.

Table B3.1-4 List of data items of mapping elements (2/2)

Data item	FB (*1)									
	Subsystem communication inputs			Subsystem communication outputs			Safety subsystem communication I/O			
	SCI_B	SCI_I	SCI_R	SCO_B	SCO_I	SCO_R	PSI_I	PSI_R	PNI_I	PNI_R
ALRM										
AOFS										
PV	Yes			Yes						
PVI32		(*2)			(*2)		(*3)		(*3)	
PVU32							(*3)		(*3)	
PVF32			Yes			Yes		Yes		Yes
PVI16		(*2)			(*2)		(*3)		(*3)	
PVU16		(*2)			(*2)		(*3)		(*3)	
OPMK	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
UAID										

*1: Yes: The data item exists.
*2: In the case of SCI_I/SCO_I, data items vary depending on the data type of communication I/O wired to function blocks. PVI32 if the data type is signed 32-bit integer, PVI16 for signed 16-bit integer and PVU16 for unsigned 16-bit integer.
*3: In the case of PSI_I/PNI_I, data items vary depending on the data type of communication I/O wired to function blocks. PVI32 if the data type is signed 32-bit integer, PVU32 for unsigned 32-bit integer, PVI16 for signed 16-bit integer and signed 8-bit integer, and PVU16 for unsigned 16-bit integer and unsigned 8-bit integer.

Table B3.1-5 List of data items of mapping blocks for each FBs

Data item	FB (*1)											
	ANLG_S	ANL-GI	VEL	OVR_* (*2)	GOV_*(*3)	MOB_11	MOB_21	MOB_RS	MOA	PASSWD	HSDTR	GASDTR
MODE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ALRM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BSTS											Yes	Yes
AFLS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Continues on the next page

Table B3.1-5 List of data items of mapping blocks for each FBs (Table continued)

Data item	FB (*1)											
	ANLG_S	ANL-GI	VEL	OVR_* (*2)	GOV_*(*3)	MOB_11	MOB_21	MOB_RS	MOA	PASSWD	HSDTR	GASDTR
AF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AOFS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
INV	Yes	Yes		Yes	Yes	Yes	Yes		Yes		Yes	Yes
PV	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Yes	Yes	Yes
FPV												Yes
HH	Yes	Yes									Yes	Yes
PH	Yes	Yes										Yes
PL	Yes	Yes										Yes
LL	Yes	Yes										Yes
HYS	Yes	Yes	Yes								Yes	Yes
FSH												Yes
FSL												Yes
F1H												Yes
F1L												Yes
F2H												Yes
F2L												Yes
F3H												Yes
F3L												Yes
OPMK	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
UAID	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SH	Yes	Yes	Yes						Yes		Yes	Yes
SL	Yes	Yes	Yes						Yes		Yes	Yes
VL			Yes									
MV				Yes	Yes	Yes	Yes	Yes	Yes	Yes		
VAL				Yes	Yes							
OUTV				Yes	Yes							
SW				Yes	Yes	Yes	Yes	Yes	Yes			
SHDN						Yes	Yes		Yes			
SS						Yes	Yes					
MTM						Yes	Yes	Yes				
FV									Yes			
SDV									Yes			
MSH									Yes			
MSL									Yes			
MH									Yes			
ML									Yes			
GRNO					Yes							
RSW											Yes	Yes
RREQ											Yes	Yes

Continues on the next page

Table B3.1-5 List of data items of mapping blocks for each FBs (Table continued)

Data item	FB (*1)											
	ANLG_S	ANL-GI	VEL	OVR_* (*2)	GOV_*(*3)	MOB_11	MOB_21	MOB_RS	MOA	PASSWD	HSDTR	GASDTR
RID											Yes	
MOS											Yes	Yes
MV01											Yes	Yes
HTRP											Yes	Yes
LTRP												Yes
HTRR											Yes	Yes
LTRR												Yes
HHH												Yes
LLL												Yes
FAULT												Yes
POFF											Yes	
RSTS											Yes	
OVRS											Yes	Yes
SWLB[1]											Yes	Yes
SWCR[1]											Yes	Yes
SWST[1]											Yes	Yes
SWOP[1]											Yes	Yes
AKLB[1]											Yes	Yes

*1: Yes: The data item exists.
*2: Indicates OVR_B, OVR_I, OVR_R, OVR_IB or OVR_IR.
*3: Indicates GOV_B or GOV_IB.

Data items common to mapping blocks/mapping elements

This section explains data items common to mapping blocks and mapping elements.

AOFS (alarm inhibition)

AOFS is a data item indicating that the process alarm of the function block is inhibited.

This item is not displayed on the HIS tuning view along with the data items, however, the alarm inhibition status can be identified by the color of the tag mark.

The data entry from HIS to this data item is possible. Using the button on the tuning view can change the block into the alarm inhibition status.

The status is as follows:

- Not Inhibit Alarm: 0 (Default)
- Inhibit Alarm: 1

OPMK (operation mark)

This data item indicates operation marks assigned to mapping blocks and mapping elements. It is not displayed in the data item list of the HIS tuning view but operation marks can be assigned using buttons in the tuning view.

Data entry is also allowed.

- Range
  The range of OPMK is from 0 to 255.

- Default
  The default value of OPMK is 0.

UAID (user application ID)

This data item indicates UAIDs corresponding to the upper level equipment names in the plant hierarchy, assigned to mapping blocks.

It is not displayed in the data item list of the HIS tuning view, but data entry is allowed.

The default value is the value specified in the Tag Name Builder.

MODE (block mode)

This data item indicates block mode.

Whether or not the block mode can be displayed on the HIS tuning view and instrument face-plate, what kind of modes a block can have varies with the types of the mapping blocks.

The mode may change according to the parameter changes of the function block, but cannot be changed from HIS.

The following modes are available:

- O/S (Out of Service)
  This is the initial status of a mapping block that all functionalities are not functioning. When SCS is working in normal state, the mapping block will not work in this mode.
- MAN (Manual)
  This is a mode that the output can be manually manipulated.
- IMAN (Initialization Manual)
  This is a mode that the output is disabled.

  This block mode exists together with other block mode.
- AUT (Automatic)
  This is a mode that the output of the function block is enabled.

The default mode of the function block is O/S(AUT), it means the function block is shifting from O/S to AUT mode. (O/S(AUT) is a transition mode.)

AFLS (alarm flashing status)

This data item is not supported. Do not change the data of this item from CENTUM.

AF (alarm detection)

This data item is not supported. Do not change the data of this item from CENTUM.

Process alarms

Process alarms notify process errors detected by the application logic as alarm messages for CENTUM. Though the process alarms are sent by mapping blocks, when the process alarms are displayed on HIS window to indicate abnormality or recovery events, the timestamps of the events will be the reception time that HIS receives the alarms.

Each mapping block provides the following process alarms. Check the explanation of individual function blocks associated with mapping blocks for details of process alarms.

Table B3.1-6 Process alarms generated from mapping blocks

Alarm Status	Mapping block (*1)											
	S_ANLGI	S_ANLG_S	S_VEL	S_OVR_* (*2)	S_GOV_* (*3)	S_PASSWD	S_MOB_21	S_MOB_11	S_MOB_RS	S_MOA	S_HSDTR	S_GASDTR
NR (*4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OOP							Yes	Yes		Yes		
IOP		Yes					Yes	Yes			Yes	Yes
HTRP	Yes	Yes									Yes	Yes
LTRP	Yes	Yes										Yes
HHH	Yes	Yes										Yes
LLL	Yes	Yes										Yes
FLT												Yes
OVR				Yes	Yes							
PERR							Yes					
PWON						Yes						
ANS+				Yes			Yes	Yes				
ANS-				Yes			Yes	Yes	Yes			
VEL+			Yes									
VEL-			Yes									

*1: Yes: Corresponding process alarm is generated.
*2: Indicates S_OVR_B, S_OVR_I, S_OVR_R, S_OVR_IB or S_OVR_IR.
*3: Indicates S_GOV_B or S_GOV_IB.
*4: NR is the status set when other process alarms are not generated. Process alarms are displayed on an HIS in the order in the table with the highest priority on the top item.

B3.2 Tag name interfaces for internal variables and I/O variables

It is possible to define mapping elements for internal variables and I/O variables to reference the data with tag name interfaces. If you define tag names using the Tag Name Builder for BOOL, DINT or REAL-type internal variables, mapping elements are created in the communication input/output (%WB) area.

When a tag name is defined for a discrete I/O variable, the tag name is associated with a %Z or %Y mapping element. When a tag name is defined for an analog I/O variable, the tag name is associated with a %WB mapping element.

■ Data items of mapping elements associated with internal variables

All mapping elements of internal variables provide the OPMK data item.

SEE ALSO For more information about description regarding OPMK (Operation mark), refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

● Data items of mapping elements (%WB) associated with BOOL-type variables (PV)

Boolean values of BOOL-type internal variables are displayed as PV. It is displayed in the HIS tuning view and the parameter display area of instrument faceplate, and will be a target of data collection for tuning trend. Data entry from an HIS is not allowed.

The range is 0 or 1.

● Data items of mapping elements (%WB) associated with DINT-type variable (PVI32)

Integer values of DINT-type internal variables are displayed as PVI32. It is displayed in the HIS tuning view and the parameter display area of instrument faceplate. Data entry from an HIS is not allowed.

The range is all signed 32-bit integers.

● Data items of mapping elements (%WB) associated with REAL-type variables (PVF32)

Real values of REAL-type internal variables are displayed as PVF32. It is displayed in the HIS tuning view and the parameter display area of instrument faceplate. Data entry from an HIS is not allowed.

The range is all single precision real numbers.

■ Data items of mapping elements associated with I/O variables

Mapping elements of I/O variables commonly support the OPMK data item.

SEE ALSO For more information about description regarding OPMK (Operation mark), refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

Data items of mapping elements (%Z, %Y) associated with IO_BOOL-type variables (PV)

Discrete data values are displayed as PV. It is displayed in the HIS tuning view and the parameter display area of instrument faceplate, and will be a target of data collection for tuning trend. Data entry from an HIS is not allowed.

The range is 0 or 1.

Data items of mapping elements (%WB) associated with IO_REAL-type variables (PVF32)

Analog data real values are displayed as PVF32. It is displayed in the HIS tuning view and the parameter display area of instrument faceplate. Data entry from an HIS is not allowed.

The range is all single precision real numbers.

Data access through process I/O terminal numbers (%Z, %Y)

Process I/O terminal numbers (%Z, %Y) corresponding to IO_BOOL type I/O variables are outlined as follows:

- Discrete inputs and outputs are accessed not only via tag names but also process input/output terminal numbers.
- 0 is obtained if data of input/output channels whose I/O variables are not wired is referenced via process input/output terminal number.

Specification syntax (%Z)

%Znnusmm

%Z: : Process I/O (FIO) identifier (fixed to %Z)

nn: : Node number (01 to 14)

u: : Slot number (1 to 8)

s: : Segment number (fixed to 1)

mm: : Terminal number (01 to 16)

Specification syntax (%Y)

%Ynnusmm

%Y : Process I/O (N-IO) identifier (fixed to %Y)

nn : Node number (01 to 32)

u : I/O unit number (1 to 6)

s : Slot number (1 to 2)

mm : Terminal number (01 to 64) [01 to 16: Discrete I/O, 17 to 64: Reserved]

Data items used to reference data status

The table below lists data items used to reference the data status of I/O variables using tag name interfaces.

Table B3.2-1 Referencing data status by tag names

Mapping element	Description	Data item used for data reference	Data item used for data status reference
%Z, %Y	Discrete (IO_BOOL type) inputs and outputs	PV	#PV
%WB	Analog (IO_REAL type) inputs and outputs	PVF32	#PVF32

Input/output status information that can be referenced from HIS and FCS of CENTUM

The I/O status information, which is the basis of the data status of I/O variables, is stored in the CPU. The status information is 32-bit data and structured in the same way as for an FCS.

This 32-bit data is transmitted when HISs and FCSs reference the status of inputs and outputs of an SCS.

The data status of I/O variables is determined by whether or not the BAD status bit is on.

Logical data of I/O variables

Data corresponding to an I/O variable consists of physical data and logical data. Physical data is concrete data such as data input from sensors and data output to actuators. Logical data is the data that can be referenced via an application logic.

The data read by tag name interfaces is logical data. The following table shows how to access data via mapping elements associated with I/O variables.

Table B3.2-2 Access to logical data of I/O variables via tag names

	Discrete	Analog
Reading (logical data)	• Tag name defined for a discrete I/O variable (%Z, %Y) • Process input/output terminal number (%Z, %Y))	Tag name defined for an analog input variable (%WB)
Writing	Not possible	Not possible

Dictionary View of SCS Manager can display both physical data and logical data of I/O variables.

SEE ALSO For more information about physical data and logical data, refer to:

A6.2, “I/O variable” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Conditions under which tag names can be defined

The conditions under which it is allowed to define tag names and assign mapping elements for I/O variables are explained in this section. Discrete I/O variables are of the IO_BOOL type. Analog I/O variables are of the IO_REAL type. Specify the Direction attribute for these variables. There are three options for the Direction attribute: Input, Output and Internal.

- Specify the Input attribute for input variables. When the Input attribute is specified, the variable can be connected to a channel of an input module.
- Specify the Output attribute for output variables. When the Output attribute is specified, the variable can be connected to a channel of an output module.

It is possible to define tag names for IO_BOOL-type and IO-REAL type variables in Tag Builder. The table below shows whether or not tag names can be defined with the Direction attribute. Tag names can be defined for variables with either the Input or Output attribute.

Table B3.2-3 Direction attribute of variables and tag name definition

	Direction (*1)		
	Input	**Output**	**Internal**
IO_REAL	OK	OK	NG
IO_BOOL	OK	OK	NG

*1: OK: tag names can be defined
NG: tag names cannot be defined

B3.3 Tag name interfaces of function blocks

By specifying tag names for function blocks using the Tag Name Builder and associating them with mapping blocks/mapping elements, it becomes possible to call them via the tag names from CENTUM and notify process alarms.

This section explains mapping blocks and mapping elements of the following function blocks.

- Analog input function block with data status (ANLG_S)
- Analog input indication (ANLGI)
- Velocity limit alarm (VEL)
- Annunciator (ANN)
- First-up alarm annunciator (ANN_FUP) (*1)
- Subsystem communication I/O (SCI_B, SCI_I, SCI_R, SCO_B, SCO_I, SCO_R)
- Safety subsystem communication I/O (PSI_I, PSI_R, PNI_I, PNI_R)
- Analog input function block for smoke and heat detectors (HSDTR)
- Analog input function block for gas and flame detectors (GASDTR)

*1: Applicable only when integrated with CENTUM VP R4.02 or later.

SEE ALSO

For more information about override FB, refer to:

B4.2, “Tag name interfaces and process alarms of override function blocks” on page B4-4

For more information about override FB with grouping function, refer to:

B4.4, “Tag name interfaces and process alarms of grouping override function block” on page B4-12

For more information about password FB, refer to:

B4.7, “Tag name interfaces and process alarms of password function blocks” on page B4-21

For more information about BOOL-type manual operation function block with answerback, refer to:

B5.1.6, “Tag name interfaces and process alarms of MOB_11 and MOB_21” on page B5-17

For more information about BOOL-type manual operation with auto-reset function, refer to:

B5.2.2, “Tag name interfaces and process alarms of MOB_RS” on page B5-27

For more information about analog-type manual operation, refer to:

B5.3.2, “Tag name interfaces and process alarms of MOA” on page B5-33

For more information about external communication function blocks, refer to:

B6.2, “Tag name interfaces of external communication function blocks” on page B6-3

■ Data items of mapping blocks associated with analog input function blocks with data status (ANLG_S)

Mapping blocks associated with analog input function blocks with data status are S_ANLG_S.

Among the data items of mapping blocks, the data items unique to S_ANLG_S are explained here. All of these data items are displayed in the HIS tuning view with the exception of MODE and INV. Note that data entry for these data items from an HIS is not allowed.

SEE ALSO

For more information about descriptions regarding MODE (Block mode), AFLS (Alarm flashing status), AF (Alarm detection), AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

“■ Data items common to mapping blocks/mapping elements” on page B3-7

MODE (block mode)

This data item indicates block mode.

The default value of MODE is O/S (AUT).

ALRM (alarm status)

This data item displays alarm status.

The default value of ALRM is NR.

INV (input value)

This item is associated with the IN parameter (analog input) of ANLG_S.

- Range
  INV is normalized data (0 to 100 %) or a physical quantity.
- Default
  The default value of IN (0) of ANLG_S is reflected in the default value of INV.

PV (scale conversion value)

This data item is associated with the OUT parameter (analog output) of ANLG_S. It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend.

In the SCS databases created by R1.03.00 or later versions, the PV data are affixed with data status signals. When the data status of IN signal of ANLG_S becomes BAD, the data status of PV will be set as BAD. However, the data status only indicates BAD. IOP, NFP or other statuses will be ignored.

TIP

- To affix the data status, the item [PV Status of S_ANLG_S] on SCS tab of SCS Constants Builder needs to be defined.
- When the database is created, the PV data are affixed with data status signals at default setting. However, if the above setting is not defined, when CENTUM station read the PV, even though the PV has data status signal, the PV will be always marked as Normal regardless the actual data status.
- In the SCS database created by R1.02, the PV of ANLG_S does not have data status signal.

- Range
  PV is normalized data (0 to 100 %) or a physical quantity.
- Default
  The default value of PV is the SL specified in Tag Name Builder.

HH (high trip setting level)

This data item is associated with the HH parameter (HI trip setting level) of ANLG_S. The HH value of ANLG_S is reflected in this item.

PH (high pre-alarm setting level)

This data item is associated with the PH parameter (HI pre-alarm setting level) of ANLG_S. The PH value of ANLG_S is reflected in this item.

PL (low pre-alarm setting level)

This data item is associated with the PL parameter (LO pre-alarm setting level) of ANLG_S. The PL value of ANLG_S is reflected in this item.

LL (low trip setting level)

This data item is associated with the LL parameter (LO trip setting level) of ANLG_S. The LL value of ANLG_S is reflected in this item.

HYS (hysteresis)

This data item is associated with the HYS parameter (hysteresis) of ANLG_S. The HYS value of ANLG_S is reflected in this item.

SH (scale high limit)

This data item displays the scale high limit defined using the Tag Name Builder.

SL (scale low limit)

This data item displays the scale low limit defined using the Tag Name Builder.

Data items of mapping blocks associated with analog input function blocks (ANLGI)

Mapping blocks associated with analog input indication function blocks are S_ANLGI.

Among the data items of mapping blocks, the data items unique to S_ANLGI are explained here. All of these data items are displayed in the HIS tuning view with the exception of MODE and INV. Note that data entry for these data items from an HIS is not allowed.

SEE ALSO For more information about descriptions regarding MODE (Block mode), AFLS (Alarm flashing status), AF (Alarm detection), AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

"■ List of data items of mapping blocks/mapping elements" on page B3-4

MODE (block mode)

This data item indicates block mode.

The default value of MODE is O/S (AUT).

ALRM (alarm status)

This data item displays alarm status.

The default value of ALRM is NR.

INV (input value)

This data item is associated with the IN parameter (analog input) of ANLGI.

- Range
  INV is normalized data (0 to 100 %) or a physical quantity.
- Default
  The default value of IN (0%) of ANLGI is reflected in the default value of INV.

PV (scale conversion value)

This data item is associated with the OUT parameter (output value) of ANLGI. It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend.

- Range
  PV is normalized data (0 to 100 %) or a physical quantity.
- Default

The default value of PV is the SL specified in Tag Name Builder.

- **HH (high trip setting level)**

  This data item is associated with the HH parameter (High trip setting level) of ANLGI. The HH value of ANLGI is reflected in this item.

- **PH (high pre-alarm setting level)**

  This data item is associated with the PH parameter (High pre-alarm setting level) of ANLGI. The PH value of ANLGI is reflected in this item.

- **PL (low pre-alarm setting level)**

  This data item is associated with the PL parameter (Low pre-alarm setting level) of ANLGI. The PL value of ANLGI is reflected in this item.

- **LL (low trip setting level)**

  This data item is associated with the LL parameter (Low trip setting level) of ANLGI. The LL value of ANLGI is reflected in this item.

- **HYS (hysteresis)**

  This data item is associated with the HYS parameter (hysteresis) of ANLGI. The HYS value of ANLGI is reflected in this item.

- **SH (scale high limit)**

  This data item displays the scale high limit defined using the Tag Name Builder.

- **SL (scale low limit)**

  This data item displays the scale low limit defined using the Tag Name Builder.

■ Data items of mapping blocks associated with velocity limit alarm function blocks (VEL)

Mapping blocks associated with velocity limit alarm function blocks are S_VEL.

Among the data items of mapping blocks, the data items unique to S_VEL are explained here. All of these data items are displayed in the HIS tuning view with the exception of MODE. Note that data entry for these data items from an HIS is not allowed.

SEE ALSO For more information about descriptions regarding MODE (Block mode), AFLS (Alarm flashing status), AF (Alarm detection), AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

- **MODE (block mode)**

  This data item indicates block mode.

  The default value of MODE is O/S (AUT).

- **ALRM (alarm status)**

  This data item displays alarm status.

  The default value of ALRM is NR.

PV (output value)

This data item is associated with the OUT parameter (output value) of VEL. It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend.

- Range
  PV is normalized data (0 to 100 %) or a physical quantity.
- Default
  The default value of PV is the SL specified in Tag Name Builder.

VL (velocity limit alarm setting value)

This data item is associated with the VL parameter (velocity limit alarm setting level) of VEL.

- Default
  The VL value of VEL is reflected in this item.

HYS (hysteresis)

This data item is associated with the HYS parameter (hysteresis) of VEL. The HYS value of VEL is reflected in this item.

SH (scale high limit)

This data item displays the scale high limit defined using the Tag Name Builder.

SL (scale low limit)

This data item displays the scale low limit defined using the Tag Name Builder.

Data items of mapping elements associated with annunciator function blocks (ANN)

Annunciator messages are message outputs that simulate behaviors of annunciator panels of instrument faceplate on an HIS. When you create ANN function blocks for the application logic, %AN mapping elements are created as well. By defining %AN messages in the Tag Name Builder, annunciator messages can be checked from an HIS. Tag name definition is not mandatory.

SEE ALSO For more information about descriptions regarding AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

ALRM (alarm status)

This data item displays alarm status. It is displayed in the HIS tuning view but data entry from an HIS is not allowed.

The default value of ALRM is NR.

PV (input value)

This data item is associated with the IN parameter (input value) of ANN. It is displayed in the HIS tuning view and the parameter display area of instrument faceplate, and will be a target of data collection for tuning trend. Data entry from an HIS is not allowed.

- Range
  The range of PV is 0 or 1.
- Default

The default value of IN (0) of ANN is reflected for the default value of PV.

Data items of mapping elements associated with first-up alarm annunciator function blocks (ANN_FUP)

The first-up alarm annunciator function block has the function to identify the first signal that shifts to the safe state within the same group. The annunciator message is output only when the received signal is the first safe state signal in the group to which the function block belongs.

When you create ANN_FUP function blocks for the application logic, %AN mapping elements are created as well. By defining %AN messages in the Tag Name Builder, annunciator messages can be checked from an HIS (*1). Tag name definition is not mandatory.

Data items of this mapping block are exactly the same as the annunciator function block.

*1: Checking annunciator messages from HIS is supported only when integrated with CENTUM VP R4.02.

Data items of mapping elements associated with subsystem communication inputs/outputs

When you create tag names for SCI_B, SCI_I, SCI_R, SCO_B, SCO_I and SCO_R function blocks in the Tag Name Builder, mapping elements are created in the communication input/output (%WB) area.

Among the data items of mapping elements, the data items unique to subsystem communication inputs/outputs are explained here.

SEE ALSO For more information about the data item OPMK (Operation mark) of subsystem communication inputs and outputs, refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

%WB data items associated with SCI_B and SCO_B (PV: BOOL data)

Mapping elements of SCI_B and SCO_B function blocks have PV (BOOL data) data items.

This data item displays BOOL-type data of the function blocks. It is displayed in the HIS tuning view and the parameter display area of instrument faceplate, and will be a target of data collection for tuning trend. Data entry from an HIS is not allowed.

The range is 0 or 1.

%WB data items associated with SCI_I and SCO_I

In the case of SCI_I and SCO_I, data items of mapping elements vary depending on the data type of communication inputs/outputs (%WB) wired to the function blocks.

Each data item displays integer data of the associated function block and is displayed in the HIS tuning view and the parameter display area of instrument faceplate. Data entry from an HIS is not allowed.

Data items for each data type of communication inputs/outputs are as follows.

- PVI32 (integer data)
  This data item is used when the data type of communication inputs/outputs wired to the associated function block is signed 32-bit integer.

  The range is all signed 32-bit integers.
- PVI16 (integer data)
  This data item is used when the data type of communication inputs/outputs wired to the associated function block is signed 16-bit integer.

  The range is all signed 16-bit integers.

- PVU16 (integer data)
  This data item is used when the data type of communication inputs/outputs wired to the associated function block is unsigned 16-bit integer.

  The range is all unsigned 16-bit integers.

%WB data items associated with SCI_R and SCO_R (PVF32: real number data)

Mapping elements of SCI_R and SCO_R function blocks have PVF32 (real number data) data items.

This data item displays the real number data value of the associated function block. It is displayed in the HIS tuning view and the parameter display area of instrument faceplate. Data entry from an HIS is not allowed.

The range is all single precision real numbers.

Data items of mapping elements associated with safety subsystem communication I/O

When you define tag names for PSI_I, PSI_R, PNI_I, and PNI_R function blocks, mapping elements are created in the area for storing safety subsystem communication I/O (%XB) data. Among the data items of mapping elements, the data items unique to safety subsystem communication I/O are explained here.

SEE ALSO For more information about the data item OPMK (Operation mark) of safety subsystem communication I/O, refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

%XB data items associated with PSI_I and PNI_I

In the case of PSI_I and PNI_I, data items of mapping elements vary depending on the data type of safety subsystem communication I/O (%XB) wired to the function blocks. Each data item is the integer data of the FB. The data items are displayed in the HIS tuning view and the parameter display area of instrument faceplate. Data entry from an HIS is not allowed.

Data items for each data type of safety subsystem communication I/O are as follows:

- PVI32 (integer data)
  This data item is used when the data type of communication I/O wired to the associated function block is signed 32-bit integer.

  The range is all signed 32-bit integers.
- PVU32 (integer data)
  This data item is used when the data type of communication I/O wired to the associated function block is unsigned 32-bit integer.

  The range is all unsigned 32-bit integers.
- PVI16 (integer data)
  This data item is used when the data type of communication I/O wired to the associated function block is signed 16-bit integer or signed 8-bit integer.

  The range is all signed 16-bit integers.
- PVU16 (integer data)
  This data item is used when the data type of communication I/O wired to the associated function block is unsigned 16-bit integer or unsigned 8-bit integer.

  The range is all unsigned 16-bit integers.

%XB data items associated with PSI_R and PNI_R (PVF32: real number data)

Mapping elements of PSI_R and PNI_R function blocks have PVF32 (real number data) data items.

This data item displays the real number data value of the associated function block. It is displayed in the HIS tuning view and the parameter display area of instrument faceplate. Data entry from an HIS is not allowed.

The range is all single precision real numbers.

Data items of the mapping block corresponding to the analog input function block for smoke and heat detectors (HSDTR)

The mapping block corresponding to the analog input function block for smoke and heat detectors is S_HSDTR. Among the data items of this mapping block, the data items unique to S_HSDTR are explained here. MODE, ALRM, BSTS, PV, HH, HYS, SH, SL, RSW, RREQ, RID, MV01, HTRP, and HTRR appear in the tuning view of HIS. Also, entry of data for MV01 only can be performed from HIS.

The data items for which the values of the HSDTR arguments are reflected as is are as follows:

- HH (high trip setting level)
- HYS (hysteresis)
- RSW (reset enabling switch)
- RREQ (reset request not from HIS)
- RID (reset group ID)
- MOS (override switch)
- HTRP (high trip (latched))
- HTRR (high trip raw data)
- POFF (device power off command)
- RSTS (reset status)
- OVRS (override status)

SEE ALSO For more information about descriptions regarding MODE (Block mode), AFLS (Alarm flashing status), AF (Alarm detection), AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

MODE (block mode)

This data item indicates block mode. The block mode cannot be changed into AUT or MAN from an HIS. The default value of MODE is O/S (AUT).

- Associating parameters of function blocks
  RSW (reset request from HIS) parameter of HSDTR is associated with MODE.
- Changes of block mode (AUT/MAN)
  The block mode becomes MAN if TRUE is input to RSW, and AUT if FALSE is input.

ALRM (alarm status)

This data item displays alarm status. The default value of ALRM is NR.

BSTS (block status)

This data item displays the block status. BSTS becomes RST when RSTS is TRUE. BSTS becomes OVR when OVRS is TRUE. In all other cases, BSTS becomes NR. When RSTS is TRUE and OVRS is TRUE, the block status displayed on the instrument faceplate becomes RST.

INV (input value)

This data item is associated with the IN parameter (analog input) of HSDTR.

- Range
  INV is normalized data (0 to 100 %) or a physical quantity.
- Default
  The default value of IN (0) of HSDTR is reflected in the default value of INV.

PV (scale conversion value)

This data item is associated with the OUT parameter (analog output) of HSDTR. It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend. When the data status of IN signal of HSDTR becomes BAD, the data status of PV will be set as BAD. However, the data status only indicates BAD. IOP, NFP or other statuses will be ignored.

- Range
  PV is normalized data (0 to 100 %) or a physical quantity.
- Default
  The default value for PV is the SL specified with Tag Name Builder.

SH (scale high limit)

This data item displays the scale high limit defined using Tag Name Builder.

SL (scale low limit)

This data item displays the scale low limit defined using Tag Name Builder.

MV01 (reset request from HIS)

This value changes to 1 when the reset button is operated with HIS. The value will return to 0 when startup of the device is complete.

- Range
  The range of MV01 is 0 or 1.
- Default
  The default value of MV01 is 0.

SWLB[1] (switch label)

The string of Button Label defined using Tag Name Builder is reflected as is.

SWCR[1] (switch indication color)

While in the reset status, the value of Button Color (Resetting) defined using Tag Name Builder is reflected as is. While not in the reset status, the value of Button Color (Normal) defined using Tag Name Builder is reflected as is.

SWST[1] (switch flashing status)

This item is not used. The value of 0 is constantly set.

SWOP[1] (switch operation disable status)

While the operation guard is displayed, the value of Operation Guard Color defined using Tag Name Builder is reflected as is. The value of 0 is set when the operation guard is not displayed.

AKLB[1] (reconfirmation label)

This data item displays the string that is displayed in the reconfirmation dialog box. The string of Button Label defined using Tag Name Builder is reflected as is. The string is the same as SWLB[1].

Data items of the mapping block associated with the analog input function block for gas and flame detectors (GASDTR)

The mapping block is associated with the analog input function block for gas and flame detectors is S_GASDTR. Among the data items of this mapping block, the data items unique to S_GASDTR are explained here. MODE, ALRM, BSTS, PV, FPV, HH, LL, PH, PL, HYS, F1H, F1L, F2H, F2L, F3H, F3L, SH, SL, RSW, RREQ, MV01, HTRP, LTRP, HTRR, LTRR, and FAULT appear in the tuning view of HIS. Also, entry of data for MV01 only can be performed from HIS.

The data items for which the values of the GASDTR arguments are reflected as is are as follows:

- HH (high trip setting level)
- LL (low trip setting level)
- PH (high pre-alarm setting level)
- PL (low pre-alarm setting level)
- HYS (hysteresis)
- FSH (scale high limit for fault)
- FSL (scale low limit for fault)
- F1H (fault 1 upper limit)
- F1L (fault 1 lower limit)
- F2H (fault 2 upper limit)
- F2L (fault 2 lower limit)
- F3H (fault 3 upper limit)
- F3L (fault 3 lower limit)
- RSW (reset enabling switch)
- RREQ (reset request not from HIS)
- MOS (override switch)
- HTRP (high trip (latched))
- LTRP (low trip (latched))
- HTRR (high trip raw data)
- LTRR (low trip raw data)
- HHH (HI pre-alarm)
- LLL (LO pre-alarm)

- OVRS (override status)

SEE ALSO For more information about descriptions regarding MODE (Block mode), AFLS (Alarm flashing status), AF (Alarm detection), AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

● MODE (block mode)

This data item indicates block mode. The block mode cannot be changed into AUT or MAN from an HIS. The default value of MODE is O/S (AUT).

- Associating parameters of function blocks
  RSW (reset request from HIS) parameter of GASDTR is associated with MODE.
- Changes of block mode (AUT/MAN)
  The block mode becomes MAN if TRUE is input to RSW, and AUT if FALSE is input.

● ALRM (alarm status)

This data item displays alarm status. The default value of ALRM is NR.

● BSTS (block status)

This data item displays the block status. BSTS becomes OVR when OVRS is TRUE. In all other cases, BSTS becomes NR.

● INV (input value)

This data item is associated with the IN parameter (analog input) of GASDTR.

- Range
  INV is normalized data (0 to 100 %) or a physical quantity.
- Default
  The default value of IN (0) of GASDTR is reflected in the default value of INV.

● PV (scale conversion value)

This data item is associated with the OUT parameter (analog output) of GASDTR. It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend. When the data status of IN signal of GASDTR becomes BAD, the data status of PV will be set as BAD. However, the data status only indicates BAD. IOP, NFP or other statuses will be ignored.

- Range
  PV is normalized data (0 to 100 %) or a physical quantity.
- Default
  The default value for PV is the SL specified with Tag Name Builder.

● FPV (PV for fault detection)

This data item displays the scale conversion value for fault detection.

● SH (scale high limit)

This data item displays the scale high limit defined using Tag Name Builder.

● SL (scale low limit)

This data item displays the scale low limit defined using Tag Name Builder.

MV01 (reset request from HIS)

This value changes to 1 when the reset button is operated with HIS. The value will return to 0 when resetting of the alarm is complete.

- Range
  The range of MV01 is 0 or 1.
- Default
  The default value of MV01 is 0.

FAULT (fault details)

This data item displays the fault details. The string specified with IDF1 appears when FLT1 is TRUE. The string specified with IDF2 appears when FLT2 is TRUE. The string specified with IDF3 appears when FLT3 is TRUE.

SWLB[1] (switch label)

The string of Button Label defined using Tag Name Builder is reflected as is.

SWCR[1] (switch indication color)

The value of Button Color (Normal) defined using Tag Name Builder is reflected as is.

SWST[1] (switch flashing status)

This item is not used. The value of 0 is constantly set.

SWOP[1] (switch operation disable status)

While the operation guard is displayed, the value of Operation Guard Color defined using Tag Name Builder is reflected as is. The value of 0 is set when the operation guard is not displayed.

AKLB[1] (reconfirmation label)

This data item displays the string that is displayed in the reconfirmation dialog box. The string of Button Label defined using Tag Name Builder is reflected as is. The string is the same as SWLB[1].

B4. Override operation from HIS

The override operations can be carried out from an HIS to an SCS. To perform the override operation, an override function block or grouping override function block is used. Using grouping override function blocks allows you to manage these function blocks as a group. This chapter explains the following points related to override operations from an HIS.

- Overview of override function blocks
- Tag name interfaces and process alarms of override function blocks
- Overview of grouping override function blocks
- Tag Name Interfaces and Process Alarms of Grouping Override Function Block
- Status Management of Function Blocks Used for Override
- Management of override using password function block
- Tag Name Interfaces and Process Alarms of Password Function Blocks

Function blocks related to override operations

During the normal operation of SCS, the operation override is performed from an HIS to fix the variable value to a predefined value that is different from the actual value.

The operation uses an override function block or grouping override function block, and is permitted by hardware switch or the password function block.

The following function blocks are supported for override operation.

Table B4-1 Function blocks related to override operations

Type of FB	Name of FB	Description
override FB	OVR_B	BOOL-type data override
	OVR_I	Integer-type data override
	OVR_R	REAL-type data override
	OVR_IB	IO_BOOL-type data override
	OVR_IR	IO_REAL-type data override
Grouping override FB	GOV_B	BOOL-type data grouping override
	GOV_IB	IO_BOOL-type data grouping override
Password FB	PASSWD	Password

B4.1 Overview of override FB

To perform override to the data from HIS that is not required for group management, the Override function block can be used. An override function block is provided for each data type.

Mechanism of override function blocks

The following figure illustrates an example where an input variable is overridden using an override function block for IO_BOOL-type variable (OVR_IB). In the example of overriding an input variable, the override function block is positioned immediately after the variable to be overridden.

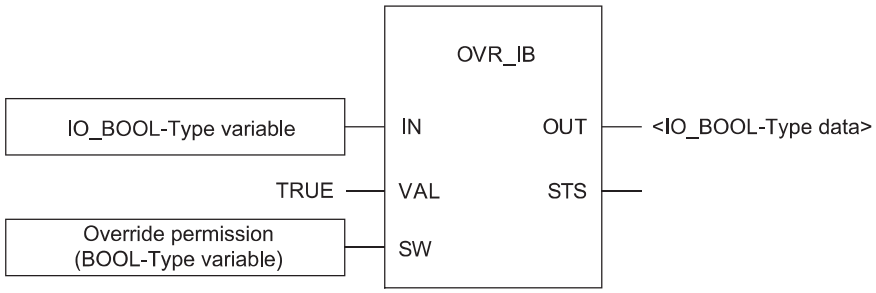


Figure B4.1-1 Example of using OVR_IB function block for an input variable

In the normal status where the variable is not overridden, the OVR_IB function block outputs the data input via input parameter IN as is from output parameter OUT. When an override operation is specified from the HIS via the mapping block, the OVR_IB function block outputs the value specified for input parameter VAL (TRUE in this case) from output parameter OUT. During overriding, the data status of output parameter OUT is always TRUE (GOOD). If the override operation is canceled from the HIS, the OVR_IB function block outputs the data input via input parameter IN as is from output parameter OUT again.

A BOOL-type variable is specified for input parameter SW of the OVR_IB function block. Under normal circumstances, this BOOL-type variable is set to be an input variable from a key switch. If the user operates the key switch, the BOOL-type variable value changes. If the BOOL-type variable becomes TRUE, input parameter SW of OVR_IB also becomes TRUE, and an override operation is permitted. If the variable becomes FALSE, the override operation is prohibited.

Note that the override operation is not canceled even if input parameter SW changes from TRUE to FALSE while the override instruction is active; output parameter OUT keeps on outputting the value specified for input parameter VAL.

TIP

It is possible to change values of BOOL-type variables by entering data along with the correct password from the faceplate of an HIS by using the password function block. Utilizing this mechanism, it can be specified whether or not to allow override operations using the password function instead of using hardware such as a key switch.

SEE ALSO

For more information about engineering of override function blocks, refer to:

B7.1.6, “Engineering for overriding from HIS” on page B7-29

For more information about password function block, refer to:

7.3, “PASSWD (password)” in POU Reference Manual (IM 32P03B20-01EN)

Data status of I/O variables

OVR_IB and OVR_IR are override function blocks for IO_BOOL-type variables and IO_REAL-type variables, respectively. These override function blocks fix the data status of output pa-

rameter OUT of the associated variables to TRUE (GOOD), which is output when the variables are placed in the override status.

The figure below illustrates a usage example of the override function block for IO_REAL-type variables. When the override status of the function block is activated via a mapping block from an HIS, output parameter OUT outputs the following.

- The data value of OUT (member "v" of structure IO_REAL) is set to the value input via input parameter VAL, which is then output to the output side. The output is fixed to 20.0 in the example of the figure below.
- The data status of OUT (member "status" of structure IO_REAL) is fixed to TRUE (GOOD).

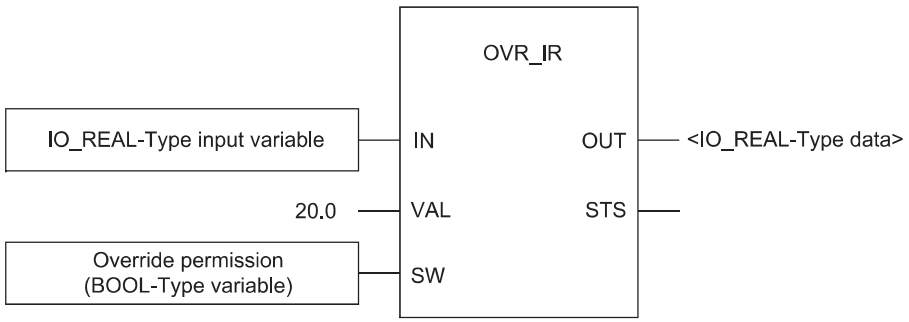


Figure B4.1-2 Override of IO_REAL-type variable

When the override operation of the function block is activated, the data status of output parameter OUT is fixed to TRUE (GOOD) but the data status of input variables connected to input parameter IN is not influenced. If the override function block is placed in the override status, only output parameters OUT and STS change.

B4.2 Tag name interfaces and process alarms of override function blocks

To be able to perform override operations from an HIS using an override function block, it is necessary to define the tag name in the Tag Name Builder and associate it with a mapping block.

Mapping blocks associated with override function blocks

The following table shows mapping blocks associated with override function blocks.

Table B4.2-1 Mapping blocks associated with override function blocks

Override FB type	Mapping block type
OVR_B	S_OVR_B
OVR_I	S_OVR_I
OVR_R	S_OVR_R
OVR_IB	S_OVR_IB
OVR_IR	S_OVR_IR

SEE ALSO For more information about procedure for defining the mapping blocks of override function blocks, refer to:

B7.1.6, “Engineering for overriding from HIS” on page B7-29

Settings in the Tag Name Builder

To be able to perform override operations from an HIS, it is necessary to make settings for instances of override function blocks in the Tag Name Builder.

Use the Tag Name Builder to make specification for alarms during override operation and answerback error alarms.

- Override ON alarm
  Specify either [Yes] or [No].

  The default is [Yes].
- Answerback error alarm
  Specify either [Both] or [No].

  The default is [Both].

SEE ALSO For more information about items defined in the tag name builder, refer to:

B7.1.5, “Defining tag names” on page B7-12

Data items of mapping blocks associated with override function blocks

Among the data items of mapping blocks, the data items unique to mapping blocks of override function blocks are explained here. All of these data items are displayed in the HIS tuning view with the exception of MODE. Note that data entry for these data items from an HIS is allowed only for MV.

SEE ALSO For more information about descriptions regarding MODE (Block mode), AFLS (Alarm flashing status), AF (Alarm detection), AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

MODE (block mode)

This data item indicates block mode.

The default value of MODE is O/S (AUT).

ALRM (alarm status)

This data item displays alarm status.

The default value of ALRM is NR.

PV (answerback input value)

This data item displays the override status and will be a target of data collection for tuning trend.

- Associating parameters of function blocks
  The STS parameter (override status) of override function blocks is associated with PV.
- Range
  The range of PV is 0 or 1.
- Correspondence between changes of the parameter value of override function blocks and changes of PV
  If STS of an override function block is TRUE, PV=1 and override operations from an HIS are executed.
- Default
  The default value of STS (0) is reflected in the default value of PV.

MV (manipulated output value)

Override operations are permitted if SW of an override function block is 1, and MV can be manipulated from an HIS. This item will be a target of data collection for tuning trend.

- Range
  The range of MV is 0 or 1.
- Default
  The default value of MV is 0.

INV (input value)

This data item is associated with the IN parameter (input) of an override function block. This is displayed in the parameter display area of instrument faceplate. This value is output from OUT when no override operation is performed. The IN value of an override function block is reflected in this item.

VAL (fixed value)

This data item is associated with the VAL parameter (override value) of an override function block. This is displayed in the parameter display area of instrument faceplate. This value is output from OUT when override operations are performed. The VAL value of an override function block is reflected in this item.

OUTV (output value)

This data item is associated with the OUT parameter (output value) of an override function block This is displayed in the parameter display area of instrument faceplate. The OUT value of an override function block is reflected in this item.

SW (switch)

This data item is associated with the SW parameter of an override function block. The range is 0 or 1. Override operations are permitted when the value of SW is 1. The SW value of an override function block is reflected in this item.

Process alarm

Mapping blocks of the override function blocks generate two types of process alarms, override ON and answerback error alarms. It is possible to specify whether or not to initiate this process alarms using the Tag Name Builder.

Answerback error alarms

Answerback error alarms can be used to examine whether or not an override operation from an HIS is functioning as instructed. A mapping block mediates the override operation between a faceplate on the HIS side and an override function block.

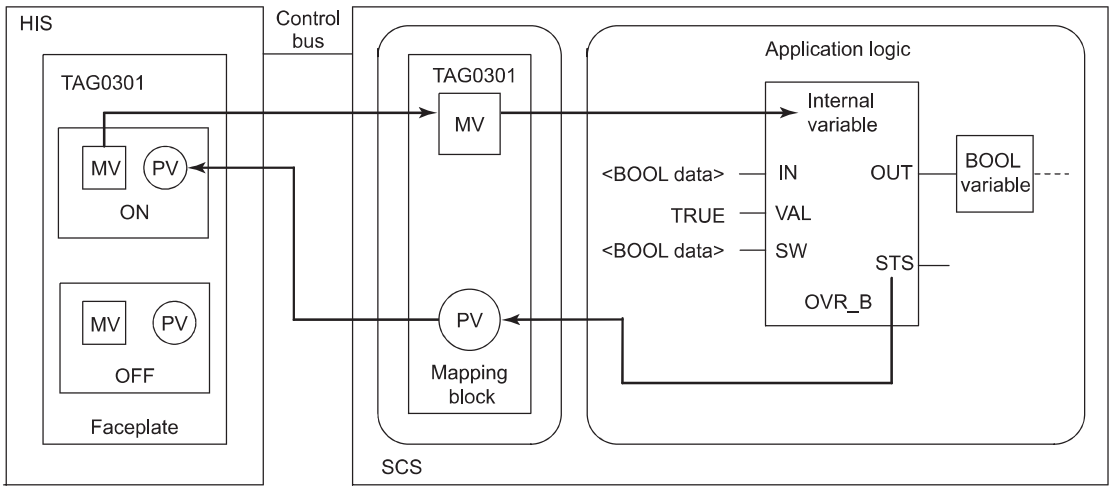


Figure B4.2-1 Flow of data between override function block and mapping block

If you perform an override operation from the faceplate of the HIS, the mapping block stores the value "1", which means "instruct override", in its own data item MV. The data of MV is then set to the internal variable of the override function block. The override function block examines the validity of the set data. If the data is considered valid, the override function block goes into override condition and changes the STS from FALSE to TRUE.

The mapping block reads the STS value of the override function block into the PV of the mapping block at the next scan period. The scan period of the mapping block is the same as the scan period of the external communication function. The default value is 1 second.

If the value (MV) instructed by the mapping block and the status value (PV) read back from the STS output of the override function block do not match, the mapping block generates an answerback error alarm. If they match later, the mapping block recovers from the answerback error alarm.

An answerback error alarm is generated under the following conditions.

- ON side answerback error alarm (ANS+)
  MV = 1 and PV ≠ 1

- OFF side answerback error alarm (ANS-)
  MV = 0 and PV ≠ 0

The mapping block recovers from an answerback error alarm under the following conditions.

- ON side answerback error alarm (ANS+)
  When PV changes to 1 or MV changes to a value other than 1
- OFF side answerback error alarm (ANS-)
  When PV changes to 0 or MV changes to a value other than 0

Override ON alarm

Override ON alarms can be used to notify an operator that the function block corresponding to the tag name of an SCS is being overridden. A mapping block generates an override ON alarm if an override function block is placed in the override status. Once the override status is canceled, the mapping block recovers from the override ON alarm.

An override ON alarm is generated under the following condition.

- PV = 1 (STS of the override function block is 1)

The mapping block recovers from an override ON alarm under the following condition.

- PV = 0 (STS of the override function block is 0)

B4.3 Overview of grouping override function block

When it is necessary to exclusively manage override operations from an HIS to multiple data items, grouping override function blocks can be used.

Types of grouping override function block are shown below.

- GOV_B BOOL-type data grouping override
- GOV_IB IO_BOOL-type data grouping override

This section explains the following functions of grouping override function block. GOV_B and GOV_IB differ only in the type of data they can handle. Their basic functions are identical.

- Group function
- Override permit switch
- Override enable status
- Block mode
- Override status cancel function
- Data status for OUT parameter of GOV_IB function block
- Operation of grouping override function block

Group function

By using a grouping override function block, it is possible to restrict the override operation of multiple data items that are defined as a group to only one at a time. Multiple groups can be defined within an SCS. The override operations can be performed simultaneously to grouping override function blocks that belong to separate groups.

There are no limits to the number or types of grouping override function blocks that can be defined as a group. Both GOV_B and GOV_IB can be included in a same group.

- If the override operation is performed for a grouping override function block in a group, the operation cannot be performed on other function blocks in the same group until it completes. When the override operation is attempted simultaneously on another function block within the same group, the override operation for that function block will be disabled.
- It is also possible to enable the override operation for individual function blocks, without grouping, using a grouping override function block.

Group number

Group number is defined for GRP. Multiple groups can be defined by assigning different group numbers.

- Up to 128 groups can be managed by a single SCS. Specify a group number (1 to 128) for GRP.
- When the group number is set to 0, that grouping override function block does not belong to any group. The number limitation on simultaneous operations will be invalid, and the override operation can be performed without being affected by the exclusive control on the override operations for other grouping override function blocks.
- The override operation cannot be performed if the group number is set to a negative number or a number equal to or greater than 129.

Override permit switch

The override operation can be performed from an HIS when the override permit switch (SW) is set to TRUE (override allowed). When SW is set to FALSE (override prohibited), the override operation cannot be performed from an HIS.

The Override Enabled status

Override Enable Status (ENS) indicates whether the override operation for a grouping override function block is allowed.

When SW is set to TRUE (override allowed) and there are no other grouping override function blocks for which override is being executed within the same group, ENS becomes TRUE (override enable status), and the override operation can be performed.

However, if there is a function block for which override is being executed within the same group, ENS of other function blocks in the group becomes FALSE (override disable status), and the override operation cannot be performed.

If SW is set to FALSE (override prohibited), ENS will always be FALSE (override disable status).

TIP

- When the group number is 0
  When the group number is set to 0, if the override permit switch (SW) is TRUE, the override enable status (ENS) is always TRUE. MODE indicated on the HIS instrument faceplate is MAN.
- When the group number is negative, or 129 or greater
  When a value outside the range is specified as the group number, the override enable status (ENS) is fixed to FALSE regardless of the state of override permit switch (SW). The override operation is not allowed. MODE indicated on the HIS instrument faceplate is always AUT.

Block mode

- The override enable status can be checked from the block mode (MODE) by specifying the tag name assigned to a grouping override function block and then calling the HIS instrument faceplate. The block mode reflects the state of the function block's override enable status (ENS). MODE becomes MAN when ENS is TRUE, and AUT when FALSE.
- The override operation is allowed only when MODE is MAN. When the override operation is not permitted because the override permit switch (SW) is FALSE, or when override is being executed for another function block in the same group, MODE indicates AUT.

Override status cancel function

Grouping override function blocks have the override status cancel function.

By changing from TRUE to FALSE the override permit switch (SW) of a grouping override function block for which override is being executed, the override status will be canceled. At that time, the override enable status (ENS) becomes FALSE.

TIP

The override status is canceled under the following conditions as well.

- When a forced cancellation command is issued from the SYS_OVR block
- When the group number is changed (The group number should be set to a fixed value. The online change download during the override operation is prohibited.)

Data status for OUT parameter of GOV_IB function block

During the override execution of GOV_IB function block, the data status of IO_BOOL-type output (OUT) will be GOOD. When override is not being executed, the data status of input parameter IN will be output as the data status of OUT.

During the override execution, if the override permit switch (SW) changes from TRUE to FALSE, or if SYS_OVR issues a forced cancellation command, the override status will be canceled even if IN data status is BAD.

Operation of grouping override function blocks

Execution of override

Grouping override function block outputs the data input from IN as is from OUT when there is no override execution.

1. Set the override permit switch (SW) to TRUE.
2. If there are no function blocks for which override is being executed within the group, MODE of tag assigned to the function block becomes MAN, the override operation can be performed. If the override operation is not allowed, MODE stays AUT.
3. If MV is set to 1 from the HIS instrument faceplate and PV of answerback signal changes to 1, data specified by VAL will be output from OUT of the grouping override function block. At this time, the mode of other function blocks that belong to the same group will be AUT.

TIP

When the override operation is disabled, or when the override status is canceled by setting SW to FALSE, MV will be reset to 0 and PV of answerback signal will be 0 as well.

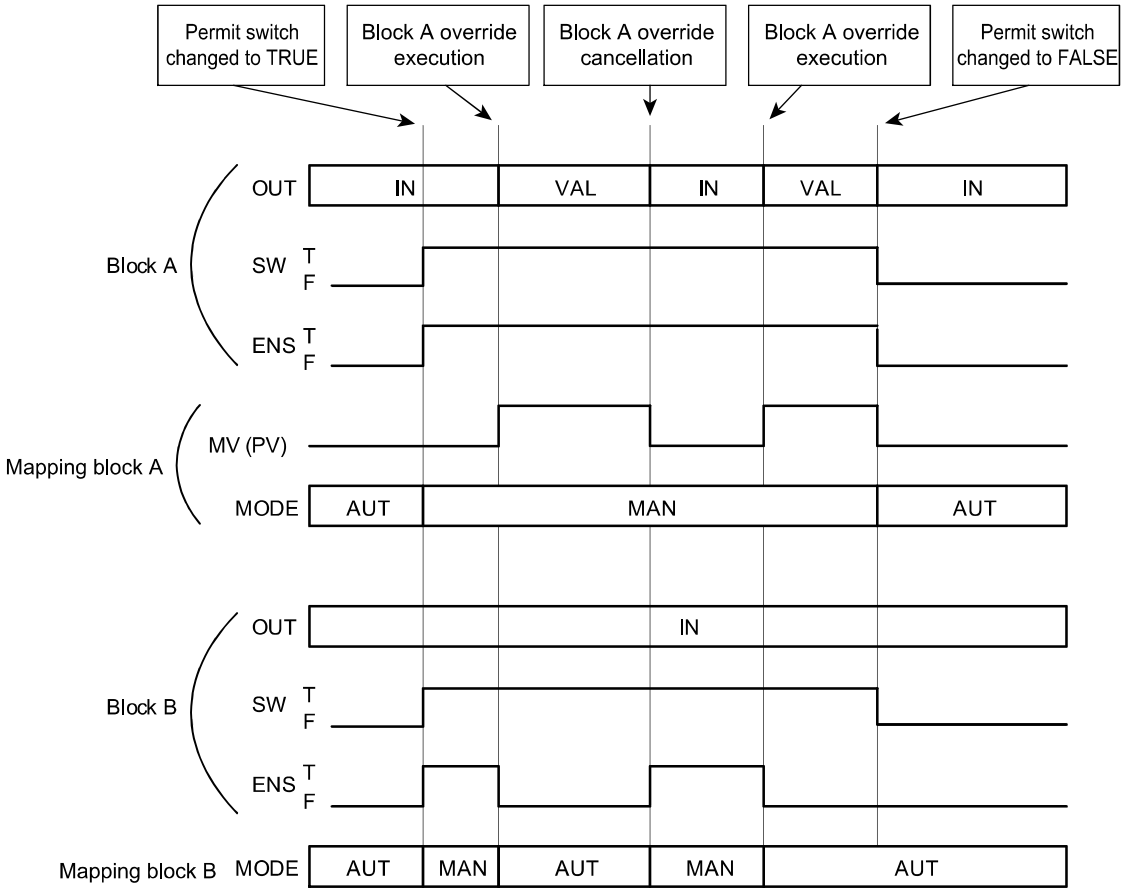
End of override

When MV is set to 0 from an HIS and the override status is canceled, the data input from IN will be output again from OUT of the grouping override function block. At this time, the mode of all function blocks that belong to the same group becomes MAN (*1).

*1: Even if it belongs in the same group, the mode of the function block whose override permit switch (SW) is set to FALSE stays AUT.

Data change during override

The figure below shows the changes in each data when block A and block B that belong to the same group are connected to the same override permit signal, and the override operation is performed for block A.



Block A is the function block for which override is executed, while block B is another function block within the same group.

Figure B4.3-1 State transition of blocks in the same group

B4.4 Tag name interfaces and process alarms of grouping override function block

To perform the override operation from an HIS using the group function, it is necessary to specify the tag name with Tag Name Builder and assign mapping blocks.

■ Mapping blocks associated with grouping override function blocks

Mapping blocks associated with grouping override function blocks are shown in the table below.

Table B4.4-1 Mapping blocks associated with grouping override function blocks

Override FB type	Mapping block type
GOV_B	S_GOV_B
GOV_IB	S_GOV_IB

■ Settings in the Tag Name Builder

When the override operation is performed from an HIS, set necessary items for the instance of grouping override function block with Tag Name Builder.

The following item is set for Alarm in Overriding.

- Alarm in overriding
  Specify either [Yes] or [No].

  The default is [Yes].

SEE ALSO For more information about items defined in the tag name builder, refer to:

B7.1.5, “Defining tag names” on page B7-12

■ Data items of mapping blocks associated with grouping override function blocks

Among the data items of mapping blocks, the data items unique to mapping blocks associated with grouping override function blocks are explained here. All of these data items are displayed in the HIS tuning view. Note that data entry for these data items from an HIS is allowed only for MV.

SEE ALSO For more information about descriptions regarding MODE (Block mode), AFLS (Alarm flashing status), AF (Alarm detection), AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

“■ Data items common to mapping blocks/mapping elements” on page B3-7

● MODE (block mode)

This data item indicates block mode. It is possible to check whether the override operation can be performed. MAN indicates the operation enable status, while AUT means the system prohibits override execution and MV manipulation (executing/ending override) from an HIS is not allowed in this case.

It is not possible to change the block mode to AUT or MAN from an HIS or FCS. The default value of MODE is O/S (AUT). This is displayed in the parameter display area of instrument faceplate.

- Associating parameters of function blocks

The ENS parameter (override enable status) of grouping override function blocks is associated with MODE.

- Change in block mode (AUT/MAN)
  If ENS is TRUE, the block mode is MAN; if FALSE, AUT.

ALRM (alarm status)

This data item displays alarm status.

The default value of ALRM is NR.

PV (answerback input value)

This data item displays the override status. This item will be a target of data collection for tuning trend.

- Associating parameters of function blocks
  The STS parameter (output status) of grouping override function blocks is associated with PV.
- Range
  The range of PV is 0 or 1.
- Correspondence between changes of the parameter value of grouping override function blocks and changes of PV
  If STS of a grouping override function block is TRUE, PV = 1 and override operations from an HIS are executed.
- Default
  The default value of STS (0) is reflected in the default value of PV.

MV (manipulated output value)

Override operations are permitted if the block mode is MAN, and MV can be manipulated from an HIS. This item will be a target of data collection for tuning trend.

- Range
  The range of MV is 0 or 1.
- Default
  The default value of MV is 0.

INV (input value)

This data item is associated with the GRP parameter (group number) of a grouping override function block. This is displayed in the parameter display area of instrument faceplate. This value is output from OUT when no override operation is performed.

The IN value of a grouping override function block is reflected in this item.

VAL (fixed value)

This data item is associated with the VAL parameter (fixed value) of a grouping override function block and is displayed in the parameter display area of instrument faceplate. This value is output from OUT when override operations are performed. The VAL value of a grouping override function block is reflected in this item.

OUTV (output value)

This data item is associated with the GRP parameter (group number) of a grouping override function block. This is displayed in the parameter display area of instrument faceplate. The OUT value of a grouping override function block is reflected in this item.

SW (switch)

This data item is associated with the SW parameter (override permit switch) of a grouping override function block.

- Range
  The range of SW is 0 or 1. The SW value of a grouping override function block is reflected in this item.
- Operations by SW changes
  Override operations are permitted only if the SW value is 1. However, the override operation can actually be performed for the function block only when the MODE is MAN.

  When SW changes from 1 to 0, the override status is canceled.

GRNO (group number)

This data item is associated with the GRP parameter (group number) of a grouping override function block. This item indicates the group number to which the function block belongs. If the value is 0, the function block does not belong to any group. The GRP value of a grouping override function block is reflected in this item.

Process alarm

Override ON alarms are notified from grouping override function blocks.

Override ON alarm

Override ON alarms can be used to notify an operator that a function block is being overridden. A mapping block generates an override ON alarm if an override function block is placed in the override status. Once the override status is canceled, the mapping block recovers from the override ON alarm.

An override ON alarm is generated under the following condition.

- PV = 1 (STS of the override function block is 1)

The mapping block recovers from an override ON alarm under the following condition.

- PV = 0 (STS of the override function block is 0)

B4.5 Status management of function blocks used for override

The SYS_OVR system function block can equally manage the statuses of override function blocks and grouping override function blocks regardless of function block types. In this section, override function blocks and grouping override function blocks are collectively referred to as override function blocks.

SEE ALSO For more information about SYS_OVR, refer to:

11.10, “SYS_OVR (override function blocks management)” in POU Reference Manual (IM 32P03B20-01EN)

Cancellation of all override statuses

The SYS_OVR function block can cancel the override statuses of all override function blocks in an SCS at once.

When UNOV is changed from FALSE to TRUE, all override statuses are forcibly canceled and a system alarm is generated.

It is possible to cancel all override statuses for a group of grouping override function blocks by inputting the same permit switch to all function blocks within the group and setting the permit switch to FALSE.

Management of the Override Enabled status

The SYS_OVR function block can manage the override enable statuses of all override function blocks in an SCS.

The override enable status refers to the condition where the SW input parameter value of a function block is TRUE.

The following types of management can be performed for override enable statuses of all override function blocks within the SCS.

TIP If there is a grouping override function block with a group number outside the specification range, the override permission signal operation for that function block is considered a part of the override enable status management.

- SWON
  SWON indicates whether or not there is a function block in the override enable status.
- NUMS
  NUMS indicates the number of override function blocks in the override enable status.

  For instance, if a common override permission signal is input to all the grouping override function blocks that comprise a group of 10 function blocks, setting the override permission signal to 1 makes NUMS to be 10.
- SWC, NOVS
  SWC is used to specify the maximum number of override function blocks that can be simultaneously placed in the override enable status. NOVS indicates whether or not the maximum number has been exceeded.

  If TRUE is set for SW of more override function blocks than the number specified by SWC, a system alarm is generated. However, it is possible to place override function blocks in the override enable status even after the maximum number has been exceeded and the system alarm has been generated.

In the case of grouping override function blocks, when a common permission signal is input to all the function blocks within the group, the number of all function blocks that belong to that group will be counted by SWC if the override permission signal is set to 1.

- CKTS, TUPS
  CKTS is used to specify the maximum duration of the status where at least one override function block in the override enable status exists. TUPS indicates whether or not the status has been continuing longer than the maximum duration.

  If the status continues longer than the duration specified by CKTS, a system alarm is generated.

Management of the override status

The SYS_OVR function block can manage the override statuses of all override function blocks in an SCS.

The override status refers to the condition where MV is set to 1 from an HIS by calling the faceplate that corresponds to the tag name assigned to the function block, and the override output value specified in VAL is being output from OUT of the function block.

- OVR
  OVR indicates whether or not there is an override function block in the override status.
- NUMO
  NUMO indicates the number of override function blocks in the override status.

  For instance, when there are two groups (A and B) of grouping override function blocks, if a function block in A is placed in the override status and a function block in B is also placed in the override state simultaneously, NUMO becomes 2.
- OVRC, NOVO
  OVRC is used to specify the maximum number of override function blocks that can be placed in the override status simultaneously. NOVO indicates whether or not the maximum number has been exceeded.

  If more function blocks than the number specified by OVRC are placed in the override status, a system alarm is generated. However, it is possible to override even after the maximum number has been exceeded and the system alarm has been generated.

  For instance, when grouping override function blocks are used and OVRC is set to 2, if the override operation is performed for the third group, a system alarm is generated.
- CKTO, TUPO
  CKTO is used to specify the maximum duration of the status where at least one override function block in the override status exists. TUPO indicates whether or not the status has been continuing longer than the maximum duration.

  If the status continues longer than the duration specified by CKTO, a system alarm is generated.

B4.6 Permission for override by password FB

It is possible to use the password function block to set a BOOL variable of an application logic to TRUE or FALSE from the faceplate of an HIS with password verification.

Operation to allow override

In order to authenticate the override operations on override function blocks, a password block can be used instead of using a hardware key switch. The permission can be granted or denied by authenticating the password.

How to utilize the password function block for authenticating the override operations will be explained below.

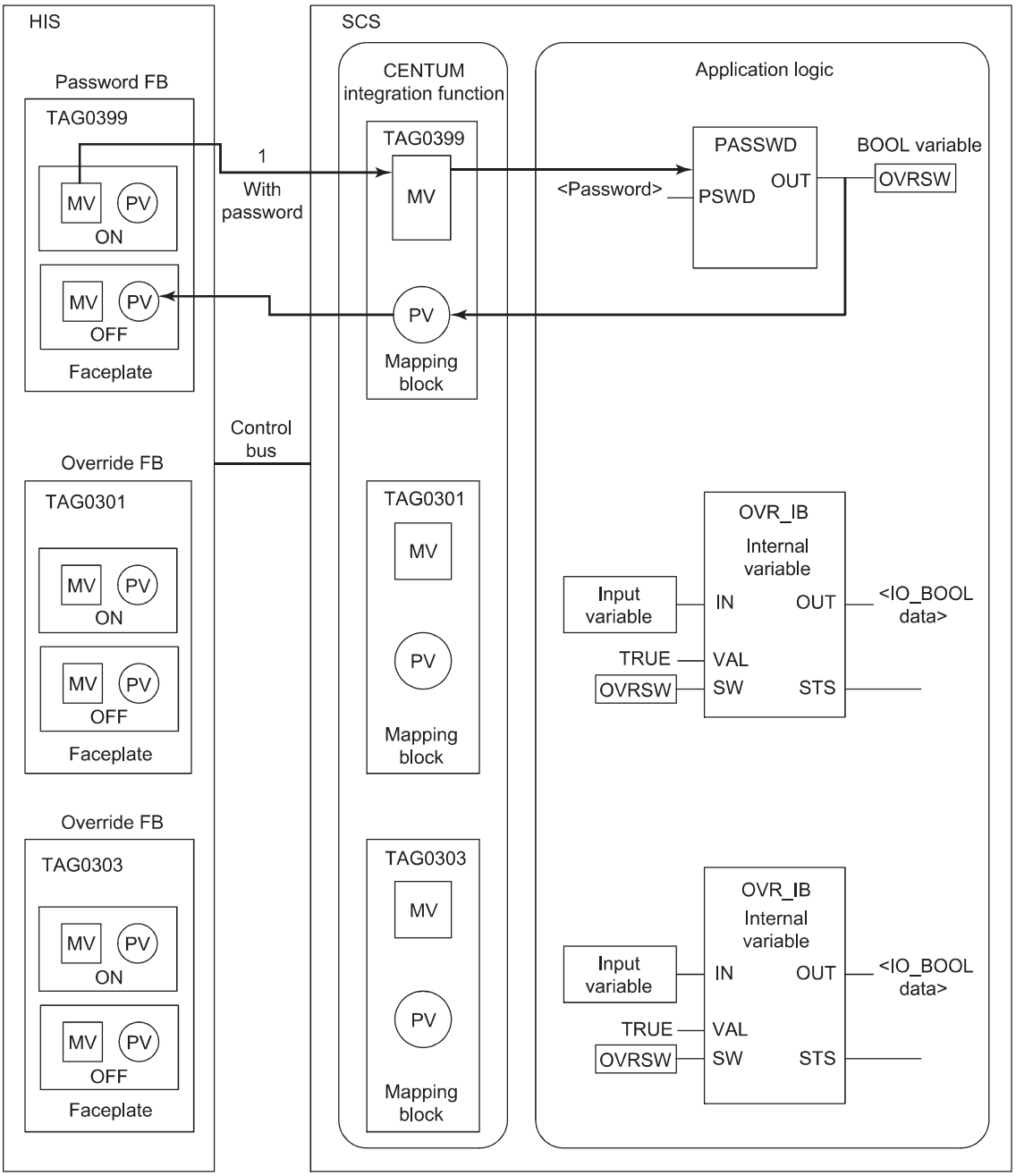
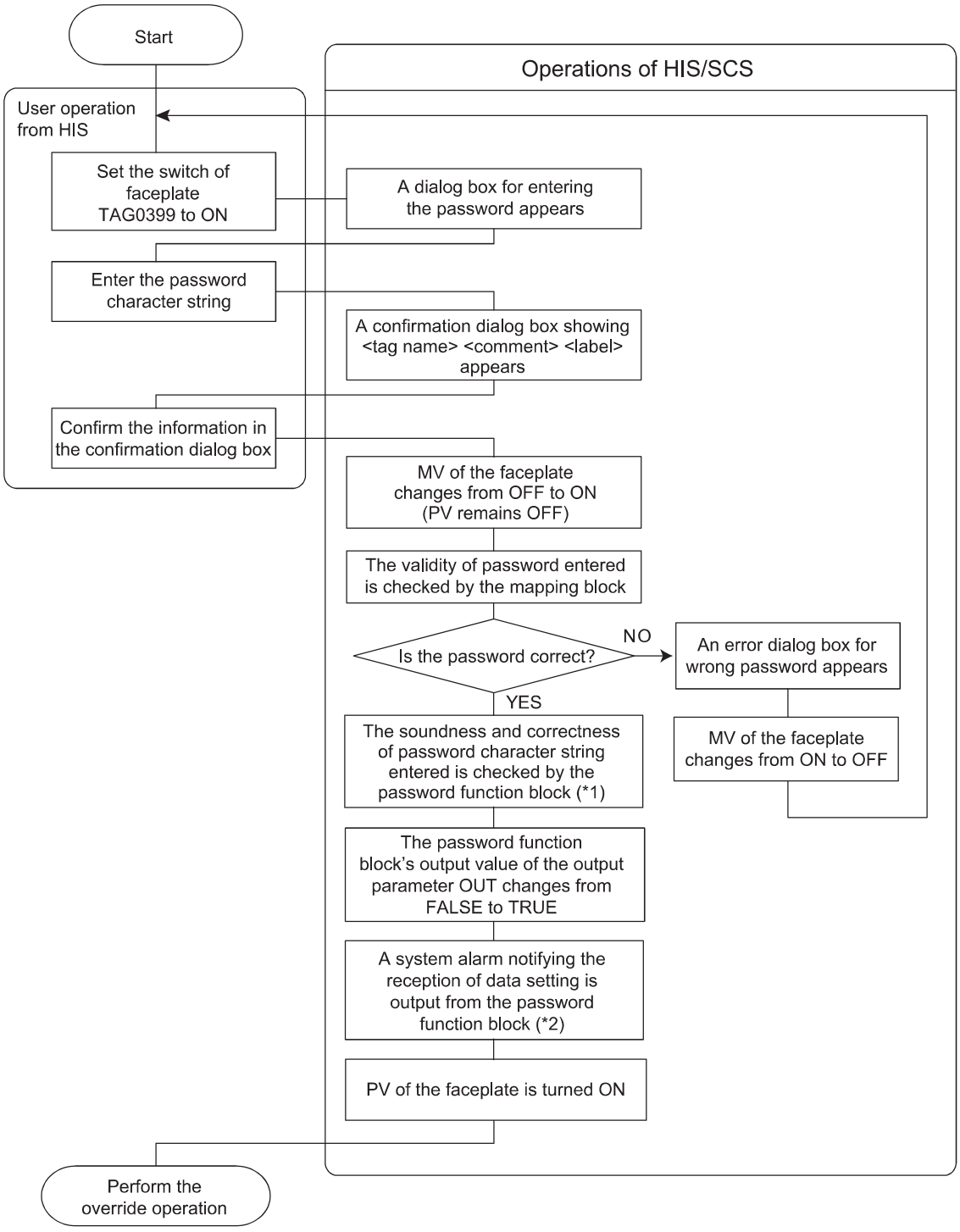


Figure B4.6-1 Switching override permission status by password (example)

The operation procedure of setting data with password verification in Figure, "Switching override permission status by password (example)" is shown below.

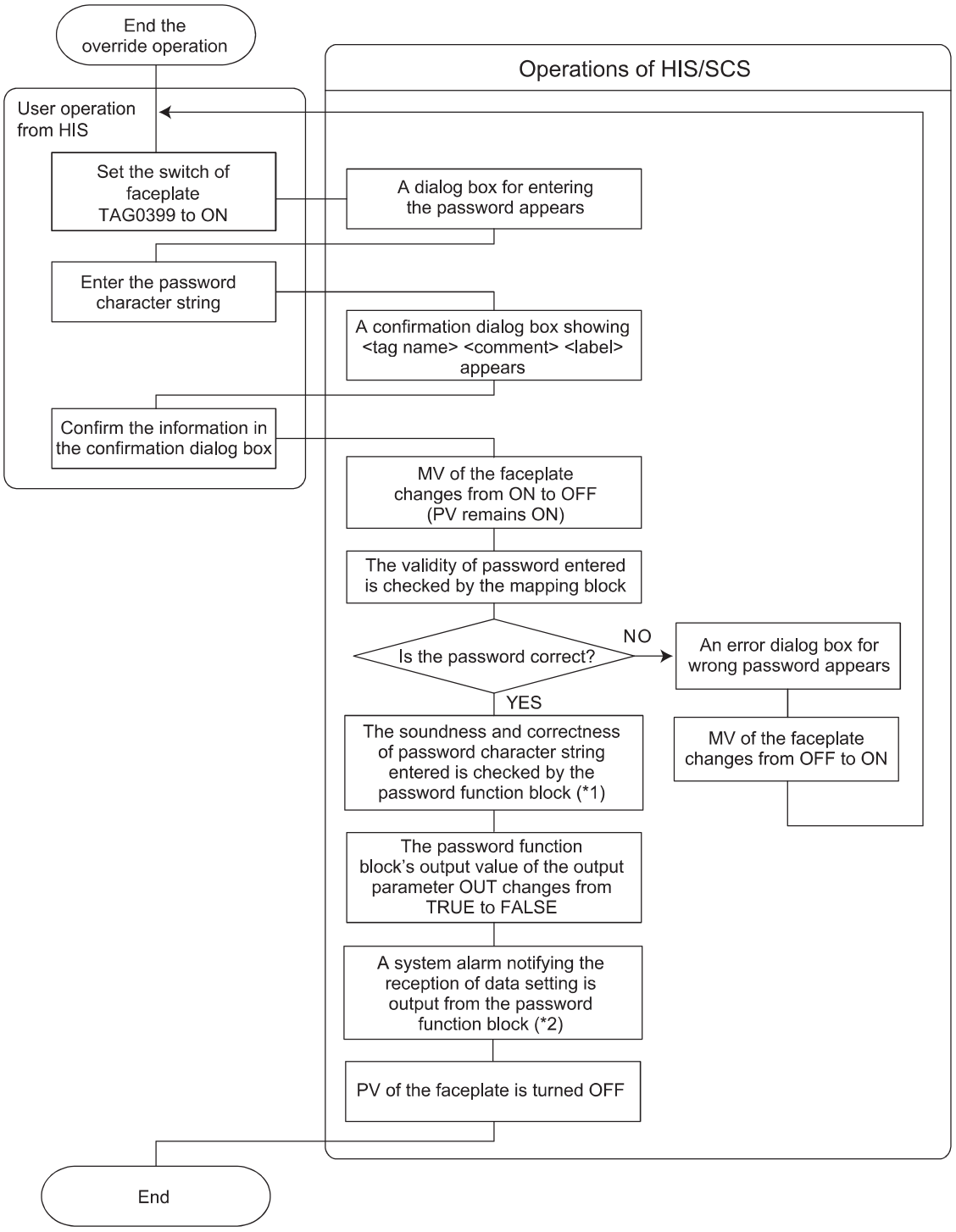
The default value of the output of the password function block is FALSE. The default status of the faceplate is OFF for both MV and PV.



*1: If there are any problems during checks by the password function block, the password function block outputs a system alarm that includes a tag name and aborts the processing.
*2: System alarm messages include the password function block instance name and tag name.

Figure B4.6-2 Permitting override operation by password function block

When override operation is complete, operation of the override function block is prohibited in the following manner.



*1: If there are any problems during checks by the password function block, the password function block outputs a system alarm that includes a tag name and aborts the processing.
*2: System alarm messages include the password function block instance name and tag name.

Figure B4.6-3 Prohibiting override operation with password function block

Management of password function block

The status of the PASSWD function block can be managed by a SYS_PSWD system function block. The SYS_PSWD function block has the following functions.

- The PASSWD function block is able to forcibly return the output from output parameter OUT of all PASSWD function blocks within an SCS to FALSE. A system alarm is generated when the SYS_PSWD function block is used for this purpose.
- The SYS_PSWD function block displays whether or not there are any PASSWD function blocks that output TRUE via output parameter OUT within an SCS. The number of such PASSWD function blocks can also be displayed.
- The SYS_PSWD function block generates a system alarm if the number of PASSWD function blocks outputting TRUE from output parameter OUT exceeds the specified maximum number. It is still possible to set more passwords even after the system alarm indicating that the maximum number is exceeded has been generated, however.
- The SYS_PSWD function block generates a system alarm if the status where there is one or more PASSWD function blocks outputting TRUE continues longer than the specified time.

SEE ALSO For more information about SYS_PSWD, refer to:

11.11, “SYS_PSWD (password function blocks management)” in POU Reference Manual (IM 32P03B20-01EN)

B4.7 Tag name interfaces and process alarms of password function blocks

In order to set values of a PASSWD function block from an HIS, it is necessary to define the tag name using the Tag Name Builder and associate it with a mapping block. S_PASSWD mapping blocks are associated with PASSWD function blocks.

Settings in the Tag Name Builder

Use the Tag name builder to make a specification for password ON alarms and answer-back error alarms.

- Password ON alarms
  Specify either [Yes] or [No].

  The default is [Yes].

SEE ALSO For more information about items defined in the tag name builder, refer to:

B7.1.5, “Defining tag names” on page B7-12

Data items of S_PASSWD

Among the data items of S_PASSWD, the data items unique to mapping blocks of S_PASSWD are explained here. All of these data items are displayed in the HIS tuning view with the exception of MODE. Note that data entry for these data items from an HIS is allowed only for MV.

SEE ALSO For more information about descriptions regarding MODE (Block mode), AFLS (Alarm flashing status), AF (Alarm detection), AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

“■ Data items common to mapping blocks/mapping elements” on page B3-7

MODE (block mode)

This data item indicates block mode.

The default value of MODE is O/S (AUT).

ALRM (alarm status)

This data item displays alarm status.

The default value of ALRM is NR.

PV (answerback input value)

This data item is associated with the OUT parameter of PASSWD. It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend.

- Range
  The range of PV is 0 or 1.
- Correspondence between changes of the parameter value of PASSWD and changes of PV
  If the input password character string is correct, TRUE is output to OUT of PASSWD and PV becomes 1.
- Default
  The default value of OUT (0) is reflected in the default value of PV.

MV (manipulated output value)

Manipulate MV from an HIS to enter a password. It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend.

- Range
  The range of MV is 0 or 1.
- Default
  The default value of MV is 0.

Process alarms

The mapping block of PASSWD FB can initiate a process alarm for Password ON. It is possible to specify whether or not to initiate this process alarms using the Tag Name Builder.

Password ON alarm

Password ON alarms can be used to notify an operator that the PASSWD function block is currently outputting TRUE. A mapping block generates a password ON alarm if the PASSWD function block outputs TRUE via output parameter OUT. The system recovers from the password ON alarm if 0 is set with password from the faceplate.

A password ON alarm (PWON) is generated under the following condition.

- PV = 1 (OUT of the PASSWD function block is TRUE)

The system recovers from a password ON under the following condition.

- PV = 0 (OUT of the PASSWD function block is FALSE)

B4.8 Application for override

This section shows an example of application for override, its creation method, operating procedure, difference in FB, and precautions.

Example of application for override

The following figure illustrates an example of application where override is executed.

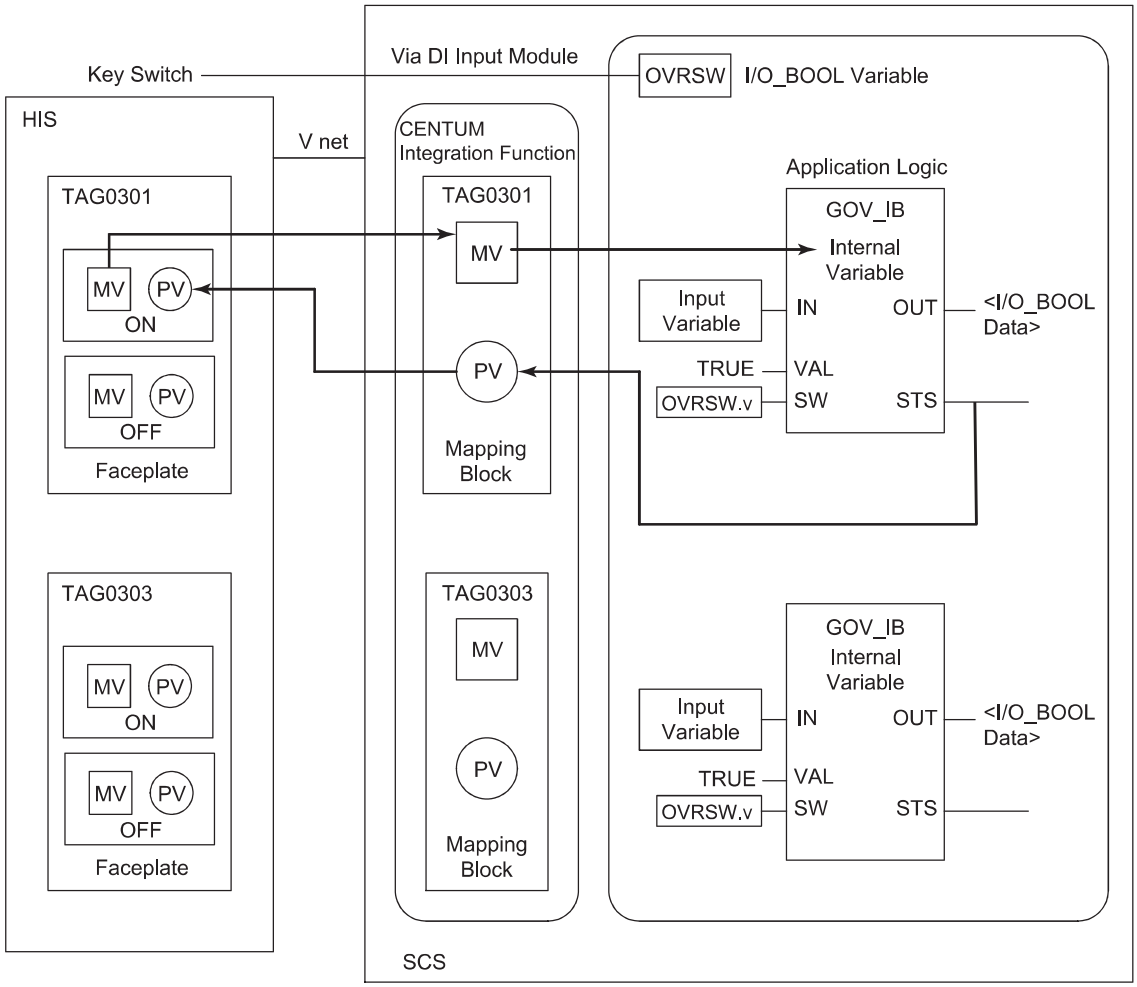


Figure B4.8-1 Override from HIS (Example of GOV_IB)

This describes the Override function with the GOV_IB function block.

Override from HIS is executed with the override function block (e.g. OVR_IB). Different Override FBs are available corresponding to the type of overridden variable. Mapping blocks (e.g. TAG0301) help override operation from a faceplate of HIS to the override FB.

Action of Override FB

- Without being overridden, data input from the IN parameter is output from the OUT parameter without any changes.
- When override is used, the override FB outputs data specified to the VAL input parameter, from the OUT parameter. This means the data is locked to the value which has already been defined to VAL.
- When override is cancelled, the override FB outputs the data input from IN again to OUT.
- To execute override, it is required that the override FB's SW parameter which enables override is TRUE and that override is operated from HIS.

- When user executes override from a faceplate of HIS while SW is TRUE, the Data Item MV of mapping block is set to 1 (override instruction). Then, the content of MV is reflected on the internal variable of override FB. The override FB checks the validity of the set data. When the test is passed, the override FB goes into the override status.
- A system alarm message is output if override is enabled for an FB while there are no override-enabled FBs. A system alarm message is also output if override is disabled for the last remaining override-enabled FB, resulting in no override-enabled FBs.
- When the override FB goes into the override status and when the status is cancelled, a diagnostic information message including the instance name and tag name of override FB is issued.

SEE ALSO For more information about override, refer to:

B4.3, “Overview of grouping override function block” on page B4-8

Create applications for override

To execute override, it is necessary to create application logic with the override FB.

1. Function blocks that meet the requirements of override FB or grouping override FB should be used.
2. Use the override function blocks, which correspond to the type of variables on which override will be executed.
3. Connect an input variable to the IN input parameter. Connect the variable on which override is executed to the OUT output parameter.
4. Define the overriding value to the VAL input parameter.
5. Use the SW input so that override cannot be executed without permission.
   Do not connect the TRUE value to the SW input.

Operational procedure of override

In this operational procedure, override is enabled/disabled by connecting a discrete input from a key switch with the SW input parameter of the override function blocks. Using the Password FB allows you to switch override through a password from HIS without the key switch.

1. The override function block goes into the ready status for overriding by turning the key switch to “Ready for override from HIS.”
   Confirm from HIS that a system alarm is output, which indicates override is enabled.
2. Switch the MV of a faceplate on HIS from which override is operated, to “ON.” When override becomes effective, the value of the VAL input parameter specified by the override function block is output from the OUT output parameter.
   - A system alarm which notices override is displayed. As instance name and tag name in the override function block are included in this system alarm, confirm they are appropriate.
   - PV of the faceplate reads back the output from the STS parameter in the override function block. Confirm that both MV and PV are “ON.”
3. Provide necessary maintenance while override is being performed.
4. Set MV to “OFF” from the faceplate after maintenance to cancel override. When override is canceled, the value from the IN input parameter is output from the OUT output parameter without any changes. The STS output parameter of GOV_IB changes from 1 to 0.
   - Confirm that a system alarm indicating override has been canceled on HIS is displayed. As instance name and tag name in the override function block are included in this system alarm, confirm they are appropriate.
   - Confirm that both MV and PV are “OFF” on the a faceplate.

5. Turn the key switch to the original position to disable override from HIS. Confirm that the system alarm indicating override is disabled.

Differences between Override FB and Grouping override FB

The differences between the override FB and the grouping override FB are listed. The override FB and the grouping override FB act differently when the override permission signal becomes OFF during override. Therefore, it is recommended not to mix the two types of override FBs. Moreover, between override FB and grouping override FB, the exclusive override cannot be executed.

Table B4.8-1 Differences between Override FB and Grouping override FB

Feature	Override FB	Grouping Override FB
Grouping function of grouping override FB	No	Yes
Action when override permission (SW) becomes OFF	Override continues	Override stops when permission signal changes from TRUE to FALSE.
Status display on mapping block	No	MAN: Override executable (operational from HIS) AUT: Override not executable (non operational from HIS)
MV of mapping block when override is automatically released (*1)	MV=1 (Answerback error)	MV=0 (Auto reset)
Manipulating the MV of mapping block when permission (SW) is OFF	Can be changed to MV=1, but it indicates answerback error.	Since the block mode is in AUT, an operation error message will be displayed. MV cannot be changed.
Overridden variables	BOOL(OVR_B) IO_BOOL(OVR_IB) DINT(OVR_I) REAL(OVR_R) IO_REAL(OVR_IR)	BOOL(GOV_B) IO_BOOL(GOV_IB)

*1: Automatic release of override
Under the following circumstances, the override will be automatically released.
- SYS_OVR sent a forcibly release override signal(to override FB or grouping override FB)
- Permission signal changes from TRUE to FALSE (grouping override FB)
- Group numbers are changed (grouping override FB)

In the grouping function of override FB with grouping function, override groups can be created by assigning group numbers to grouping override FBs. When the override permission signal changes to TRUE, the override FB becomes overridable. If multiple grouping override FBs have the identical group number, only one of the grouping override FBs can be overridden at a time. In other words, other grouping override FBs in the same group cannot be overridden until the currently overridden FB is released. Grouping management is not applied to the override FBs whose group number is 0.

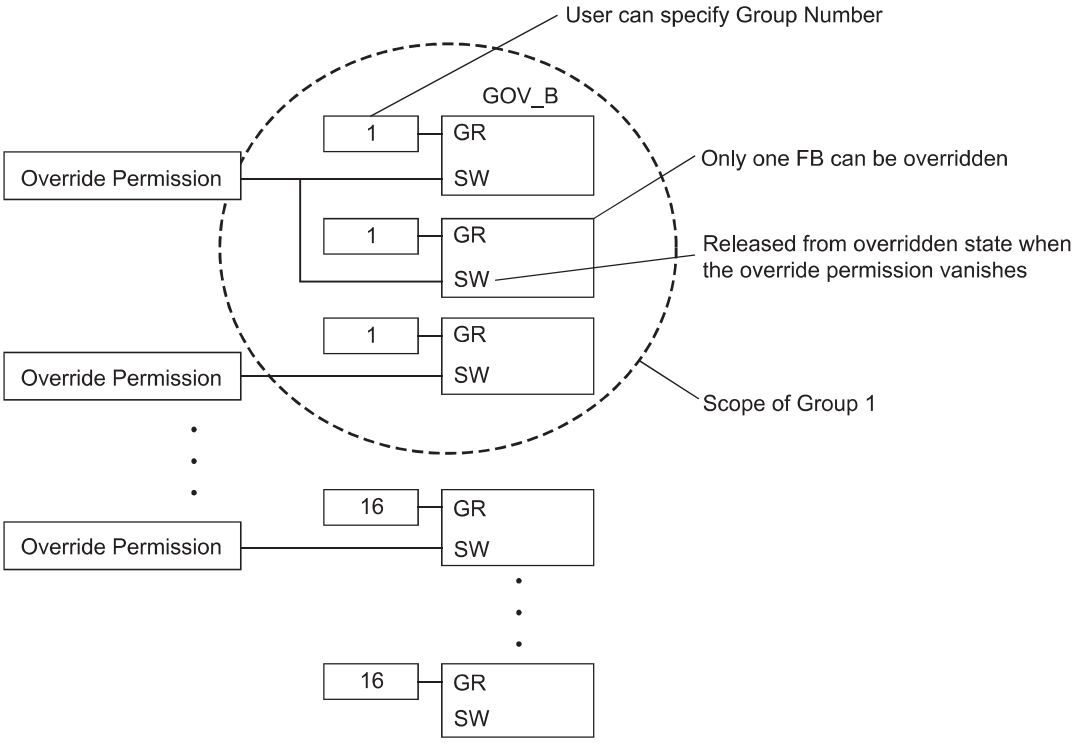


Figure B4.8-2 Grouping override FB overview

SEE ALSO For more information about detailed procedures for operating the override, refer to:

B4., “Override operation from HIS” on page B4-1

Precautions for override

- The length of variable name displayed as a system alarm is 80 characters at maximum. Set a variable name length not to exceed the maximum so that the variable name can be identified when forcing and override are enabled/disabled.
- Do not execute online change download while executing override from HIS.
- When using the Password FB, set different passwords for each FB.
- If a permission signal SW is from a DI, and the permission signal becomes FALSE due to a DI related device fault, the override will be automatically released.
- When group number is mistakenly specified, the system cannot find this error. Therefore, during the logic test, if the group numbers have been properly specified or not must be carefully inspected.
- During override, do not use online change to change the group number and run online change downloading. If you do, override is automatically deactivated. If you assign a variable to a group number and change the variable value, override is automatically deactivated.

B5. Manipulation of manual operation function blocks from HIS

Manual operation function blocks are used to output values manipulated by an operator via an HIS to the application logic. Note that it is also possible to prohibit manipulation from an HIS and set output values of function blocks with the application logic.

There are the following four types of manual operation function blocks.

- MOB_11 (BOOL-type data manual operation function block with two-position answer-back)
- MOB_21 (BOOL-type data manual operation function block with three-position answer-back)
- MOB_RS (auto-reset BOOL-type data manual operation)
- MOA (analog-type data manual operation)

SEE ALSO

For more information about MOB_11, refer to:

- B5.1, “HIS interfaces of MOB_11 and MOB_21 (BOOL-type data manual operation function block with answerback)” on page B5-3
- 7.4, “MOB_11 (BOOL-type data manual operation function block with two-position answerback)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about MOB_21, refer to:

- B5.1, “HIS interfaces of MOB_11 and MOB_21 (BOOL-type data manual operation function block with answerback)” on page B5-3
- 7.5, “MOB_21 (BOOL-type data manual operation function block with three-position answerback)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about MOB_RS, refer to:

- B5.2, “HIS interfaces of MOB_RS (auto-reset BOOL-type data manual operation)” on page B5-21
- 7.6, “MOB_RS (auto-reset BOOL-type data manual operation)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about MOA, refer to:

- B5.3, “HIS interfaces of MOA (analog-type data manual operation)” on page B5-29
- 7.7, “MOA (analog-type data manual operation)” in POU Reference Manual (IM 32P03B20-01EN)

Overview of manual operation from HIS

For each of the four types of manual operation function blocks, parameter values of function blocks can be changed by manual operations by an operator from an HIS. It is also possible to specify whether or not to permit such manual operations with the application logic. If manual operations are prohibited, output values can be changed from the application logic. Some manual operation function blocks can also receive shutdown signals from the application logic, forcing them to output shutdown signals.

All manual operation function blocks have functions to read back the results of manual operations, so that the operator is able to check via HIS instrument faceplate that operation instructions are correctly received. These function blocks are safety function blocks. There is no need for users to take safety measures as in the case of external communication function blocks.

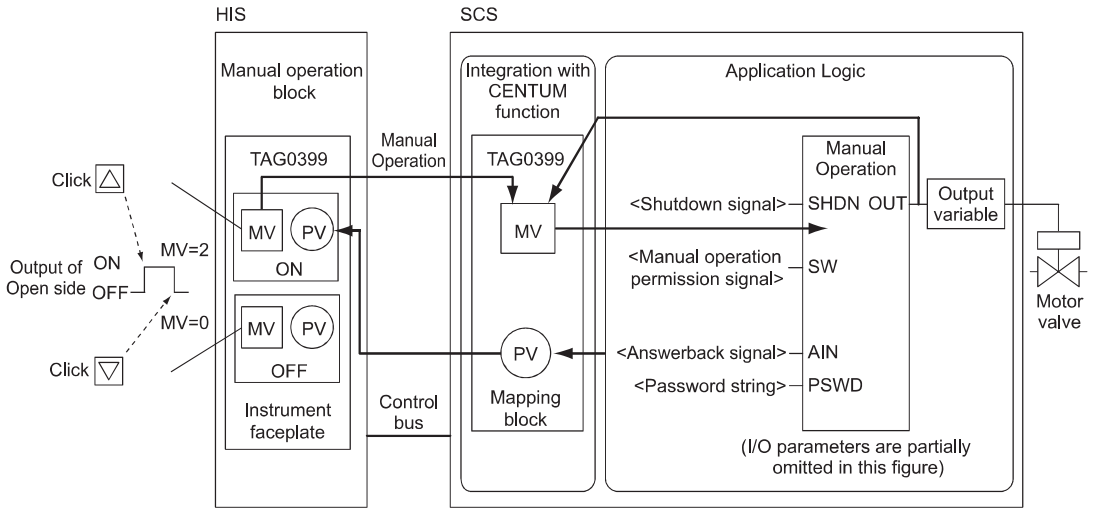


Figure B5-1 Overview of manual operation from HIS

B5.1 HIS interfaces of MOB_11 and MOB_21 (BOOL-type data manual operation function block with answerback)

BOOL-type data manual operation function blocks with answerback have 1 or 2 DI inputs, which are typically used to connect the answerback input from a limit switch, and 1 DO output, which is typically connected to a valve. In addition to manipulation of the output value from an HIS, it is possible to set the output value from the application logic.

BOOL-type data manual operation function blocks with answerback also have a parameter for receiving shutdown events; they can output shutdown logic signals with the highest priority at occurrence of shutdown events.

This section explains the following functions of MOB_11 and MOB_21.

- Manual Operation Permission Function
- Password at Manual Operations
- Output Enable Status Display Function
- Answerback check
- Monitoring IOP and OOP

SEE ALSO For more information about description of the MOB_11 parameters, refer to:

7.4, “MOB_11 (BOOL-type data manual operation function block with two-position answerback)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about description of the MOB_21 parameters, refer to:

7.5, “MOB_21 (BOOL-type data manual operation function block with three-position answerback)” in POU Reference Manual (IM 32P03B20-01EN)

Types of BOOL-type data manual operation function blocks with answerback

There are two types of BOOL-type data manual operation function blocks with answerback, which are distinguished by the number of answerback inputs.

- MOB_11 (BOOL-type Data manual operation function block with two-position answerback)
  This type corresponds to SIO-11 function block of FCS and receives answerback input from either one of the limit switches, open or close.
- MOB_21 (BOOL-type data manual operation function block with three-position answerback)
  This type is also corresponds to SIO-21 function block of FCS and receives answerback input from both limit switches, open and close.

SEE ALSO For more information about FCS switch instruments, refer to:

- 2.4, "Switch Instrument Block and Enhanced Switch Instrument Block" in the Function Blocks Reference Vol.2 (IM 33J15A31-01EN)
- 2.4, "Switch Instrument Block and Enhanced Switch Instrument Block" in the Function Blocks Reference Vol.2 (IM 33K03E23-50E)

Example of configuration of MOB_11 and MOB_21

The figure below shows a usage example of MOB_11 in a CENTUM integration structure.

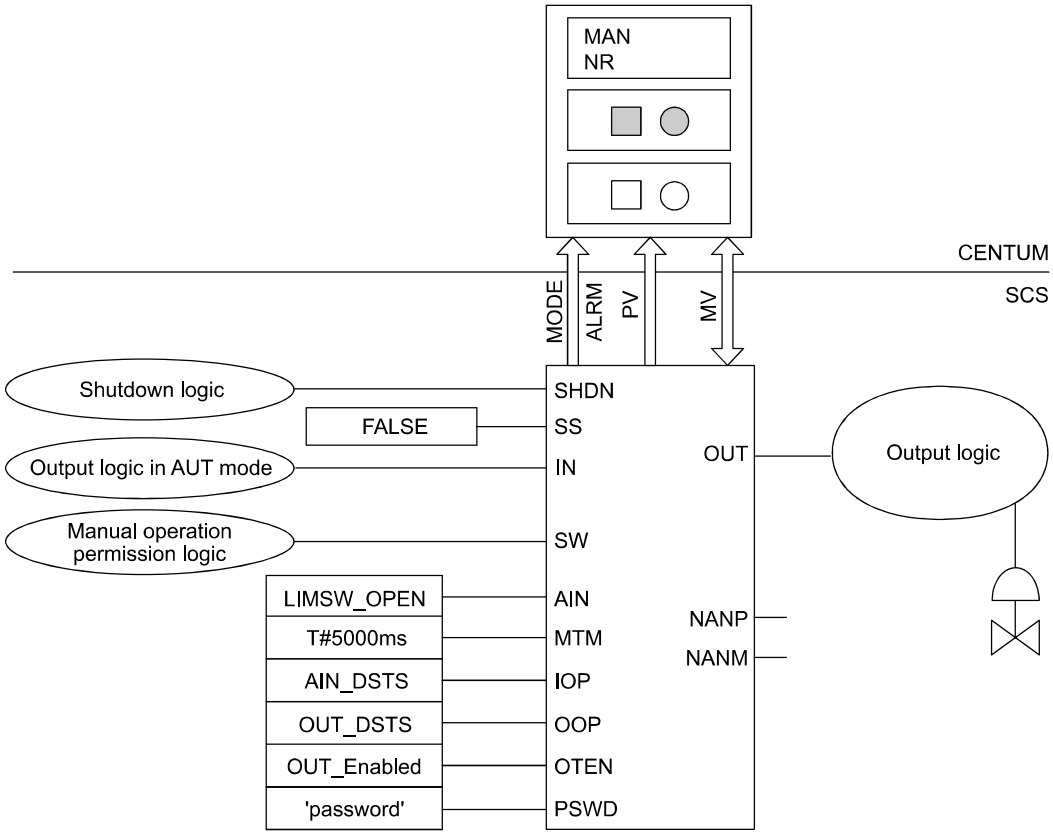


Figure B5.1-1 Usage example of BOOL-type data manual operation function block with two-position answerback

The figure below shows a usage example of MOB_21 in a CENTUM integration structure.

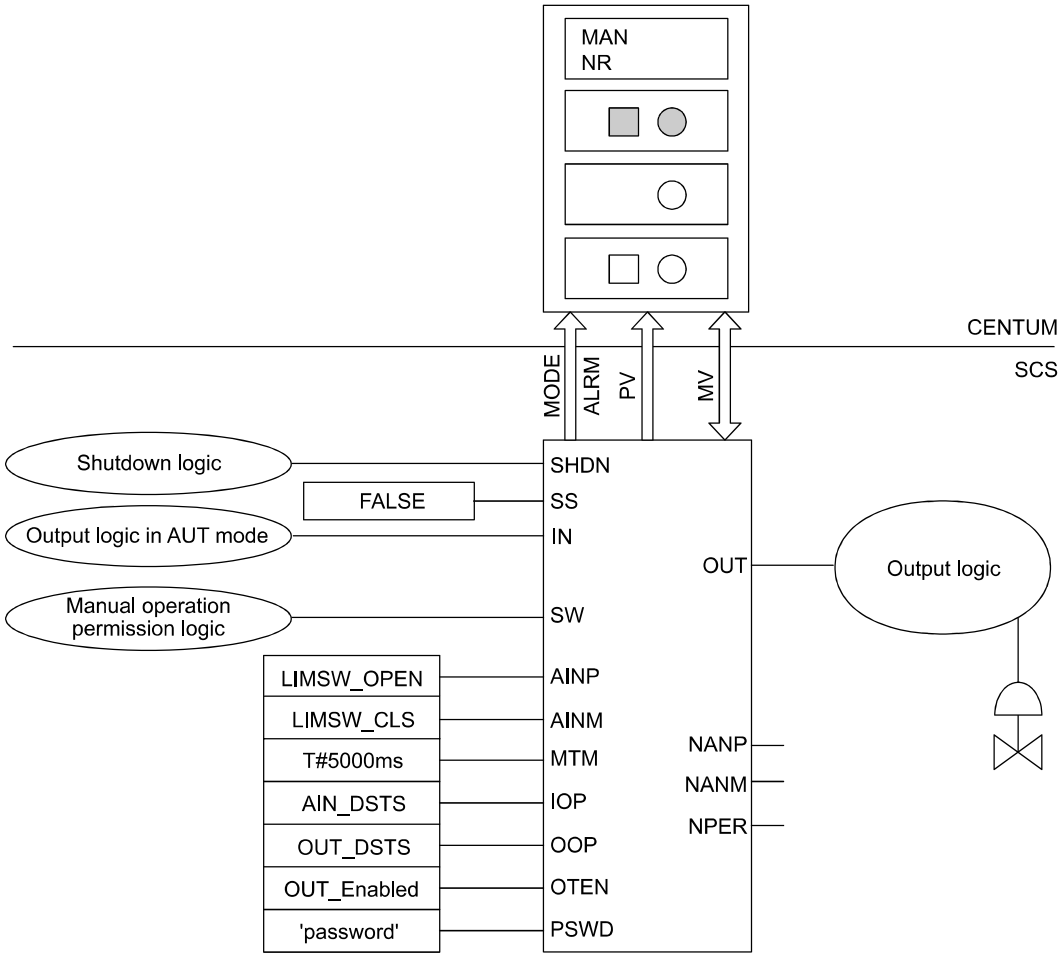


Figure B5.1-2 Usage example of BOOL-type data manual operation function block with three-position answerback

The associated parameter values of SCS function blocks are sent to indicate the block mode (MODE), process alarms (ALRM) and answerback input values (PV) on the CENTUM side via mapping blocks. The value of OUT is displayed as MV on the HIS instrument faceplate and operations on MV from the HIS are sent to OUT of the SCS in the manual mode (MAN).

Overview of processing BOOL-type data manual operation function block with answerback

The figure below shows an overview of the processing of BOOL-type data manual operation function blocks with answerback in SCS and data flow.

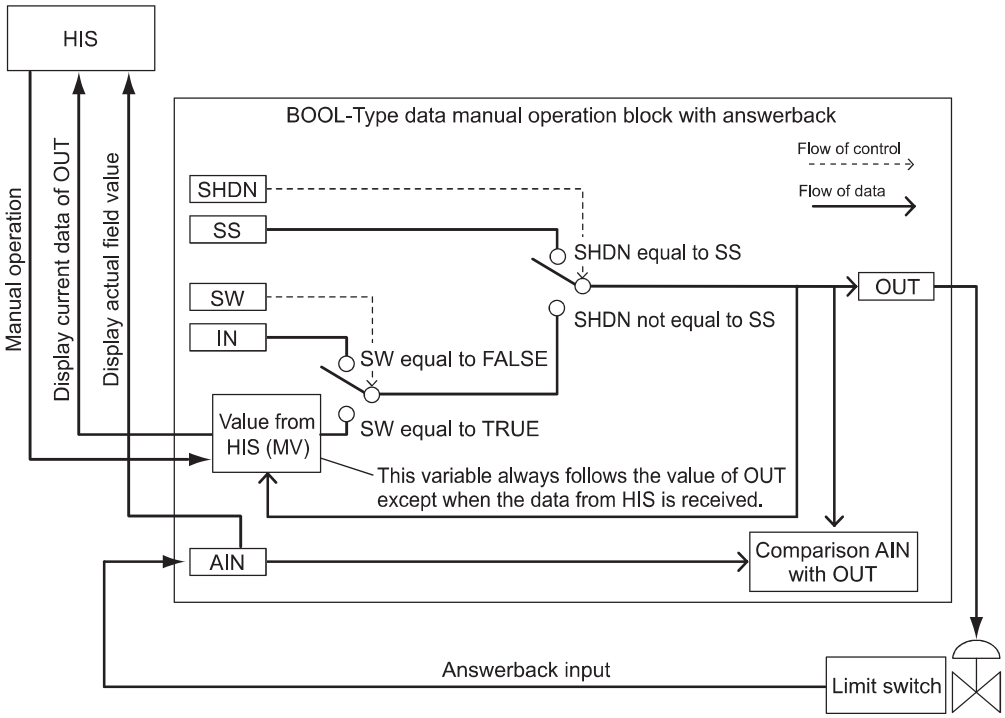


Figure B5.1-3 Flow of control and data (example of MOB_11)

Shutdown processing

If the input value of SHDN (shutdown signal) matches the safe state specified by the input value of SS, the safe state is output from OUT. At this point, all data settings from input parameters other than SHDN and SS as well as an HIS are ignored.

Prohibition of manual operations

If the input value of SHDN does not match the safe state specified by the input value of SS and the manual operation permit switch SW is set to FALSE (manual operations prohibited), data input to IN is output to OUT as is. If an operator attempts to perform manual operations from an HIS when the input to SW is FALSE, the attempt will fail. IN can be used to change the output value of OUT from the application logic when no shutdown instruction is input to SHDN (i.e., the system is in a safe state).

For example, after the value of SHDN becomes FALSE in the DTS logic and the valve closes, FALSE should be input to SW and the IN value kept as FALSE. In this way, it is possible to prevent the valve from opening immediately when the value of SHDN becomes TRUE as the shutdown conditions are removed.

Permission of manual operations

If the input value of SHDN does not match the safe state specified by the input value of SS and SW is set to TRUE (manual operations permitted), the result of manual operations carried out by an operator from an HIS is output from OUT. Note that password entry is required to perform manual operations. The password is checked within a function block. If the passwords do not match, the value of OUT does not change. The status where manual operations are permitted can be used when it is desired to open/close a valve by a user operation without issuing a shutdown instruction from SHDN (i.e., the system is in a safe state).

Answerback check

Regardless of whether the input to SW is TRUE or FALSE, it is checked whether the OUT value and answerback input value match as an answerback input check.

For example, by connecting OUT to the output signal to a valve and the answerback input value (AIN for MOB_11) to the limit switch of the valve, it is possible to confirm that the output

result of OUT is correctly transmitted to the process. It is also possible to bypass the answerback input value check for a fixed period of time only after changing the value of OUT, taking into consideration the time that the valve requires to change from full open to full close.

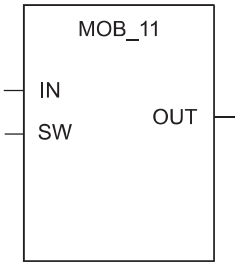
B5.1.1 Manual operation permission function

With MOB_11 and MOB_21, it is possible to switch between whether or not manual operations from an HIS are permitted. If MV is manipulated from an HIS when manual operations are permitted, the output from OUT of function blocks is set accordingly. Prohibition of manual operations can be used to prevent operations from an HIS at occurrence of demands other than shutdown to output a value determined by the application logic.

Switching between whether or not manual operations are permitted

In MOB_11 and MOB_21, it is possible to specify whether or not manual operations are permitted. When shutdown events occur, however, the shutdown processing takes the priority, and outputs set by manual operations as explained in this section and outputs from the application logic connected to IN become invalid.

The following parameters are related to specification of whether or not manual operations are permitted in MOB_11 and MOB_21.



Note: Other parameters are omitted.

Figure B5.1.1-1 Parameters related to manual operations

Overview of manual operations

- SW is TRUE: The value set by a manual operation from an HIS to this FB is output from OUT.
- SW is FALSE: The value input to IN is output from OUT.

Details of manual operations

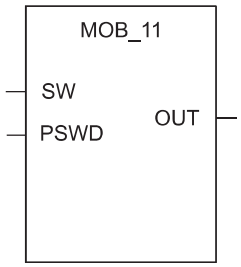
- If the input value of SW is TRUE, manual operations from an HIS are permitted. This status is called manual mode and MAN is displayed for the block mode in HIS instrument faceplate. The value of OUT changes according to the changes of MV which is manipulated from an HIS (for example, from a instrument faceplate). The value of IN is not used.
- If the input value of SW is FALSE, manual operations from an HIS are not allowed. The value determined by the application logic and input to IN of a function block is output from OUT. If the value of OUT changes due to a change in the input to IN, the associated MV value on the CENTUM side also changes accordingly. This status is called automatic mode and AUT is displayed for the block mode in HIS instrument faceplate.

B5.1.2 Password at manual operations

It is possible to prompt users to enter passwords for the purpose of limiting the member of users that are able to manipulate function blocks via manual operations from an HIS.

■ Password processing

The following parameters are related to password entry when manual operations are permitted.



Note: Other parameters are omitted.

Figure B5.1.2-1 Parameters related to password entry when manual operations are permitted

● Overview

- Set a password in PSWD when you create POU.
- If the input to SW is TRUE, manual operations from an HIS are permitted and entry of a password is required when an operator enters a value for MV. Manipulations of MV are permitted only if the set password and the input password match.

● Setting password character string

A password for allowing MV manipulations from an HIS should be set in PSWD in advance. Set PSWD as follows:

- Specify a password character string as a character constant.
- A character string of up to 16 single-byte alphanumeric characters can be set. If you specify a character string exceeding 16 characters, only the first 16 characters are set as the password character string and the remaining part is ignored.
- It is recommended to specify a password character string for each instance of the function blocks that require passwords (PASSWD, MOB_21, MOB_11 and MOA) and be sure each password is unique within a system.
- If it is not necessary to restrict MV manipulations by password entry, set an empty character string for PSWD. You can specify from the SCS Constants Builder whether to skip the display of the Password Input dialog box on HIS when an empty string constant is set in PSWD of the function block.

SEE ALSO For more information about "● specification to skip the Password Input dialog box" in "■ Settings with the Communication Tab" in C1.2.6, "SCS Constants Builder" in Engineering Guide Vol. 1 (IM 32P01C10-01EN), refer to:

"● Skip password dialog box for manual operation FB" in "■ Settings with the Communication Tab" in C1.2.6, "SCS Constants Builder" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

● Operation in HIS

If the input to SW is TRUE, i.e., the system is in the manual mode (MAN), a user is allowed to perform manual operations from an HIS. After inputting MV, the user is required to enter a password.

The entered password is checked within the SCS function block. If the password is incorrect, a warning message for the illegal operation will be displayed and the MV will be unchanged.

TIP

Even if you set an empty string constant in the PSWD of the function block, if you do not specify that display of the Password Input dialog box should be skipped in SCS Constants Builder, the Password Input dialog box appears on HIS. In this case, just press the Enter key.

Regardless of whether the Password Input dialog box is displayed or not, the reconfirmation dialog box is displayed.

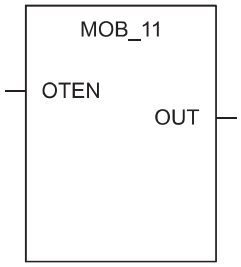
If a communication error with an HIS occurs during manual operations, OUT retains the current value.

B5.1.3 The Output Enable status display function

It is possible to display the output enable status in the instrument faceplate.

The Output Enable status display

The following parameters are related to output enable status display of MOB_11 and MOB_21.



Note: Other parameters are omitted.

Figure B5.1.3-1 Parameters related to the Output Enable status display

Overview of the Output Enable status display

If a signal indicating output enable status is input to OTEN, the output enable status is displayed in HIS instrument faceplate as block mode. If the value of OTEN is FALSE, IMAN is displayed as block mode.

Details of the Output Enable status display

Acquire the output status associated with the channel connected to OUT by using an SYS_OUTEN, SYS_N_OUTEN, or SYS_CH_OUTEN function block, and then connect it to OTEN.

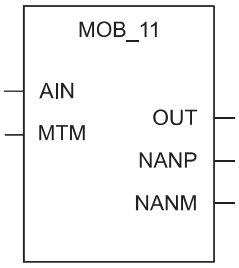
The value of OTEN does not affect output behaviors or answerback check operations of MOB_11 and MOB_21.

B5.1.4 Answerback check function

The operation of answerback check is different for MOB_11 and MOB_21.

Answerback check of MOB_11

The following parameters are related to answerback check of MOB_11.



Note: Other parameters are omitted.

Figure B5.1.4-1 Parameters related to answerback check of MOB_11

The table below explains the parameters.

Table B5.1.4-1 Explanation of parameters related to answerback check

IN/OUT	Arguments	Data type	Description
IN	AIN	BOOL	Answerback input value TRUE: Open status FALSE: Close status
	MTM	TIME	Answerback check mask time (Must be an integer multiple of the scan period)
OUT	OUT	BOOL	Open/close operation output value TRUE: Open instruction FALSE: Close instruction
	NANP	BOOL	Answerback status of the open side TRUE: Normal status FALSE: Abnormal status
	NANM	BOOL	Answerback status of the close side TRUE: Normal status FALSE: Abnormal status

Details of answerback processing for MOB_11

- Answerback check operation
  In an answerback check operation, the answerback input value (AIN) is compared with the OUT value to see if they are the same. The check result is output from NANP (answerback status of the open side) and NANM (answerback status of the close side) of a function block as well as notified to an HIS as a process alarm (ANS+ or ANS-) on the CENTUM side.

  Note that detection of answerback errors does not affect the output behavior of OUT.

- Answerback check mask
  In practice, it takes some time for operations to be completed after changing the value of OUT. For this reason, MOB_11 is equipped with MTM (answerback check mask time). By setting this parameter, it is possible to prevent errors from being notified for a fixed time specified by MTM after OUT is changed, even if the value of OUT and the answerback input values are different. After the value of OUT is changed, if the answerback input status is still abnormal after the time specified by MTM has elapsed, answerback errors on the open and close sides are output to NANP and NANM, respectively.

- Timing to perform answerback check processing
  The answerback check and answerback check mask processing can be performed either while a shutdown instruction is being output, application logic signals are being output because the input to SW is FALSE, or manual operations from an HIS are performed because the input to SW is TRUE.

Relationship between answerback check and parameters

The figure below shows how each parameter changes due to answerback check processing.

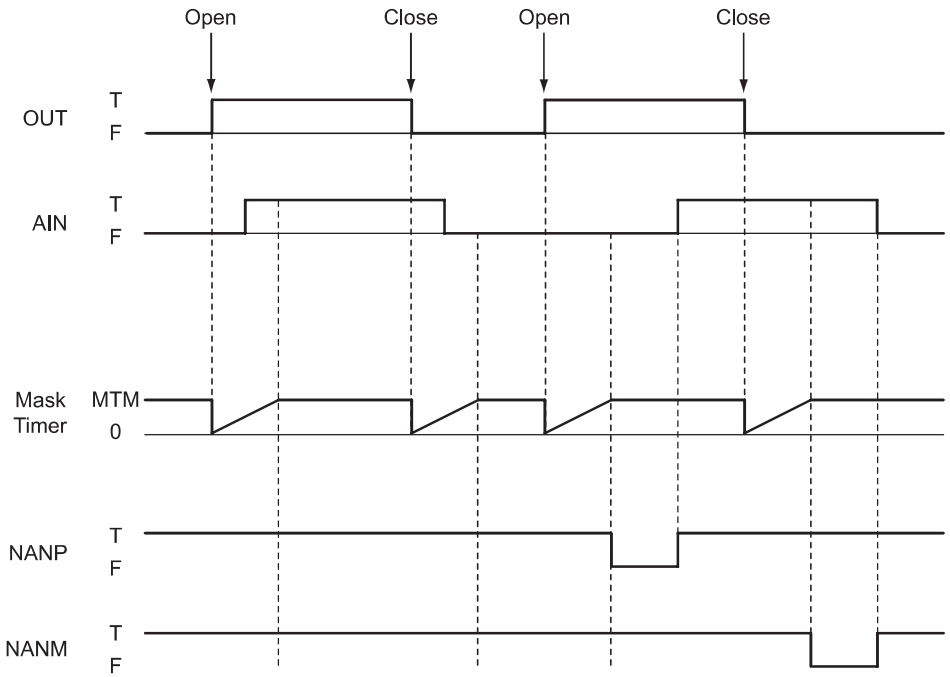
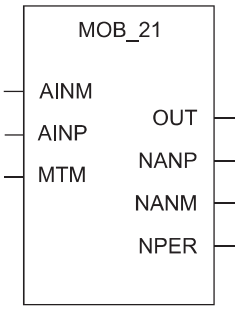


Figure B5.1.4-2 Detection of answerback errors in MOB_11

- When OUT changes, the mask timer for answerback check will be started. The mask for answerback check will continue until the time specified by MTM has elapsed. Within this masked time period, the answerback error will be ignored.
- Immediately after the value of OUT is changed, TRUE (normal) is set to NANP and NANM once. Process alarms of answerback errors are also canceled once.

Answerback check for MOB_21

The following parameters are related to answerback check of MOB_21.



Note: Other parameters are omitted.

Figure B5.1.4-3 Parameters related to answerback check of MOB_21

The table below explains the parameters.

Table B5.1.4-2 Explanation of parameters related to answerback check

IN/OUT	Arguments	Data type	Description
IN	AINP	BOOL	Answerback input value on the open side TRUE: Full open status FALSE: Not full-open status
	AINM	BOOL	Answerback input value on the close side TRUE: Full close status FALSE: Not full-close status
	MTM	TIME	Answerback check mask time (Must be an integer multiple of the scan period.)
OUT	OUT	BOOL	Open/close operation output value TRUE: Open instruction FALSE: Close instruction
	NANP	BOOL	Answerback status of the open side TRUE: Normal status FALSE: Abnormal status
	NANM	BOOL	Answerback status of the close side TRUE: Normal status FALSE: Abnormal status
	NPER	BOOL	Answerback pattern TRUE: Normal status FALSE: Abnormal status

Details of answerback processing of MOB_21

- Answerback check operation
  In the case of MOB_21, the input values of both AINP (answerback input value of the open side) and AINM (answerback input value of the close side) are compared with the value of OUT to see if they are the same in the answerback check processing. The check result is output from NANP (answerback status of the open side) and NANM (answerback status of the close side) of a function block as well as notified to an HIS as a process alarm (ANS+ or ANS-) on the CENTUM side.

  MOB_21 checks answerback pattern errors as well. Answerback pattern errors refer to an abnormal status where a full open signal and a full close signal are input at the same time. If a status where AINP (answerback input value of the open side) is TRUE (full open status) and AINM (answerback input value of the close side) is also TRUE (full close status) occurs,

  - FALSE (abnormal status) is output from NPER (answerback pattern)
  - and is also notified to the HIS as a process alarm (PERR) on the CENTUM side.

  Note that detection of answerback errors does not affect the output behavior of OUT.

- Answerback check mask
  In practice, it takes some time for operations to be completed after changing the value of OUT. For this reason, MOB_21 is equipped with MTM (answerback check mask time). By setting this parameter, it is possible to prevent errors from being notified for a fixed time specified by MTM after OUT is changed, even if the value of OUT and the answerback input values are different. After the value of OUT is changed, if the answerback input status is still abnormal after the time specified by MTM has elapsed, answerback errors on the open and close sides are output to NANP and NANM, respectively.

  Note that NPER (answerback pattern error) is detected independently of the answerback check mask time.

- Timing to perform answerback check processing
  The answerback check and answerback check mask processing can be performed either while

  - a shutdown instruction is being output,

- application logic signals are being output because the input to SW is FALSE,
- or manual operations from an HIS are performed because the input to SW is TRUE.

Relationship between answerback check and parameters

The figure below shows how each parameter changes due to answerback check processing.

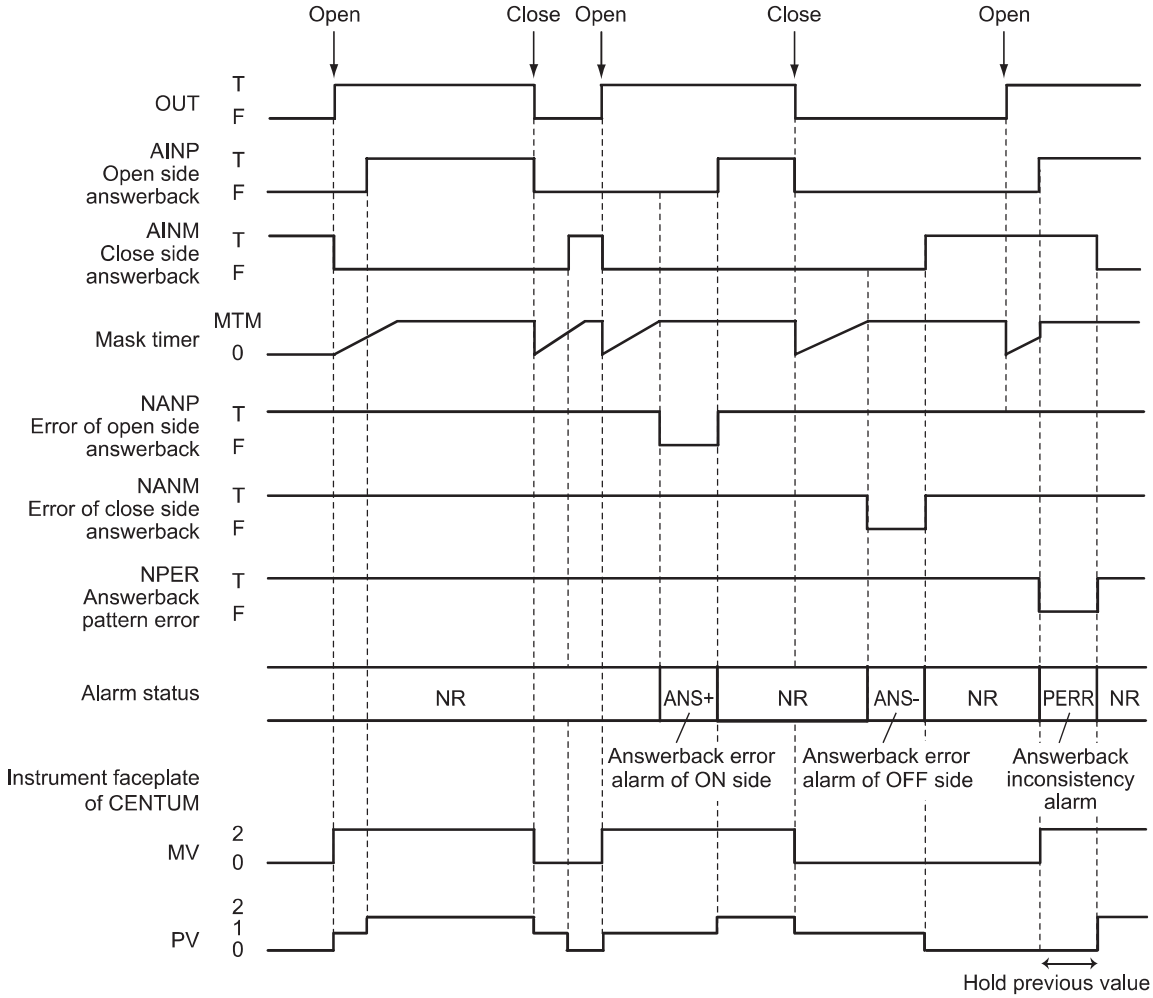


Figure B5.1.4-4 Detection of answerback errors in MOB_21

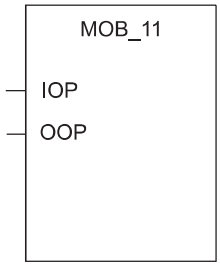
- When OUT changes, the mask timer for answerback check will be started. The mask for answerback check will continue until the time specified by MTM has elapsed. Within this masked time period, the answerback error will be ignored.
- Immediately after the value of OUT is changed, TRUE (normal) is set to NANP and NANM once. Process alarms of answerback errors are also canceled once.
- In the case of an answerback pattern error (NPER is FALSE), the answerback statuses on both the open and close sides (NANP and NANM) are retained.
- In detection of answerback pattern errors (NPER), answerback check mask is ignored. FALSE (abnormal) is thus output to NPER as soon as the conditions for pattern error are met (AINP = TRUE and AINM = TRUE).
- When the answerback check is masked and the answerback pattern error occurs, the answerback check mask will be disabled. If the answerback pattern error is recovered and the answerback check is performed, the results will be available in NANP and NANM.

B5.1.5 Monitoring IOP and OOP

IOP and OOP are functions that monitor the statuses of inputs and outputs and notify process alarms on the CENTUM side. Inputs to IOP and OOP do not affect output operations and answerback check operations of the function block.

Parameters related to IOP/OOP

Parameters related to IOP and OOP are the same for MOB_11 and MOB_21.



Note: Other parameters are omitted.

Figure B5.1.5-1 Parameters related to IOP and OOP

The table below explains the parameters.

Table B5.1.5-1 Explanation of parameters related to IOP/OOP

IN/OUT	Arguments	Data type	Description
IN	IOP	BOOL	Signal for monitoring input status TRUE: Normal status FALSE: Abnormal status
	OOP	BOOL	Signal for monitoring output status TRUE: Normal status FALSE: Abnormal status

Signal connection to IOP

- In the case of MOB_11, connect the data status of the answerback input (input variable connected to AIN) and similar signals to IOP.
- In the case of MOB_21, connect the logical product of the data statuses of the two answerback inputs (input variables connected to AINP and AINM) and similar signals to IOP.

Signal connection to OOP

Connect the data status of the output (output variable connected to OUT) and similar signals to OOP.

B5.1.6 Tag name interfaces and process alarms of MOB_11 and MOB_21

In order to manually operate BOOL-type data manual operation function blocks with answerback from an HIS, it is necessary to specify the tag names using the Tag Name Builder and associate them with mapping blocks. This allows them to be called via tag names and notification of process alarms.

The following mapping blocks are associated with BOOL-type data manual operation function blocks with answerback.

- Mapping blocks of MOB_11: S_MOB_11
- Mapping blocks of MOB_21: S_MOB_21

■ Settings in the Tag Name Builder

To perform manual operations from an HIS, make settings for the relevant instances of MOB_11 and MOB_21 in the Tag Name Builder. Specify whether or not to notify answerback error alarms according to the following procedure.

- Answer back Alarm (answerback error alarm)
  Specify either [Both], [ON], [OFF] or [No].

  The default is [Both].

  Specify [ON] to detect only ANS+ alarms (PV ≠ 2 when MV = 2) and [OFF] to detect only ANS- alarms (PV ≠ 0 when MV = 0).

■ Data items of S_MOB_11 and S_MOB_21

Among the data items of mapping blocks, the data items unique to S_MOB_11 and S_MOB_21 are explained here. All of these data items are displayed in the HIS tuning view.

SEE ALSO For more information about descriptions regarding MODE (Block mode), AFLS (Alarm flashing status), AF (Alarm detection), AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

● MODE (block mode)

This data item indicates block mode. The block mode cannot be changed into AUT or MAN from an HIS. The default value of MODE is O/S (AUT).

- Associating parameters of function blocks
  The SHDN (shutdown signal), SS (safe state specification), SW (manual operation permit/prohibit toggle switch) and OTEN (signal indicating output enable status) parameters of a function block are associated with MODE.
- Changes of block mode (AUT/MAN)
  The block mode becomes AUT if SHDN matches with SS (safe state specification). If they do not match, the block mode becomes MAN if TRUE is input to the function block parameter SW, and AUT if FALSE is input to SW.
- Changes of block mode (output enable status)
  The block mode IMAN is added to the block mode if OTEN is FALSE and IMAN is removed from the block mode if OTEN is TRUE.

● ALRM (alarm status)

This data item displays alarm status.

Data entry from an HIS is not allowed.

The default value of ALRM is NR.

SHDN (shutdown signal)

This data item displays signals used for shutdown logic. Data entry from an HIS is not allowed.

- Associating parameters of function blocks
  The SHDN parameter (shutdown signal) of a function block is associated with SHDN. The SHDN value of a function block is reflected in this data item.
- Range
  The range of SHDN is 0 or 1.
- Correspondence between changes of the parameter value of function blocks and changes of SHDN
  Changes of the SHDN (shutdown signal) value of a function block match with changes of SHDN.

  If the value of SHDN matches with SS (safe state specification), the value of SHDN is output as a shutdown signal from the OUT parameter (corresponding to the data item MV) of a function block.

SS (safe state specification)

This data item displays the safe state (value output as a shutdown signal) of a shutdown signal. Data entry from an HIS is not allowed.

- Associating parameters of function blocks
  The SS parameter (safe state specification) of a function block is associated with SS. The SS value of a function block is reflected in this data item.
- Range
  The range of SS is 0 or 1.

INV (logic input value)

This data item is associated with the value specified to be output under conditions where the shutdown logic is not effective and operations from an HIS are prohibited. Data entry from an HIS is not allowed.

- Associating parameters of function blocks
  The IN parameter (specified output value when manual operations are prohibited) of a function block is associated with INV. The default value of IN of MOA is reflected in this data item.
- Range
  The range of INV is 0 or 2.
- Correspondence between changes of the parameter value of function blocks and changes of INV
  INV is 2 if the IN parameter of a function block is TRUE and 0 if IN is FALSE.

SW (switch)

This data item displays the status of the manual operation permit/prohibit toggle switch of the FB. Data entry from an HIS is not allowed.

The value of the data item SW is determined as follows according to the value of the FB parameter and the SCS Constants Builder specification.

Table B5.1.6-1 Value set for data item SW

SW of FB	PSWD of FB	SCS Constants Builder specification	Data item SW
FALSE	- (*1)	- (*1)	0

Continues on the next page

Table B5.1.6-1 Value set for data item SW (Table continued)

SW of FB	PSWD of FB	SCS Constants Builder specification	Data item SW
TRUE	Other than an empty string constant	- (*1)	1
	Empty string constant	Do not skip the Password Input dialog box.	1
		Skip the Password Input dialog box.	2

*1: It does not affect the value of data item SW

PV (answerback input value)

This data item displays answerback input signals of a function block. Data entry from an HIS is not allowed. It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend.

- Associating parameters of function blocks
  For MOB_11, the AIN parameter (answerback input value), and for MOB_21, the combination of values of AINP (answerback input value of the open side) and AINM (answerback input value of the close side) is associated with PV.
- Range
  The range of PV is 0, 1 or 2.
- Correspondence between changes of the parameter value of MOB_11 and changes of PV
  PV=2 if AIN (answerback input value) of MOB_11 is TRUE (open) and PV=0 if FALSE (close).
- Correspondence between changes of the parameter value of MOB_21 and changes of PV
  In MOB_21, the value of PV changes according to the combination of values of AINP (answerback input value of the open side) and AINM (answerback input value of the close side).
  - PV=2 if AINP=TRUE (full open) and AINM=FALSE (not full-close)
  - PV=1 if AINP=FALSE (not full-open) and AINM=FALSE (not full-close)
  - PV=0 if AINP= FALSE (not full-open) and AINM=TRUE (full close)
  - PV retains the previous value if AINP=TRUE (full open) and AINM=TRUE (full close)
- Default
  The default value (0) of the associated parameter of the function block is reflected in the default value of PV.

MV (manipulated output value)

This data item is associated with the operation output value of a function block. Its value can be changed if manual operations from an HIS are permitted (MODE=MAN). It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend.

- Associating parameters of function blocks
  The OUT parameter (open/close operation output value) of function blocks is associated with MV.
- Range
  The range of MV is 0 or 2.
- Correspondence between changes of the parameter value of function blocks and changes of MV

The value of OUT of the associated function block is TRUE (the operation output value is open) if MV=2, and OUT is FALSE (the operation output value is close) if MV=0.

When operations from an HIS are permitted (MODE=MAN), the output value OUT of a function block is changed if MV is manipulated from the HIS. Changes of the value of OUT can be monitored on the HIS as changes of MV.

- Default
  The default value of MV is 0.

MTM (mask time)

This data item display the answerback check mask time. The default value is 0. The unit is seconds and the fractional part indicates milliseconds. Data entry from an HIS is not allowed.

- Associating parameters of function blocks
  The MTM parameter (answerback check mask time) of a function block is associated with MTM.

Process alarms

MOB_11 and MOB_21 notify process alarms of answerback error and IOP/OOP.

Answerback error alarms

If an answerback error occurs, a process alarm is notified when the associated parameter of a function block changes under the following conditions. Notification of generation of answerback pattern errors and recovery from the errors is made only from MOB_21.

- Notification of answerback error on the open side (ANS+): At a falling edge of NANP
- Notification of answerback error on the close side (ANS-): At a falling edge of NANM
- Notification of answerback pattern error (PERR): At a falling edge of NPER

If the system recovers from an answerback error, a process alarm is notified. The notification is made if the parameters of a function block change under the following conditions.

- Recovery notification of answerback error on the open side (ANS+ cancellation): At a rising edge of NANP
- Recovery notification of answerback error on the close side (ANS- cancellation): At a rising edge of NANM
- Recovery notification of answerback pattern error (PERR cancellation): At a rising edge of NPER

IOP and OOP

If you connect a signal indicating whether or not the answerback input signal is normal to the IOP parameter and a signal indicating whether or not the output signal is normal to the OOP parameter, input/output errors can be notified as process alarms. The notification is made if the parameters of a function block change under the following conditions.

- Input error occurrence alarm: At a falling edge of IOP
- Output error occurrence alarm: At a falling edge of OOP

The notification of recovery is made if the parameters of the function blocks change under the following conditions.

- Input error recovery alarm: At a rising edge of IOP
- Output error recovery alarm: At a rising edge of OOP

B5.2 HIS interfaces of MOB_RS (auto-reset BOOL-type data manual operation)

Auto-reset BOOL-type data manual operation function blocks output pulses when operated manually from an HIS.

B5.2.1 Operations of MOB_RS from HIS

This section explains the following functions of MOB_RS.

- Permission of manual operations and automatic reset of operation output values
- Answerback check

SEE ALSO For more information about description of the MOB_RS parameters, refer to:

7.6, “MOB_RS (auto-reset BOOL-type data manual operation)” in POU Reference Manual (IM 32P03B20-01EN)

Example of configuration of MOB_RS

The following figure shows a usage example of MOB_RS in a CENTUM integration structure.

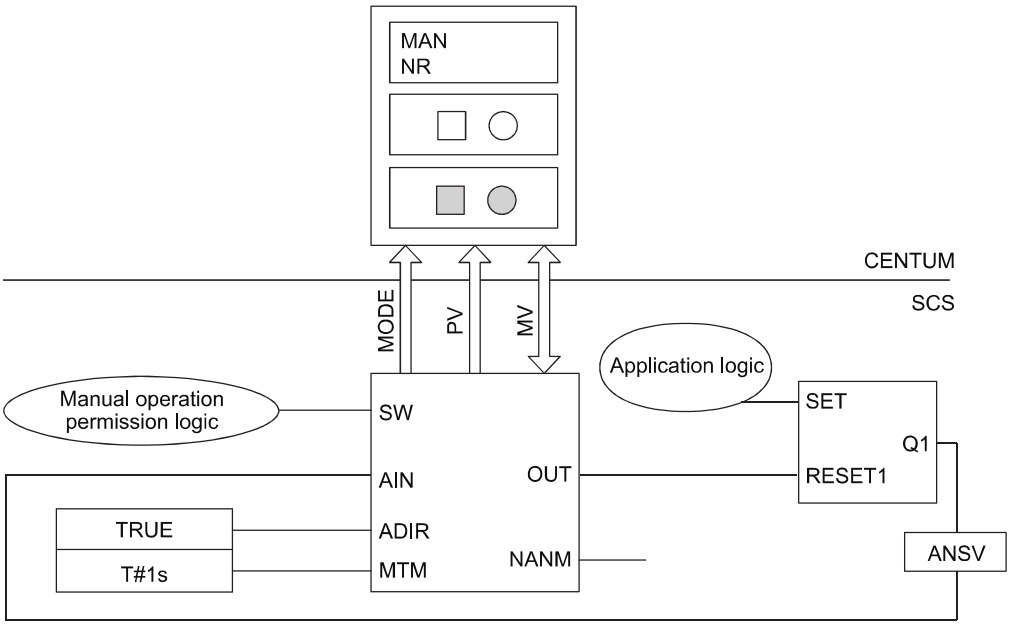


Figure B5.2.1-1 Overview of MOB_RS configuration

The associated parameter values of the SCS function block are sent to indicate the block mode (MODE) and answerback input value (PV) on the CENTUM side via the mapping blocks. The value of OUT is displayed as MV on the HIS instrument faceplate and operations on MV from the HIS are sent to OUT of the SCS in the manual mode (MAN).

Overview of processing MOB_RS

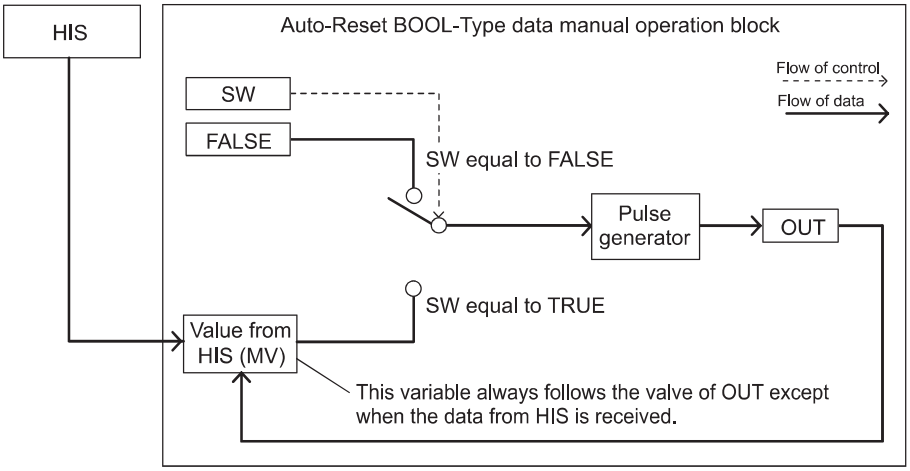


Figure B5.2.1-2 Flow of control and data of MOB_RS

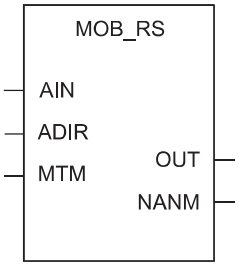
- Prohibition of Manual operations
  If the manual operation permit switch SW is FALSE, OUT is fixed to FALSE. If an operator attempts to perform manual operations from an HIS when the input to SW is FALSE (manual operations prohibited), the attempt will fail.
- Permission of Manual Operations and Automatic Reset of Operation Output Value
  Manual operations by an operator from an HIS are permitted if TRUE is input to SW. If MV is changed from 0 to 2 in an HIS, the output value of OUT of MOB_RS changes to TRUE. The output of OUT returns to FALSE automatically after the next scan in the scan period. The value of MV in the CENTUM system also returns to 0.

Confirmation of MOB_RS behavior via answerback input

The output value of MOB_RS caused by manual operations returns to FALSE quickly and an operator typically cannot check whether the manual operations were acknowledged or not. To alleviate this problem, it is a good idea to create a latch variable or similar that is reset by a pulse signal output from MOB_RS and input its value to the answerback input of MOB_RS. The changes of this value can then be displayed in the instrument faceplate. This way, it is possible to check whether the manual operations took effect through the instrument faceplate.

Answerback check

The following parameters are related to answerback check of MOB_RS.



Note: The SW parameter is omitted.

Figure B5.2.1-3 Parameters related to answerback check of MOB_RS

The table below explains the parameters.

Table B5.2.1-1 Explanation of parameters related to answerback check

IN/OUT	Argu-ments	Data type	Description
IN	AIN	BOOL	Answerback input value.
	ADIR	BOOL	Answerback operation direction specification. TRUE: Forward operation. FALSE: Reverse operation.
	MTM	TIME	Answerback check mask time (Must be an integer multiple of the scan period).
OUT	OUT	BOOL	Operation output value for logic reset (pulse signal).
	NANM	BOOL	Answerback status. TRUE: Normal status. FALSE: Abnormal status.

Answerback operation direction

Specify whether the answerback input signal becomes TRUE at normal or abnormal status, using the answerback operation direction specification (ADIR).

- Specification of forward operation
  A forward operation refers to an operation where the answerback signal is latched to TRUE when the specified events occur and return to FALSE due to the pulse output from OUT. Specify TRUE for ADIR.
- Specification of reverse operation
  A reverse operation refers to an operation where the answerback signal is latched to FALSE when the specified events occur and return to TRUE due to the pulse output from OUT. Specify FALSE for ADIR.

Answerback operation at forward operation

In a forward operation, the relationship between the output signal OUT and the answerback signal is as illustrated in the figure below.

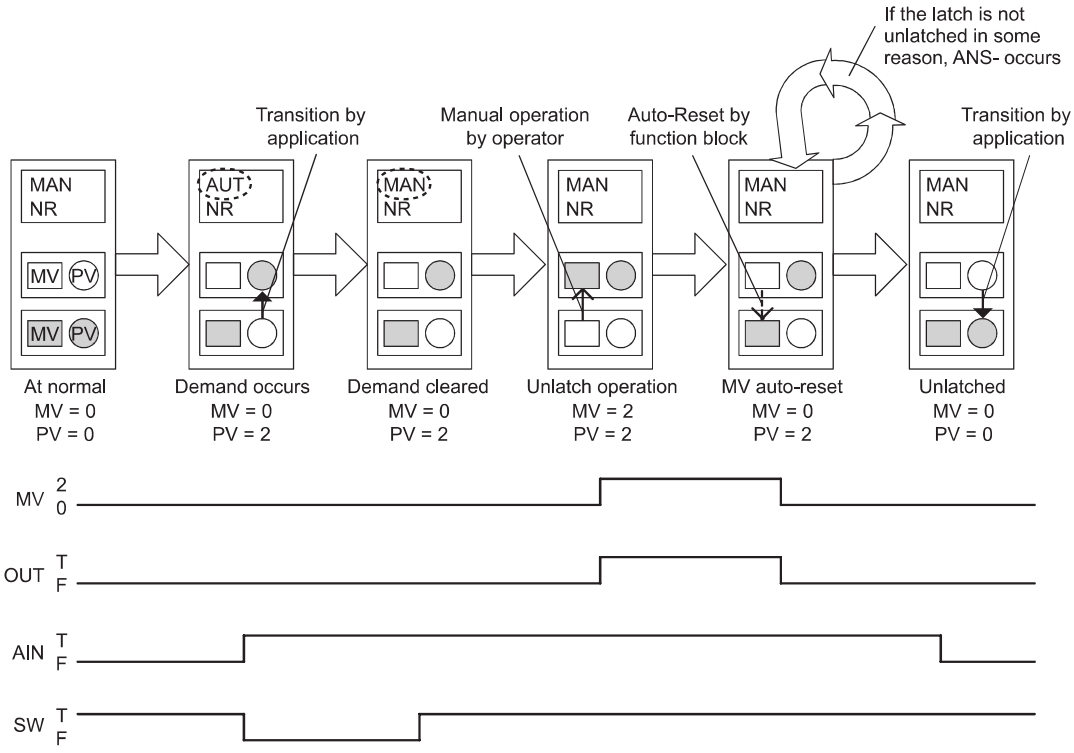


Figure B5.2.1-4 Relationship between MV manipulation and answerback (forward operation)

The data items of CENTUM and parameter values of MOB_RS are related in the following ways.

- The AIN parameter (answerback input value) of MOB_RS is associated with PV on the CENTUM side. PV=2 if AIN=TRUE and PV=0 if AIN=FALSE.
- The OUT parameter of MOB_RS is associated with MV on the CENTUM side. OUT=TRUE if MV=2 and OUT=FALSE if MV=0.

1. At normal status, MV=0 and FALSE is output to OUT of MOB_RS.
2. Create application logic such that AIN of MOB_RS is latched to TRUE at the occurrence of a demand. If AIN becomes TRUE, PV becomes 2.
3. If MV is changed to 2 from an HIS to reset the latch, OUT of MOB_RS changes to TRUE. OUT returns to FALSE after one scan (automatic reset).
4. Create application logic such that the latch is reset upon changes of OUT from FALSE to TRUE and AIN returns to FALSE. PV becomes 0 if AIN becomes FALSE.

Answerback operation at reverse operation

In a reverse operation, the relationship between the output signal OUT and the answerback signal is as illustrated in the figure below.

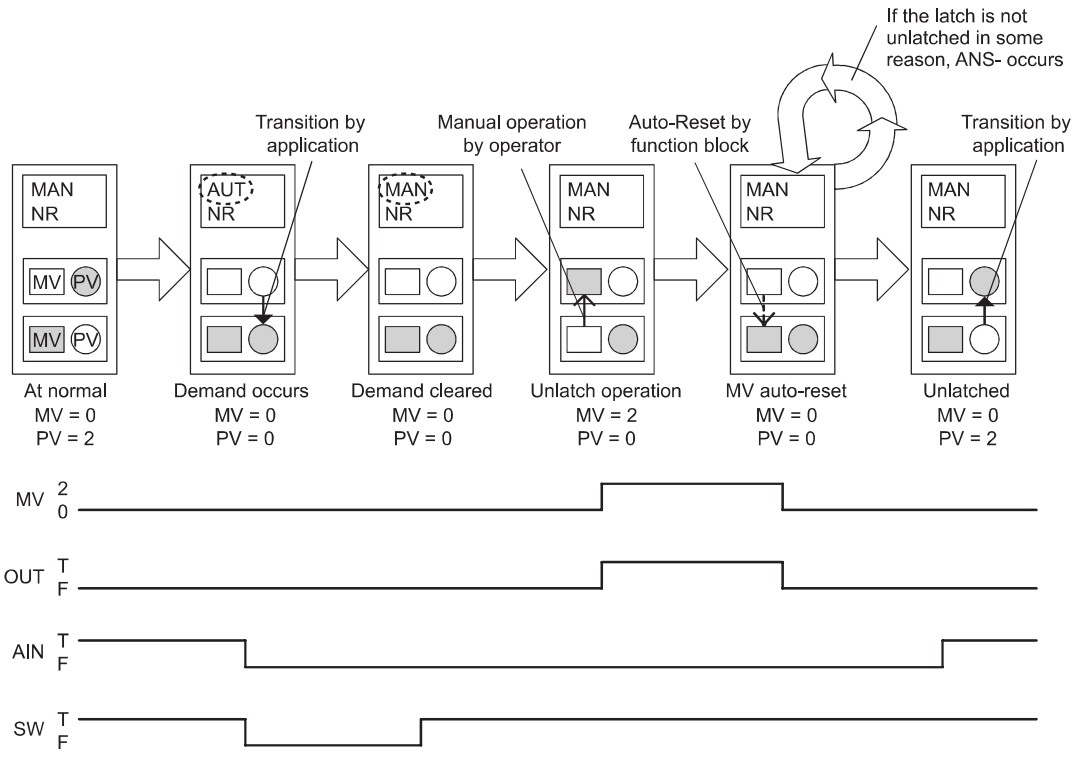


Figure B5.2.1-5 Relationship between MV manipulation and answerback (reverse operation)

A reverse operation is normal if the values of PV and MV are opposite in the HIS instrument faceplate.

Notification of answerback errors

An answerback error occurs if AIN (answerback signal) does not return to the normal value within the time specified by MTM (answerback check mask time) after a pulse signal is generated by manipulation of MV. The normal value of AIN is FALSE in the case of forward operations and TRUE in the case of reverse operations. If an answerback error is detected, FALSE is output from NANM (answerback status) and a notification is made to an HIS as a process alarm (ANS-) on the CENTUM side.

The system recovers from an answerback error if MV is manipulated again or AIN (answerback signal) returns to the normal value. On recovery, TRUE is output from NANM (answerback status).

Note that if 0 seconds are specified for MTM, answerback check is started from the next scan after OUT becomes TRUE.

B5.2.2 Tag name interfaces and process alarms of MOB_RS

In order to manually operate auto-reset BOOL-type data manual operation function blocks from an HIS, it is necessary to specify the tag names using the Tag Name Builder and associate them with mapping blocks. This allows them to be called via tag names and notification of process alarms.

Mapping blocks associated with auto-reset BOOL-type data manual operation function blocks are S_MOB_RS.

■ Settings in the Tag Name Builder

To perform manual operations from an HIS, make settings for the relevant instances of MOB_RS in the Tag Name Builder. Specify whether or not to notify answerback error alarms according to the following procedure.

- Answer back Alarm (answerback error alarm)
  Specify either [Both] or [No].

  Specify [Both] to notify answerback error alarms. Only ANS- process alarms are generated even if [Both] is specified.

■ Data items of S_MOB_RS

Among the data items of mapping blocks, the data items unique to S_MOB_RS are explained here. All of these data items are displayed in the HIS tuning view.

SEE ALSO For more information about descriptions regarding MODE (Block mode), AFLS (Alarm flashing status), AF (Alarm detection), AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

● MODE (block mode)

This data item indicates block mode. The block mode cannot be changed into AUT or MAN from an HIS. The default value of MODE is O/S (AUT).

- Associating parameters of function blocks
  The SW parameter (manual operation permit/prohibit toggle switch) of MOB_RS is associated with MODE.
- Changes of block mode (AUT/MAN)
  The block mode becomes MAN if TRUE is input to SW, and AUT if FALSE is input.

● ALRM (alarm status)

This data item displays alarm status.

Data entry from an HIS is not allowed.

The default value of ALRM is NR.

● PV (answerback input value)

This data item displays answerback input signals connected to MOB_RS. Data entry from an HIS is not allowed. It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend.

- Associating parameters of function blocks
  The AIN parameter (answerback input value) of MOB_RS is associated with PV.
- Range
  The range of PV is 0 or 2.

- Correspondence between changes of the parameter value of MOB_RS and changes of PV
  PV=2 if AIN (answerback input value) of MOB_RS is TRUE and PV=0 if FALSE.
- Default
  The default value (0) of AIN is reflected in the default value of PV.

MV (manipulated output value)

This data item is associated with the operation output value of MOB_RS. Its value can be changed if manual operations from an HIS are permitted (block mode=MAN). It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend.

- Associating parameters of function blocks
  The OUT parameter (logic reset operation output value) of MOB_RS is associated with MV.
- Range
  The range of MV is 0 or 2.
- Correspondence between changes of the parameter value of function blocks and changes of MV
  MV=2 if OUT of MOB_RS is TRUE and MV=0 if FALSE.

  When operations from an HIS are permitted (MODE=MAN), OUT of MOB_RS changes if MV is manipulated from the HIS.
- Default
  The default value of MV is 0.

SW (switch)

This data item displays the status of the manual operation permit/prohibit toggle switch of MOA. Data entry from an HIS is not allowed.

- Associating parameters of function blocks
  The SW parameter (manual operation permit/prohibit toggle switch) of a function block is associated with SW. The SW value of MOB_RS is reflected in this item.
- Range
  The range of SW is 0 or 1.

MTM (mask time)

This data item display the answerback check mask time. The unit is seconds and the fractional part indicates milliseconds. Data entry from an HIS is not allowed.

- Associating parameters of function blocks
  The MTM parameter (answer back check mask time) of MOB_RS is associated with MTM.
- Default
  The default value of MTM is 0.

Process alarms

MOB_RS notifies answerback error alarms.

Answerback error alarms

If an answerback error occurs, a process alarm is notified when NANM of MOB_RS changes under the following condition.

- Notification of answerback error occurrence (ANS-): At a falling edge of NANM

B5.3 HIS interfaces of MOA (analog-type data manual operation)

Analog-type data manual operation function blocks can monitor the values of analog output variables via an HIS, and it is possible to change the output values from the HIS.

Analog-type data manual operation function blocks also have a parameter for receiving shut-down events and are able to output the shutdown logic signal with the highest priority at the occurrence of a shutdown event.

B5.3.1 Operations of MOA from HIS

This section explains the following functions of MOA.

- Feedback input
- OOP detection

The password for manual operations is the same as MOB_11 and MOB_21.

SEE ALSO For more information about password for allowing manual operation, refer to:

B5.1.2, “Password at manual operations” on page B5-9

For more information about display of output enabled status, refer to:

B5.1.3, “The Output Enable status display function” on page B5-11

For more information about description of MOA parameters, refer to:

7.7, “MOA (analog-type data manual operation)” in POU Reference Manual (IM 32P03B20-01EN)

Example of configuration of MOA

The figure below shows a usage example of MOA in a CENTUM integration structure.

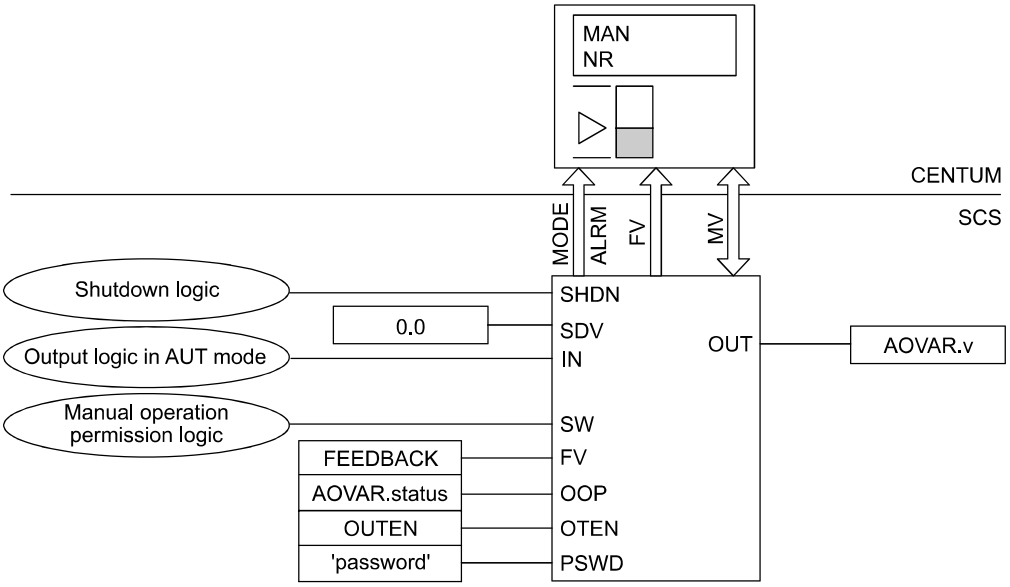


Figure B5.3.1-1 Analog-type data manual operation function blocks

The associated parameter values of the SCS function block are sent to indicate the block mode (MODE), process alarms (ALRM) and feedback input value (FV) on the CENTUM side via the mapping blocks. The value of OUT is displayed as MV on the HIS instrument faceplate and operations on MV from the HIS are sent to OUT of the SCS in the manual mode (MAN).

Overview of processing MOA

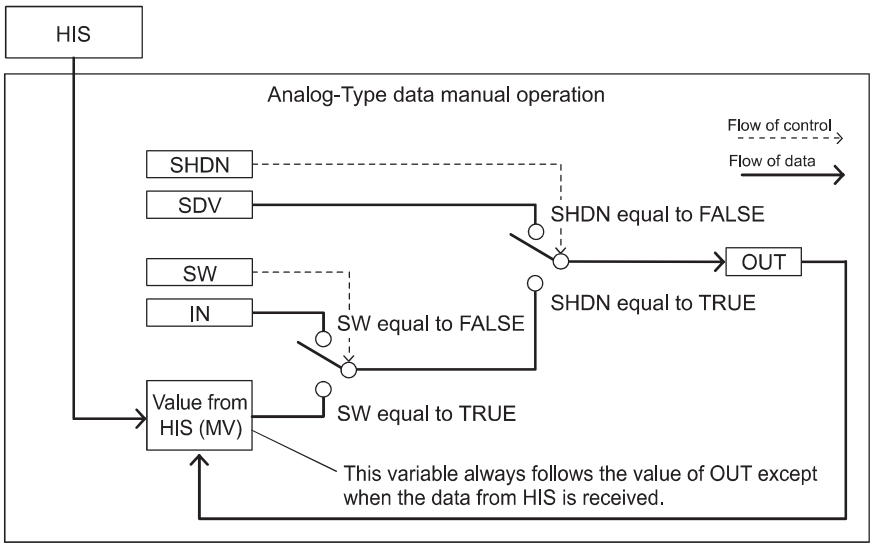


Figure B5.3.1-2 Flow of control and data (MOA)

Shutdown processing

If the input value of SHDN (shutdown signal) becomes FALSE, the value of SDV (shutdown output value) is output from OUT. At this point, all data settings from input parameters other than SHDN and SDV as well as an HIS are ignored. The SHDN input of MOA supports only DTS logic (normal: TRUE, abnormal: FALSE). Connect a reversed shutdown logic signal to SHDN in the case of ETS logic (normal: FALSE, abnormal: TRUE).

Prohibition of manual operations

If the input value of SHDN is set to TRUE (status where shutdown processing is not performed) and the manual operation permit switch SW is set to FALSE (manual operations prohibited), the value input to IN is output to OUT as is. If an operator attempts to perform manual operations from an HIS when the input to SW is FALSE, the attempt will fail. IN can be used to change the output value of OUT from the application logic when no shutdown instruction is input to SHDN (i.e., the system is in a safe state).

Permission of manual operations

Manual operation can be permitted when the SHDN value is TRUE and it is in a safe state where shutdown processing is not being performed. If SHDN is TRUE and SW is TRUE (manual operation permitted), manual operation by the operator from HIS is permitted and the result is output from OUT. Note that password entry is required to perform manual operations. The password is checked within a function block. If the password is incorrect, a warning message for the illegal operation is displayed and OUT remains unchanged.

TIP

You can specify with the SCS Constants Builder whether to skip the password dialog box on HIS when an empty string constant is set in PSWD of the function block. As a result of specifying not skipping, when the Password Input dialog box appears on HIS, just press the Enter key.
Regardless of whether the Password Input dialog box is displayed or not, the reconfirmation dialog box is displayed.

SEE ALSO

For more information about specification to skip the Password Input dialog box, refer to:

"● Skip password dialog box for manual operation FB" in "■ Settings with the Communication Tab" in C1.2.6, "SCS Constants Builder" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Feedback input

The feedback input (FV: data type is REAL) can be used for the purpose of checking the result of manipulating MV from an HIS on instrument faceplate and so on. Input a signal indicating the degree of opening of a valve or similar connected to the output variable channel connected to OUT, to FV.

- It is not checked that the values of OUT and FV match.
- The value of FV is used for checking purposes only in an HIS. It has no influence on the output behavior of OUT.

OOP detection

It is possible to use OOP (whose data type is BOOL) to check whether or not an output signal is normal. Input the data status of an output signal (output variable connected to OUT) or similar to OOP. Process alarms are notified on the CENTUM side according to the change of the OOP value.

- The value of OOP has no influence on the output behavior of OUT.

B5.3.2 Tag name interfaces and process alarms of MOA

In order to manually operate analog-type data manual operation function blocks from an HIS, it is necessary to specify the tag names using the Tag Name Builder and associate them with mapping blocks. This allows them to be called via tag names and notification of process alarms.

Mapping blocks associated with analog-type data manual operation function blocks are displayed as S_MOA.

Settings in the Tag Name Builder

To perform manual operations from an HIS, make settings for the relevant instances of MOA in the Tag Name Builder. The settings related to MOA are as follows.

Output high and low limits

The output scale high and low limits are valid setting items when the block is in the mode that manual operation is allowed (MODE=MAN). This indicates the range of MV value that can be set by the operator without confirmation. When a value beyond the limits is set from HIS to the MV, a dialog box will be displayed for confirmation to set the MV beyond the limits. If you approve, the MV value is set.

This function is different from the Output Limiter function of FCS.

- Output high limit
  Specify a value in the range from 0.0 to 100.0%. The default is 100.0%.

  This item is associated with data item MH of mapping block.
- Output low limit
  Specify a value in the range from 0.0 to 100.0%. The default is 0.0%.

  This item is associated with data item ML of mapping block.

Output scale high and low limits

The output scale high and low limits are valid setting items when the block is in the mode that manual operation is allowed (MODE=MAN). These settings indicate the upper and lower limits at entering MV value from HIS. A value beyond these high and low limits cannot be entered from HIS.

- Output Scale High Limit
  The value of this item is fixed to 100.0%. The value cannot be changed.

  This item is associated with data item MSH of mapping block.
- Output Scale Low Limit
  The value of this item is fixed to 0.0%. The value cannot be changed.

  This item is associated with data item MSL of mapping block.

TIP When a block is in a block mode that the manual operation is not allowed (MODE=AUT), the output from OUT will not be affected by the output high and low limits or the output scale high and low limits. The values specified by the parameters of IN or SDV of MOA will be intact and directly outputted.

Data items of S_MOA

Among the data items of mapping blocks, the data items unique to S_MOA are explained here. All of these data items are displayed in the HIS tuning view with the exception of SH and SL.

SEE ALSO For more information about descriptions regarding MODE (Block mode), AFLS (Alarm flashing status), AF (Alarm detection), AOFS (Alarm inhibition), OPMK (Operation mark), and UAID (User application ID), refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

MODE (block mode)

This data item indicates block mode. The block mode cannot be changed into AUT or MAN from an HIS. The default value of MODE is O/S (AUT).

- Associating parameters of function blocks
  The SHDN (shutdown signal), SW (manual operation permit/prohibit toggle switch) and OTEN (signal indicating output enable status) parameters of MOA are associated with MODE.
- Changes of block mode (AUT/MAN)
  The block mode becomes AUT if the SHDN parameter of MOA is FALSE. If SHDN is TRUE, the block mode becomes MAN if TRUE is input to the SW parameter of MOA, and AUT if FALSE is input to SW.
- Changes of block mode (output enable status)
  The block mode IMAN is added to the block mode if OTEN is FALSE and IMAN is removed from the block mode if OTEN is TRUE.

ALRM (alarm status)

This data item displays alarm status.

Data entry from an HIS is not allowed.

The default value of ALRM is NR.

FV (feedback input value)

This data item displays the feedback input signal connected to MOA. Data entry from an HIS is not allowed. It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend.

- Associating parameters of function blocks
  The FV parameter (feedback input value) of MOA is associated with FV. The value of FV changes according to the changes of the FV value of MOA.
- Range
  The range of FV is 0 to 100%.
- Default
  The default value of parameter (0%) of MOA is reflected in the default value of FV.

MV (manipulated output value)

This data item is associated with the operation output value of MOA. Its value can be changed if manual operations from an HIS are permitted (block mode=MAN). It is displayed in the parameter display area of instrument faceplate and will be a target of data collection for tuning trend.

- Associating parameters of function blocks
  The OUT parameter (analog operation output value) of MOA is associated with MV. The value of MV changes according to the changes of the OUT value of MOA.
- Range
  The range of MV is 0 to 100%.
- Default
  The default value of MV is 0%.

SHDN (shutdown signal)

This data item displays signals used for shutdown logic. Data entry from an HIS is not allowed.

- Associating parameters of function blocks
  The SHDN parameter (shutdown signal) of MOA is associated with SHDN. The SHDN value of MOA is reflected in this data item.
- Range
  The range of SHDN is 0 or 1.
- Correspondence between changes of the parameter value of function blocks and changes of SHDN
  Changes of the SHDN (shutdown signal) value of MOA match with changes of SHDN.

  If the value of SHDN is 0, the value of SDV (shutdown output value) is output as a shutdown signal from the OUT parameter (corresponding to a data item MV) of MOA.

SDV (shutdown output value)

This data item displays a value output as a shutdown signal when shutdown processing is performed. Data entry from an HIS is not allowed.

- Associating parameters of function blocks
  The SDV parameter (shutdown output value) of MOA is associated with SDV. The SDV value of MOA is reflected in this data item.
- Range
  The range of SDV is 0 to 100%.

INV (logic input value)

This data item is associated with the value specified to be output under conditions where the shutdown logic is not effective and operations from an HIS are prohibited. Data entry from an HIS is not allowed.

- Associating parameters of function blocks
  The IN parameter (specified output value when manual operations are prohibited) of MOA is associated with INV. The default value of IN of MOA is reflected in this data item. The value of INV changes according to changes of the IN value of MOA.
- Range
  The range of INV is 0 to 100%.

SW (switch)

This data item displays the status of the manual operation permit/prohibit toggle switch of the FB. Data entry from an HIS is not allowed.

The value of the data item SW is determined as follows according to the value of the FB parameter and the SCS Constants Builder specification.

Table B5.3.2-1 Value set for data item SW

SW of FB	PSWD of FB	SCS Constants Builder specification	Data item SW
FALSE	- (*1)	- (*1)	0
TRUE	Other than an empty string constant	- (*1)	1
	Empty string constant	Do not skip the Password Input dialog box.	1
		Skip the Password Input dialog box.	2

*1: It does not affect the value of data item SW

MSH (output range high limit)

This data item displays the output scale high limit. Data entry from an HIS is not allowed. The value is fixed to 100%.

MSL (output range low limit)

This data item displays the output scale low limit. Data entry from an HIS is not allowed. The value is fixed to 0%.

MH (output high limit)

This data item displays the output high limit defined in the Tag Name Builder. Data entry from an HIS is not allowed. The range is 0 to 100%.

ML (output low limit)

This data item displays the output low limit defined in the Tag Name Builder. Data entry from an HIS is not allowed. The range is 0 to 100%.

SH (FV scale high limit)

This data item is used to display the high limit of FV bar in an instrument faceplate. The value is fixed to 100%.

SL (FV scale low limit)

This data item is used to display the low limit of the FV bar in an instrument faceplate. The value is fixed to 0%.

Process alarms

MOA notifies process alarms of OOP.

OOP

If you connect a signal indicating whether or not the output signal is normal to the OOP parameter of MOA, output errors are notified as process alarms. The notification is made if the parameter of MOA changes under the following condition.

- Output error occurrence alarm: At a falling edge of OOP

The notification of recovery is made if the parameter of MOA changes under the following condition.

- Output error recovery alarm: At a rising edge of OOP

B6. Data setting using external communication function blocks

Data setting from FCSs is performed via tag name interfaces using external communication function blocks dedicated for data setting. These function blocks allow data setting not only from FCS, but also from HIS. External communication function blocks are provided for each of the data types.

Data setting from FCS

In order to set data via tag name interfaces, define tag names for instances of external communication function blocks in Tag Builder in an SENG. Once tag names are defined, mapping elements (%WB) are generated. By accessing these mapping elements using the syntax "<tag name>.<data item>," data can be referenced and set. The table below lists data item names used when accessing data.

Table B6-1 Data items of tag name interfaces

External communication FB	Data item name(referencing and setting)
ECW_B	PV
ECW_I	PVI32
ECW_R	PVF32

Tag name interfaces use the same data item names for referencing and setting data. For example, if the tag name TAG0702 is defined for an ECW_I function block, the specification "TAG0702.PVI32" can be used when both referencing and setting data of this function block. If the tag name TAG0703 is set for an ECW_R function block, "TAG0703.PVF32" is used to access data.

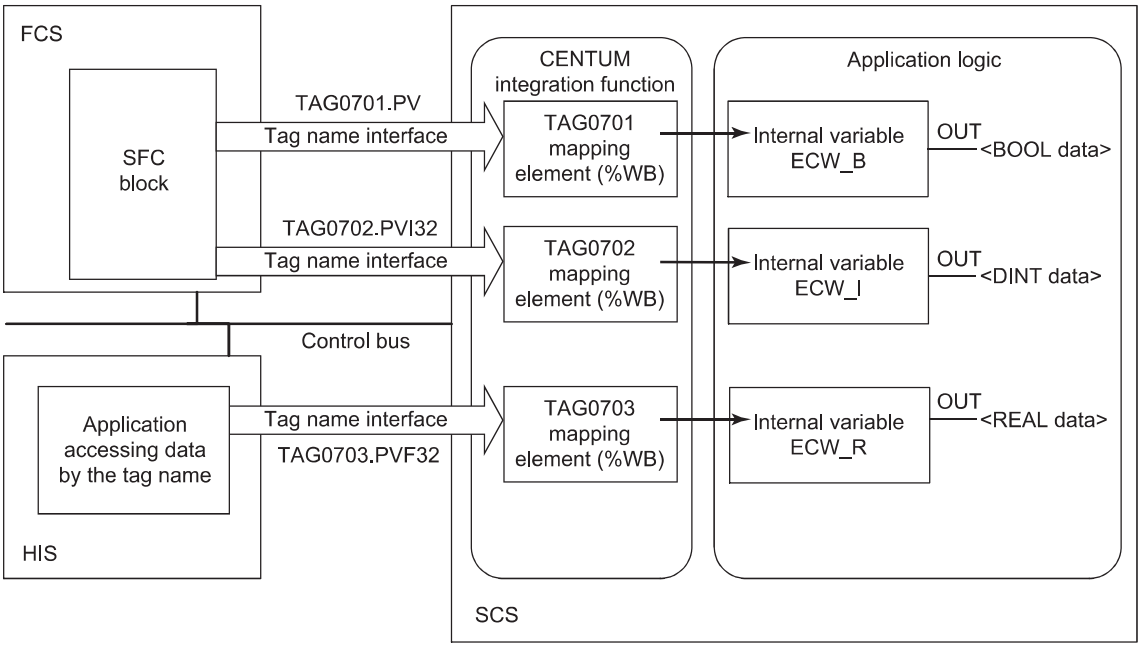


Figure B6-1 Data setting using tag name interfaces of external communication function blocks

B6.1 Confirmation of setting data

In order to use data set by external communication function blocks in an application used in a safety loop, it is necessary to incorporate certain safety measures (various functions to secure safety) with a user application.

An example that uses an application logic that checks the status of data set from an HIS or FCS as a safety measure is shown below.

Confirmation of data set via tag name interfaces

The data set from an FCS is stored temporarily in a mapping element (WT003) and then reflected in an external communication function block. The figure below shows an example of an application that checks whether the set data reached the application logic or not.

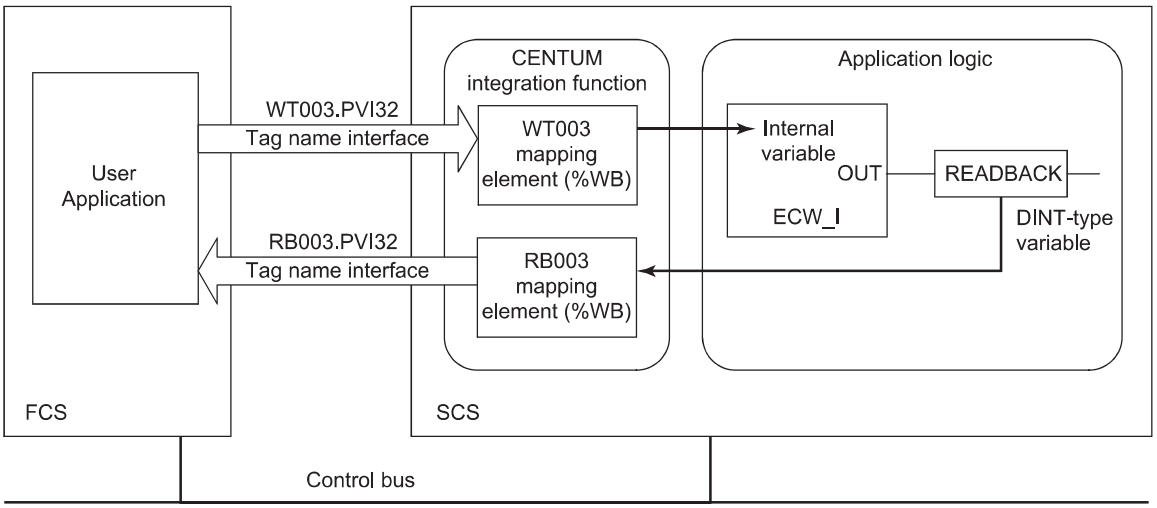


Figure B6.1-1 Example of application that checks data setting using readback variable

Connect the variable READBACK (DINT-type variable) to the OUT variable so that the output from the OUT variable can be read back with a user application. By doing so, it can be confirmed that the data has been set correctly.

The procedure to set DINT-type data is shown below.

1. Define a tag name for data setting for an ECW_I (external communication function block) (WT003 in the example).
2. Define a tag name for data readback for the variable that will be used for reading the desired data back (RB003 in the example).
3. Set data from the external device (FCS in this example) using the specification "<tag name for data setting>.PVI32." In the example, data is set via WT003.PVI32.
4. Read the data back to the external device (FCS in the example) using the specification "<tag name for data readback>.PVI32." In the example, data is read back via RB003.PVI32.

B6.2 Tag name interfaces of external communication function blocks

This section explains data items of mapping elements associated with external communication function blocks.

■ Data items of mapping elements associated with external communication function blocks

By associating tag names with ECW_B, ECW_I and ECW_R type function blocks, it becomes possible to set data from outside an SCS using tag name interfaces. If you define tag names using the Tag Name Builder, mapping elements are created in the communication input/output (%WB) area.

Mapping elements of external communication commonly have OPMK data items.

SEE ALSO For more information about description regarding OPMK (Operation mark), refer to:

"■ Data items common to mapping blocks/mapping elements" on page B3-7

● Data items of mapping elements (%WB) associated with ECW_B (PV)

The Boolean value of ECW_B is displayed as PV. It is displayed in the HIS tuning view and the parameter display area of instrument faceplate, and will be a target of data collection for tuning trend. Data entry from an HIS is allowed.

The range is 0 or 1. The default value of ECW_B is reflected in the default value of PV.

● Data items of mapping elements (%WB) associated with ECW_I (PVI32)

The integer value of ECW_I is displayed as PVI32. It is displayed in the HIS tuning view and the parameter display area of instrument faceplate. Data entry from an HIS is allowed.

The range is all signed 32-bit integers. The default value of ECW_I is reflected in the default value of PVI32.

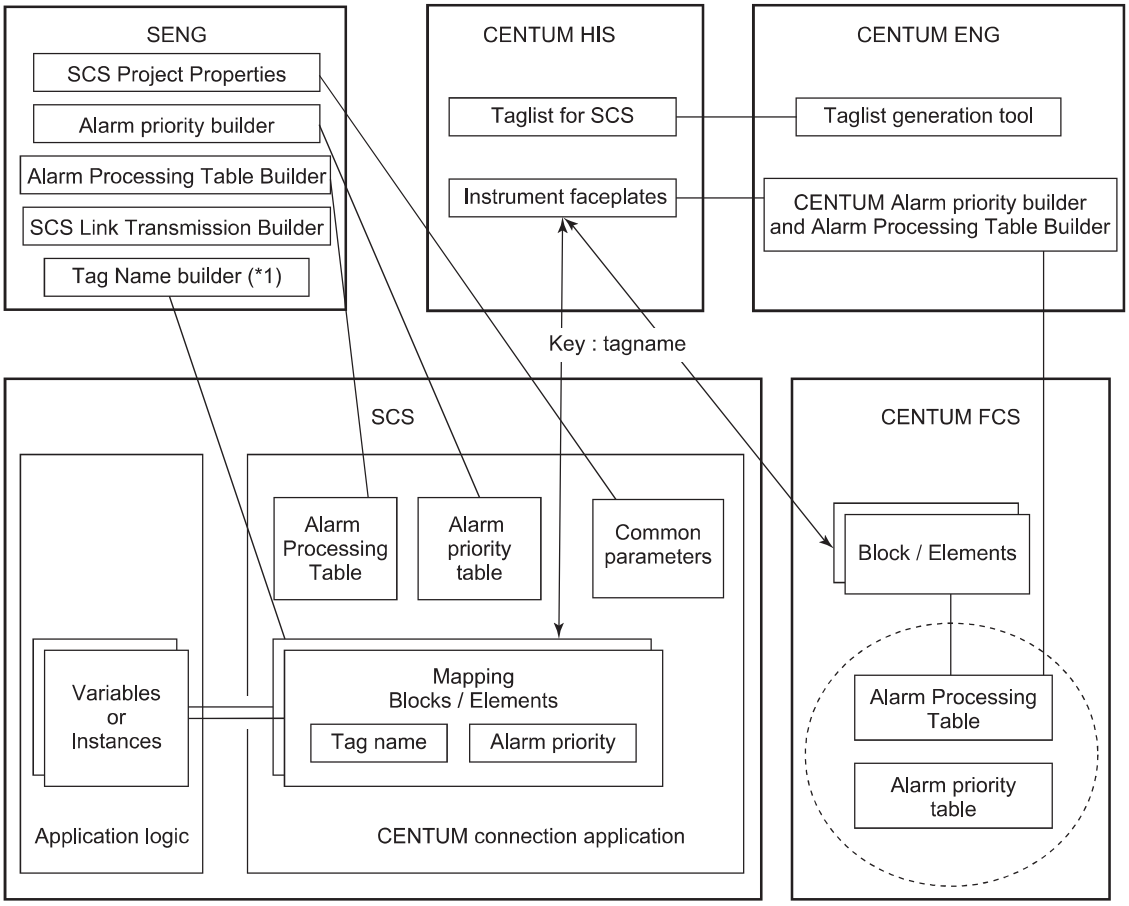
● Data items of mapping elements (%WB) associated with ECW_R (PVF32)

The value of ECW_R is displayed as PVF32 (a real number). It is displayed in the HIS tuning view and the parameter display area of instrument faceplate. Data entry from an HIS is allowed.

The range is all single precision real numbers. The default value of ECW_R is reflected in the default value of PVF32.

B7. Engineering for CENTUM integration

To realize the CENTUM integration, you need to connect a CENTUM project and an SCS project. To connect these projects, you need to engineer both the SCS project and the CENTUM project. This section describes the engineering tasks required for the CENTUM integration.



*1 : In the engineering with iDefine, you can also define tag names in iDefine.

Figure B7-1 Targets of engineering on SENG and CENTUM

SEE ALSO

For more information about overview of engineering procedures for integration with CENTUM, refer to:

"■ Engineering procedure of CENTUM integration configuration" on page B2-3

For more information about relationship between CENTUM projects and SCS projects, refer to:

"■ Relationship between projects" on page B2-5

■ Overview of engineering for CENTUM integration

The ENG is a PC which has a license for the CENTUM system builders. Each CENTUM application generated on the ENG is managed as part of a CENTUM project.

Applications to be downloaded to SCS are created on the SENG. One of such applications relates to tag names. A part of the tag-name-related application used for CENTUM integration is also written in the CENTUM project. The tag-name-related definition data written in the

CENTUM project is used in the engineering tasks, so that you can operate and monitor SCS from HIS and can access SCS data from FCS.

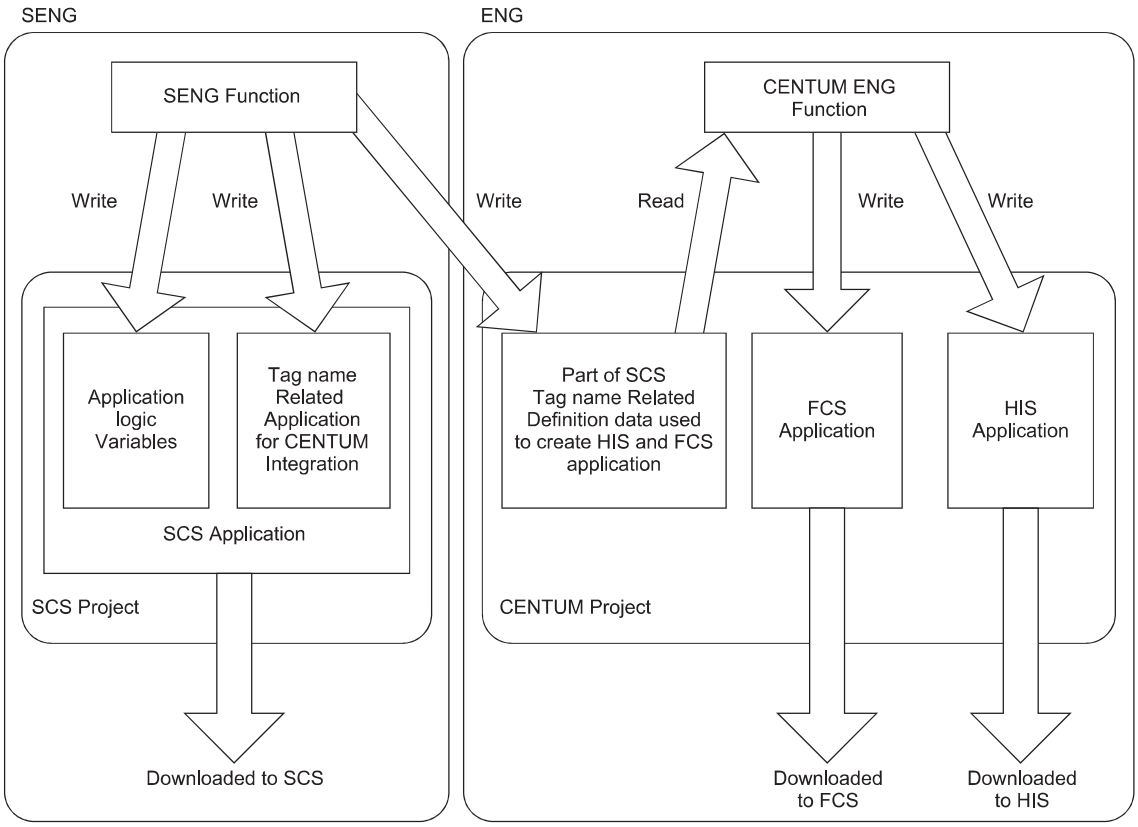


Figure B7-2 SCS project and CENTUM project

B7.1 Engineering on the SENG side

This section describes the engineering tasks performed on the SENG side, which is one of the tasks required to connect an SCS project and a CENTUM project.

B7.1.1 Setting of SCS project property

An SCS project and a CENTUM project can be connected using SCS Project Properties in an SCS manager. In SCS Project Properties, specify the folder of the CENTUM project you want to connect to the SCS project. The information for CENTUM integration that has been set in the SCS project can be copied to the CENTUM project folder.

The connection of an SCS project and a CENTUM project is set only in one direction: from the SCS project to the CENTUM project.

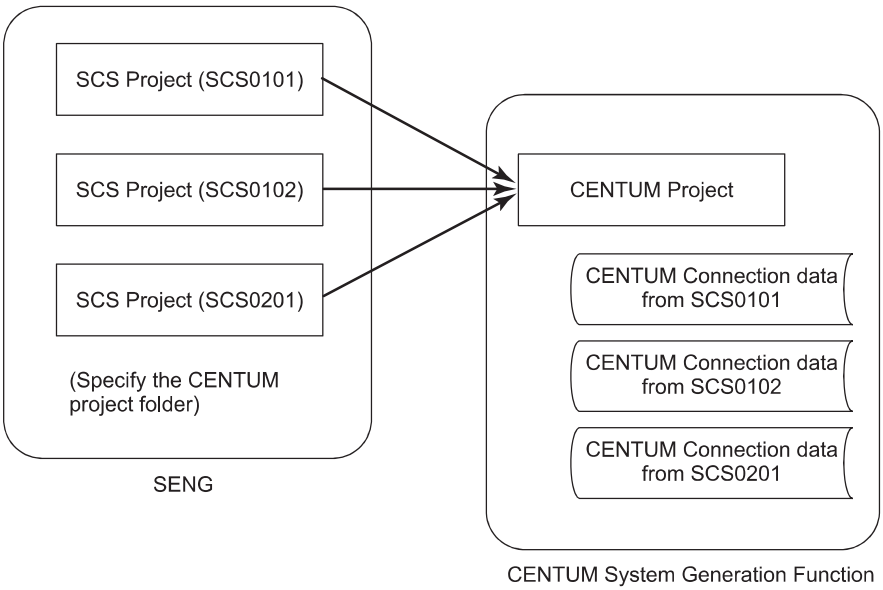


Figure B7.1.1-1 Settings for connection between SCS project and CENTUM project

SEE ALSO

For more information about relationship between SCS projects and CENTUM projects, refer to:

C1.1, “Type of project” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about specifying project folders, refer to:

C1.2.5, “SCS Project Properties dialog box” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

B7.1.2 Defining alarm priorities

Process alarms occurred on SCS can be monitored in the Process Alarm view of CENTUM HIS. Alarm priorities for monitoring on the CENTUM HIS can also be defined for the process alarms that occur on SCS.

This section describes the definition of Alarm Priorities in Alarm Priority Builder of ProSafe-RS.

ProSafe-RS Alarm Priority Builder

By using the Alarm Priority Builder, you can define the alarm output format and alarm action when an alarm has occurred or returned to a normal state for each SCS. Alarm priorities are classified as high-priority alarm, medium-priority alarm, low-priority alarm, logging alarm, and reference alarm.
To start the Alarm Priority Builder, do the following: From the SCS Manager, click [Tools] > [Engineering] to start the Engineering Launcher, and select [Alarm Priority Builder] from the menu.

For each alarm priority, set the alarm flashing action, re-warning, and flashing action upon returning to NR. Ensure that the [NR (Flashing)] setting on the Alarm Priority Builder on SENG is the same as the [NR] setting that is configured on the Alarm Priority Builder of the CENTUM System Builders.

TIP

The ProSafe-RS Alarm Priority Builder is different from the CENTUM Alarm Priority Builder. You cannot set the behavior of HIS from the 'Alarm Priority Builder on SENG.'

Downloading to an SCS

When alarm priorities are defined, the information is reflected in the SCS download database. Perform offline download of the database to the SCS using SCS Manager on SENG.

SEE ALSO

For more information about offline download, refer to:

C7., "Offline download to the target SCS" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Differences from CENTUM Alarm Priority Builder

When connecting an SCS project to a CENTUM project, two alarm priority builders must be used properly: one is ProSafe-RS Alarm Priority Builder launched from SCS Manager on the SENG, the other is Alarm Priority Builder launched from CENTUM System View. These two builders are used for their respective projects, with the following differences between the two:

- Target station
  ProSafe-RS Alarm Priority Builder can be used to change definitions for each SCS.

  CENTUM Alarm Priority Builder is common throughout the CENTUM project, and the definitions set in this builder apply to all HIS and FCS.

- Setting items
  ProSafe-RS Alarm Priority Builder is used to set SCS data, while CENTUM Alarm Priority Builder is used to set HIS and FCS data. Accordingly, the setting items are different between the two alarm priority builders.

Table B7.1.2-1 Setting items in ProSafe-RS and CENTUM Alarm Priority Builders

Title	Item	ProSafe-RS Alarm Priority Builder	CENTUM Alarm Priority Builder
CRT	Window display	Setting item not available	Can be set

Continues on the next page

Table B7.1.2-1 Setting items in ProSafe-RS and CENTUM Alarm Priority Builders (Table continued)

Title	Item	ProSafe-RS Alarm Priority Builder	CENTUM Alarm Priority Builder
PRT	Printing	Setting item not available	Can be set
Historical File	Storing in files	Setting item not available	Can be set
Buzzer Sound	Buzzer sound generation	Setting item not available	Can be set
Alarm Action	Alarm flashing action	Can be set	Can be set (*1)
Rewarning	Rewarning	Can be set	Can be set (*1)
NR (Flashing)	Flashing action upon returning to the NR state	Can be set (*2)	Can be set (*1)

*1: Defined only for FCSs
*2: Must be the same as settings on CENTUM Alarm Priority Builder

- File compatibility
  The builder files created in ProSafe-RS Alarm Priority Builder as well as their copies saved in different names cannot be opened in or imported to CENTUM Alarm Priority Builder, or vice versa. CSV files must be used to exchange data between the two builders.
- Other
  ProSafe-RS Alarm Priority Builder has no download menu. Downloading from this builder is performed in SCS Manager.

Window of ProSafe-RS Alarm Priority Builder

The following figure shows the Alarm Priority Builder main window:

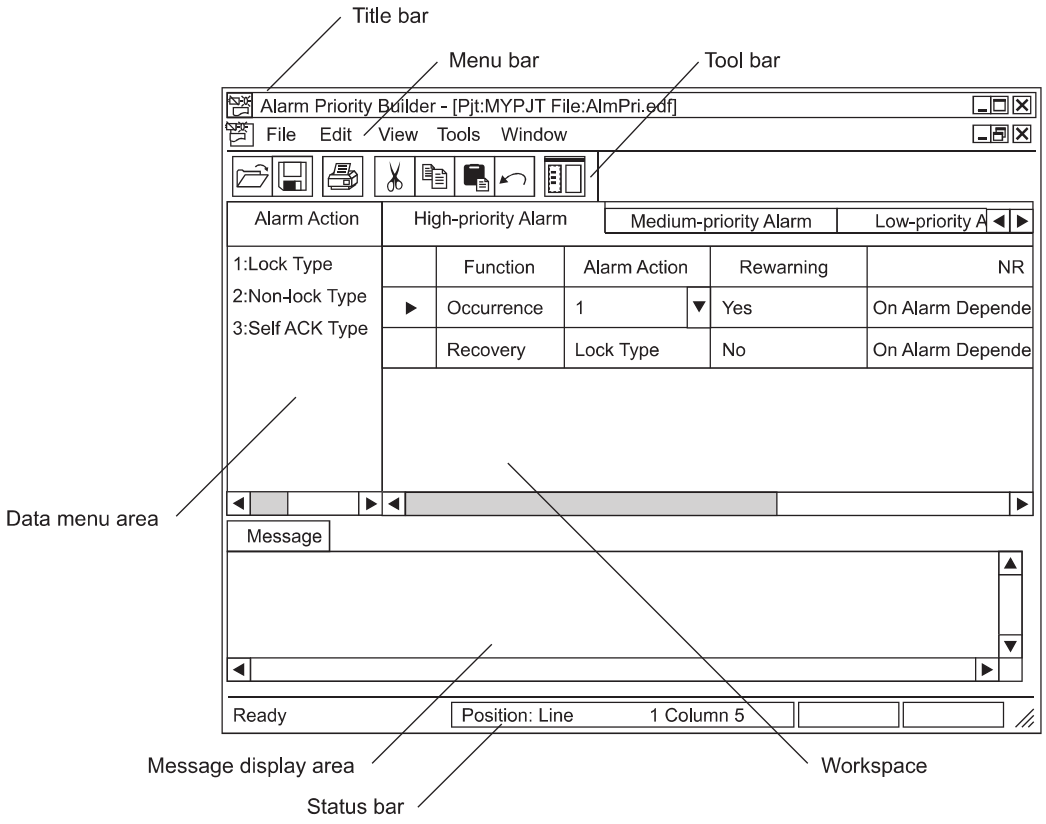


Figure B7.1.2-1 Main window of the Alarm Priority Builder

Setting items

ProSafe-RS Alarm Priority Builder has tabs corresponding to different alarm priority levels. All or some of the following items can be set in each of these tabs:

Table B7.1.2-2 Setting items

Item	Description
Alarm Action	Specify the alarm flashing action.
Rewarning	Specify whether to enable or disable rewarning.
NR (Flashing)	Specify the alarm action upon returning to the NR state.

In ProSafe-RS Alarm Priority Builder, set each action upon occurrence and recovery of alarms, for each alarm priority.

The actions corresponding to the blank fields in the following table cannot be set:

Table B7.1.2-3 Alarm priorities and settable items

Item	High-priority alarm(*1)		Medium-priority alarm (*1)		Low-priority alarm (*1)		Logging alarm(*1)		Reference alarm (*1)	
	Occurrence	Recovery	Occurrence	Recovery	Occurrence	Recovery	Occurrence	Recovery	Occurrence	Recovery
Alarm Action	Yes	Lock	Yes	Lock	Yes	Non-lock	Self ACK	Self ACK	Self ACK	Self ACK
Rewarning	Yes	No	-							
NR (Flashing)	Yes	On Alarm Dependent								

*1: Yes: Can be set
Other than Yes: Fixed value (cannot be specified)

Alarm Action

In Alarm Action (alarm flashing action), set the flashing indication used to notify the operator when an alarm has occurred. The desired flashing indication can be selected from the following three types:

Table B7.1.2-4 Types of flashing indication

Type	Action
Lock	The flashing indication will continue until the operator performs an acknowledgement operation, even after the alarm is reset upon returning to the NR state.
Non-lock Type	The flashing indication will stop without the operator performing an acknowledgement operation, when the alarm is reset upon returning to the NR state.
Self ACK	Flashing indication is not implemented, since the system will automatically acknowledge the alarm as soon as it is generated.

Rewarning

Rewarning is the alarm that notifies the operator of a continuing alarm state. This item can be specified only for high-priority alarms. The alarm message will be output again at the rewarning periods or when specified by command.

Table B7.1.2-5 Types of rewarning

Type	Description
0: No	Rewarning is not issued
1: Yes	Rewarning is issued

The rewarning period is set in SCS Constants Builder.

SEE ALSO For more information about SCS Constants Builder, refer to:

C1.2.6, “SCS Constants Builder” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

NR (Flashing)

NR (Flashing) defines the flashing indication used to notify the operator that all alarms in a given function block have been recovered upon returning to the NR state. The following two types of flashing display definitions are available for notifying the operator: This item can be specified only for high-priority alarms.

Table B7.1.2-6 Types of alarm action upon returning to NR

Type	Description
On Alarm Dependent	When all alarms have been reset upon returning to the NR state, the current flashing status will continue. If the indicator is flashing when the NR state is restored, the flashing will continue. If the indicator is not flashing when the NR state is restored, the non-flashing status will continue.
Notification at Return (*1)	When all alarms have been reset upon returning to the NR state, the flashing to indicate the NR state will start. Even when this flashing is not acknowledged, the flashing will stop when a new alarm is generated. Return of the entire function block to the NR state is notified by a Non-Lock action.

*1: Must be the same as the settings on CENTUM Alarm Priority Builder.
If the two settings are different, for example, the [NR] on CENTUM is set to [On Alarm Dependent] and the [NR (Flashing)] on the ProSafe-RS is set to [Notification at Return], the process alarm LED on the SCS blinks according to [Notification at Return], but no return sound is output.

If Alarm Action is set to "Self ACK" and alarm type upon returning to NR is set to "Notification at Return," an error message will be output when a file is saved.

B7.1.3 How to change the display color of alarms

You can change the display color of alarms generated by the mapping block in the CENTUM integration structure.

If you want to change the display color of alarms, configuration is required on both CENTUM VP and ProSafe-RS.

Operation procedure

If you want to change the display color of alarms, specify the color by using the Alarm Processing Table Builder on CENTUM VP.

IMPORTANT

- You must use an alarm processing level No. that is specified an appropriate priority to the related SCS among existing definitions and that is not used in CENTUM tags.
- Do not change the priority. If you change the priority by mistake, function blocks/elements of all FCSs in the related CENTUM project become invalid elements. Offline download is required to solve invalid elements.

This section describes how to change the text color of “FLT” for the mapping block S_GASDTR to cyan by using the alarm processing level No. 13 (classified to alarm processing level 1 (high-priority alarm) priority by default as well as the alarm processing level No. 1) as an example.

TIP

- You can use an alarm processing level No. from 5 to 16.
- “FLT” is assigned to the bit position 19.
- By default, “FLT” is shown in red.

1. In the Alarm Processing Table Builder on CENTUM VP, perform these steps:
   a. Set the same value of the color as the alarm processing level No. 1 to the color for the alarm processing level No. 13 for all bit positions.
   b. Change the color for the alarm processing level No. 13 on the bit position 19 to cyan.

IMPORTANT

Before you save in the Alarm Processing Table Builder on CENTUM VP, ensure that the settings except for the above settings remain unchanged. Unlike ProSafe-RS builders, download is executed immediately after you save in the Alarm Processing Table Builder on CENTUM VP. You must be careful not to change the priority. Otherwise, all FCSs in the related CENTUM project become invalid elements.

2. On SENG, import AlmTbl.edf that you have edited in the step 1 by using Alarm Processing Table Builder.
3. In the Tag Name Builder, set the Alarm Level of S_GASDTR tag to [13: User(13)].

SEE ALSO

For more information about procedure for importing to the Alarm Processing Table Builder, refer to:

B7.1.4, “Defining the alarm processing table” on page B7-11

For more information about Alarm Level in the Tag Name Builder, refer to:

“● Alarm Level” on page B7-24

For more information about the procedure for setting the alarm processing level by using the Alarm Processing Table Builder on CENTUM, refer to:

7.4, "Alarm Status Character String and Alarm Processing" in the Human Interface Stations Reference Vol. 2 (IM 33J05A11-01EN)

B7.1.4 Defining the alarm processing table

You can monitor the process alarms raised by the SCS from the Process Alarm view on the CENTUM HIS. This section describes how to operate Alarm Processing Table Builder.

TIP The Alarm Processing Table Builder on the ProSafe-RS and the Alarm Processing Table Builder on CS 3000 are two different entities.

Alarm Processing Table Builder

The Alarm Processing Table Builder determines the priority of alarms raised by Mapping block on SCS. The priority levels are 1 to 16.

Set the color and priority levels on the Alarm Processing Table Builder on the CENTUM and import the settings to the Alarm Processing Table Builder on ProSafe-RS because the builder on ProSafe-RS has no editing feature.

Engineering flow

Unlike the other builders, the Alarm Processing Table Builder on the ProSafe-RS imports the contents of settings on the Alarm Processing Table Builder on CENTUM. If the settings for the table used by SCS are changed on the Alarm Processing Table Builder on CENTUM, be sure to import the file for the Alarm Processing Table Builder on CENTUM to the Alarm Processing Table Builder on the ProSafe-RS. To reflect the imported data on the SCS, offline-downloading is required.
The engineering procedure is as follows:

With the SCS Manager, display the [SCS Project Properties] dialog box, select the [Project] tab, and enter the 'top folder of the CENTUM Project' into the field [CENTUM Project Folder]. Do this before going on to the following steps.

1. Start the Alarm Processing Table Builder:
   From the SCS Manager, click [Tools] > [Engineering] to start the Engineering Launcher, and select [Alarm Processing Table Builder] from the menu.
2. From the menu, select [File] > [External file] > [Import...].
   The following Import dialog appears.

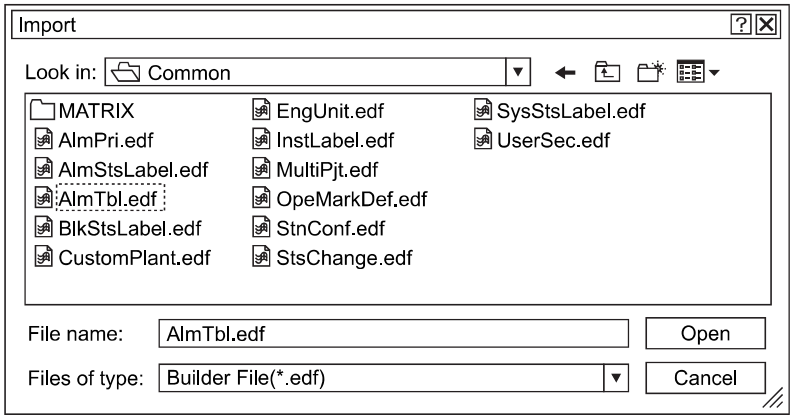


Figure B7.1.4-1 Import dialog box

3. Select the AlmTbl.edf of a CENTUM project and click the [Open] button.
4. From the menu of the Alarm Processing Table Builder, select [File] > [Save]. The AlmTbl.edf is saved in the SCS Project.
5. To reflect the contents in the AlmTbl.edf file on the SCS, execute [Build] in SCS Manager before offline-downloading.

B7.1.5 Defining tag names

When SCS project and CENTUM project are connected, tag names must be defined so that application logic variables and function blocks can be accessed from HIS or FCS. Tag names are defined in Tag Name Builder.

You can also define tag names from the editor of iDefine. If you export data from iDefine, import it to AD Organizer and run Reflection, the tag name definitions are reflected in the Tag Name Builder. Tag names and parameters that are defined using iDefine cannot be edited in the Tag Name Builder.

To use the Tag Name Builder, you must have a CENTUM integrated environment. Information of tag names defined by using iDefine without a CENTUM Integration are not reflected in SCS projects.

SEE ALSO For more information about defining tag names by using iDefine, refer to:

6., “PROSAFE-RS IO TAG NAME” in iDefine User Guide (Yokogawa Extensions) (PR12002-MAN-980_01)

■ Overview of tag name definition

This section explains the procedure to define tag names using the Tag Name Builder.

In the Tag Name Builder, define tag names for application logic variables or function block instances. Function blocks or variables having a defined tag name can be accessed from HIS based on their correspondence to Mapping Block/Element.

The following information is defined using Tag Name Builder: Tag names can only be defined for certain types of variable.

- Tag name
- Parameters required by Mapping Block/Element on SCS
- Parameters required by instrument faceplates on HIS

The procedure for defining tag names is as follows:

1. Define application logic variables or function block instances in Dictionary View of SCS Manager.
2. Define tag names and parameters in Tag Name Builder.

   To start the Tag Name Builder, do the following: From the SCS Manager, click [Tools] > [Engineering] to start the Engineering Launcher, and select [Tag Name Builder] from the menu.
3. Execute [Build] in SCS Manager to generate SCS database.

SEE ALSO For more information about variables for which tag names can be defined and details on the definition items, refer to:

“■ Setting items” on page B7-14

For more information about mapping blocks/elements, refer to:

B3.1, “Overview of tag name interfaces” on page B3-2

■ Window of Tag Name Builder

The following figure shows the Tag Name Builder main window:

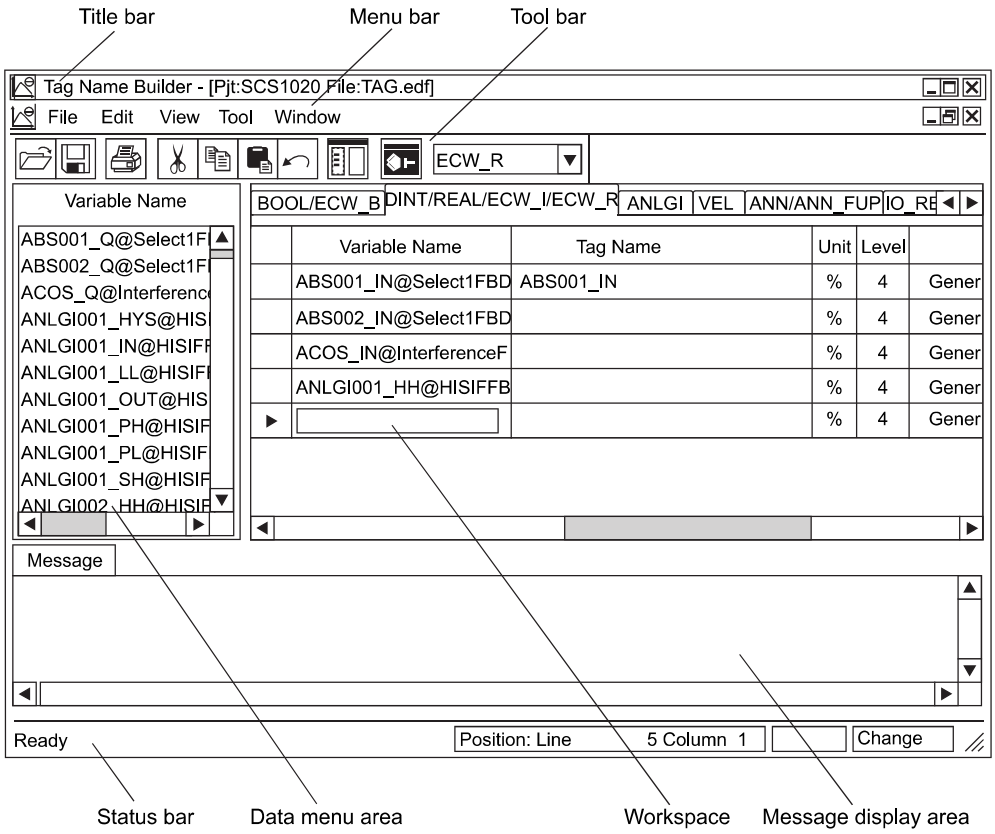


Figure B7.1.5-1 Main window of the Tag Name Builder

You can register a variable name in Tag Name Builder by dragging the variable name from Dictionary View and dropping it into a variable name field in Tag Name Builder. When multiple variable names are dragged and dropped, the variable names are registered in multiple variable fields starting from the top field. If a variable name is already registered in the variable name field, the variable name field is overwritten.

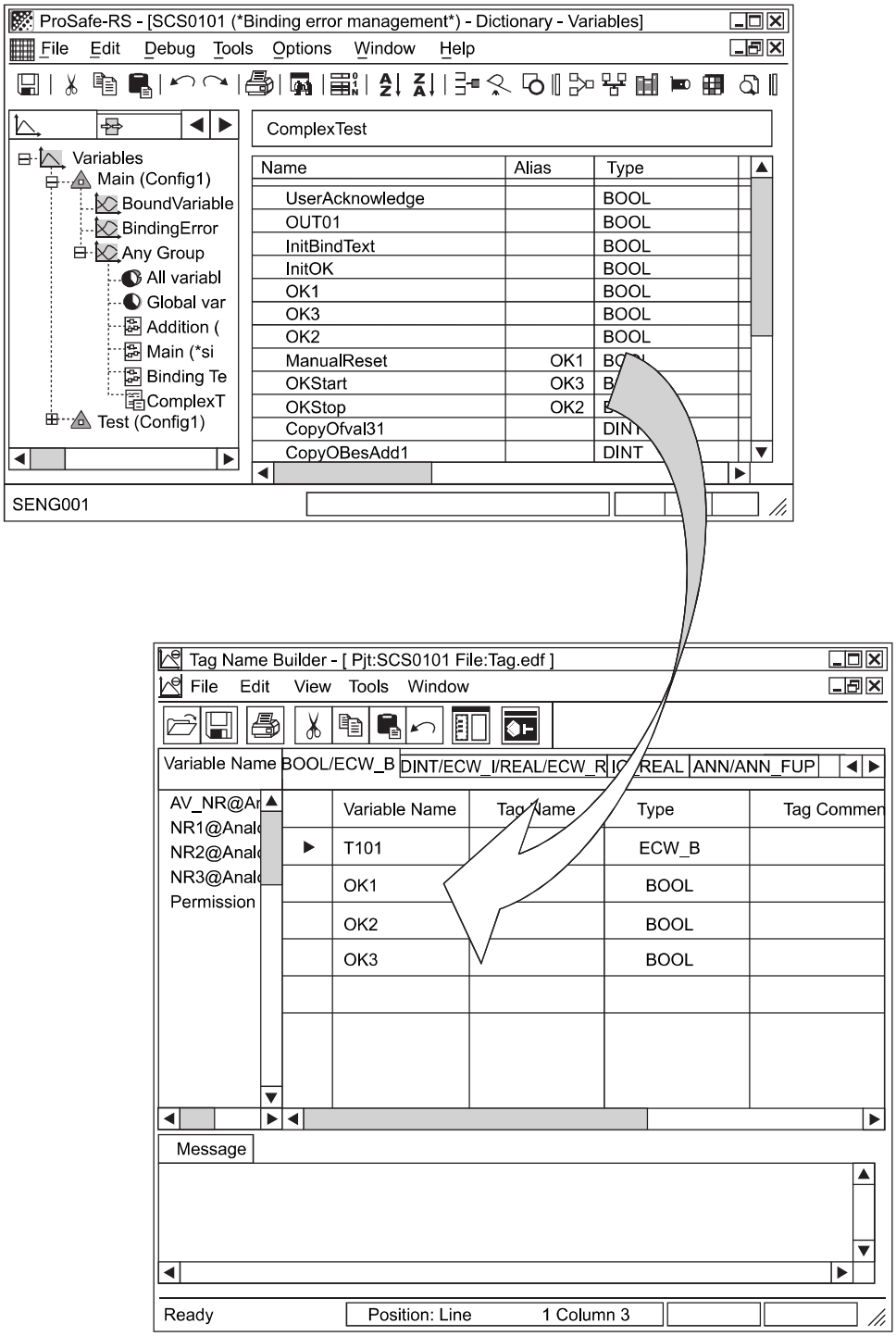


Figure B7.1.5-2 Dragging and dropping from the Dictionary View

Setting items

The following table shows the variable types for which tag names can be defined with Tag Name Builder. The setting Advanced Setting Items of Tag Name Builder vary depending on the variable type.

Table B7.1.5-1 Variable types whose tag name can be defined with the Tag Name Builder

Type	Description
BOOL	BOOL variable

Continues on the next page

Table B7.1.5-1 Variable types whose tag name can be defined with the Tag Name Builder (Table continued)

Type	Description
DINT	Integer variable
REAL	Real variable
ANLG_S	Instance of the analog input function block with data status
ANLGI	Instance of ANLGI function block
VEL	Instance of VEL function block
ANN	Instance of ANN function block
ANN_FUP	Instance of ANN_FUP function block
IO_REAL	Analog real input variable
IO_BOOL	Discrete BOOL I/O variable
GOV_B	Instance of Grouping override function block (BOOL type)
GOV_IB	Instance of Grouping override function block (discrete BOOL I/O variable)
OVR_B	Instance of Override function block (BOOL type)
OVR_I	Instance of Override function block (integer type)
OVR_R	Instance of Override function block (real type)
OVR_IR	Instance of Override function block (analog real input variable)
OVR_IB	Instance of Override function block (discrete BOOL I/O variable)
PASSWD	Instance of Password function block
ECW_B	Instance of External communication function block (BOOL type)
ECW_I	Instance of External communication function block (integer type)
ECW_R	Instance of External communication function block (real type)
SCI_B	Instance of Subsystem communication function block (BOOL type input variable)
SCO_B	Instance of Subsystem communication function block (BOOL type output variable)
SCI_I	Instance of Subsystem communication function block (integer type input variable)
SCO_I	Instance of Subsystem communication function block (integer type output variable)
SCI_R	Instance of Subsystem communication function block (real type input variable)
SCO_R	Instance of Subsystem communication function block (real type output variable)
PSI_I	Instance of Safety subsystem communication function block (integer-type fire and gas communication input)
PSI_R	Instance of Safety subsystem communication function block (real-type fire and gas communication input)
PNI_I	Instance of Safety subsystem communication function block (integer-type PROFINET communication input)
PNI_R	Instance of Safety subsystem communication function block (real-type PROFINET communication input)
MOB_11	Manual operation block instance with two-position answerback (BOOL)
MOB_21	Manual operation block instance with three-position answerback (BOOL)
MOB_RS	Manual operation block instance with auto-reset (BOOL)
MOA	Instance of Analog manual operation block
HSDTR	Instance of the analog input function block for smoke and heat detectors
GASDTR	Instance of the analog input function block for gas and flame detectors

The following table shows the setting items for Tag Name Builder and whether each setting item can be changed online. The table also shows the reference-only items in addition to the setting items. The reference items cannot be changed with Tag Name Builder. All items can be printed.

Table B7.1.5-2 Items

Item	Online changes (*1)	Remarks
Variable Name	Yes	-
Element Name	No	This item is only displayed in the ANN/ANN_FUP tab. (For SCSP1/SCSV1: %AN0001 to %AN1000, for SCSP2/SCSP3/SCSL2: %AN0001 to %AN2000) For annunciator with tag name, [T] is attached after the element name. (Example: %AN0100[T])
Type	No	The variable type defined in Dictionary View is displayed. This item is not displayed in the tab pages for a single variable type.
Comment	No	A comment for the applicable variable defined in Dictionary View is displayed.
Wiring Position	No	The installation position of the channel that is wired to an I/O variable is displayed.
Tag Name	Yes	Even if the tag name field is left blank, ANN or ANN_FUP can be accessed from CENTUM by using its element name. With no tag name specified, nothing is printed for the tag name.
Tag Comment	Yes	-
Annunciator Message	Yes	-
Low Limit	Yes	-
High Limit	Yes	-
Unit	Yes	-
Level	Yes	-
Label	Yes	-
Button 1	Yes	-
Button 2	Yes	-
Button Top	Yes	-
Button Bottom	Yes	-
Switch Position Label	Yes	-

*1: Yes: Online changeable
-: Not applicable

The following table shows the advanced setting items for Tag Name Builder and whether each setting item can be changed online. To display the items, in the View menu, place a check mark next to Detailed Setting Items.

Table B7.1.5-3 Advanced setting items

Item	Online changes (*1)	Remarks
Tag Mark	Yes	-
Alarm Level	Yes	Specify a value of 1 to 16.
Upper Window	Yes	Set the upper window created on the CENTUM.

Continues on the next page

Table B7.1.5-3 Advanced setting items (Table continued)

Item	Online changes (*1)	Remarks
Help	Yes	Set the help message created using CENTUM Help Builder.
Scale Reverse	Yes	-
Scale-division	Yes	-
Double Authentication	Yes	-
Alarm in Overriding	Yes	-
Answer back Alarm	Yes	-
Password ON Alarm	Yes	-
Output High Limit	Yes	-
Output Low Limit	Yes	-
Output Scale High Limit	Yes	-
Output Scale Low Limit	Yes	-
Time to Chattering Recovery Notice	Yes	-
Upper Equipment Name	Yes	-
Switch Color Change Part	Yes	-
Operation Guard	Yes	-
Flashing when prompt for Acknowledgment	Yes	-
Color Change after Acknowledgment	Yes	-
Color Change Area	Yes	-
Use of Button	Yes	-
Button Label	Yes	-
Button Color (Normal)	Yes	-
Button Color (Resetting)	Yes	-
Operation Guard Color	Yes	-

*1: Yes: Online changeable

The following table shows the setting items for each variable type:

Table B7.1.5-4 Variable types and setting items (1/2)

Setting item	Variable type (*1)							
	BOOL ECW_B	DINT REAL ECW_I ECW_R	ANLG_S ANLGI	VEL	ANN ANN_FUP	IO_REAL	IO_BOOL	GOV_B GOV_IB OVR_B OVR_IB
Variable Name	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tag Name	Yes	Yes	Yes	Yes	Yes (*2)	Yes	Yes	Yes
Tag Comment	Yes	Yes	Yes	Yes	-	Yes	Yes	Yes
Annunciator Message	-	-	-	-	Yes	-	-	-
Low Limit	-	-	Yes	Yes	-	-	-	-

Continues on the next page

Table B7.1.5-4 Variable types and setting items (1/2) (Table continued)

Setting item	Variable type (*1)							
	BOOL ECW_B	DINT REAL ECW_I ECW_R	ANLG_S ANLGI	VEL	ANN ANN_FUP	IO_REAL	IO_BOOL	GOV_B GOV_IB OVR_B OVR_IB
High Limit	-	-	Yes	Yes	-	-	-	-
Unit	-	Yes	Yes	Yes	-	Yes	-	-
Level	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Label	Yes	-	-	-	Yes	-	Yes	Yes
Button 1	Yes	-	-	-	-	-	Yes	-
Button 2	Yes	-	-	-	-	-	Yes	-
Button Top	-	-	-	-	-	-	-	Yes
Button Bottom	-	-	-	-	-	-	-	Yes
Switch Position Label	Yes	-	-	-	Yes	-	Yes	Yes

*1: Yes: Can be set
-: Setting item not available
*2: Tag name specification is not required (even if a tag name is not defined, the variable can still be accessed from HISs using an element number).

Table B7.1.5-5 Variable types and setting items (2/2)

Setting item	Variable type (*1)							
	OVR_I OVR_R OVR_IR	PASSWD	SCI_B SCO_B	SCI_I SCO_I SCI_R SCO_R PNI_I PNI_R PSI_I PSI_R	MOB_11 MOB_21	MOB_RS	MOA	HSDTR GASDTR
Variable Name	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tag Name	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tag Comment	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Annunciator Message	-	-	-	-	-	-	-	-
Low Limit	-	-	-	-	-	-	-	Yes
High Limit	-	-	-	-	-	-	-	Yes
Unit	Yes	-	-	Yes	-	-	-	Yes
Level	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Label	Yes	Yes	Yes	-	Yes	Yes	-	-
Button 1	-	-	Yes	-	-	-	-	-
Button 2	-	-	Yes	-	-	-	-	-
Button Top	Yes	Yes	-	-	Yes	Yes	-	-

Continues on the next page

Table B7.1.5-5 Variable types and setting items (2/2) (Table continued)

Setting item	Variable type (*1)							
	OVR_I OVR_R OVR_IR	PASSWD	SCI_B SCO_B	SCI_I SCO_I SCI_R SCO_R PNI_I PNI_R PSI_I PSI_R	MOB_11 MOB_21	MOB_RS	MOA	HSDTR GASDTR
Button Bottom	Yes	Yes	-	-	Yes	Yes	-	-
Switch Position Label	Yes	Yes	Yes	-	Yes	Yes	-	-

*1: Yes: Can be set
-: Setting item not available

Table B7.1.5-6 Variable types and advanced setting items (1/2)

Setting item	Variable type (*1)							
	BOOL ECW_B	DINT REAL ECW_I ECW_R	ANLG_S ANLGI	VEL	ANN ANN_FUP	IO_REAL	IO_BOOL	GOV_B GOV_IB OVR_B OVR_IB
Tag Mark	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Alarm Level	-	-	Yes	Yes	Yes	-	-	Yes
Upper Window	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Help	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scale Reverse	-	-	Yes	Yes	-	-	-	-
Scale-division	-	-	Yes	Yes	-	-	-	-
Double Authen-ti-cation	-	-	-	-	-	-	-	Yes
Alarm in Over-riding	-	-	-	-	-	-	-	Yes
Answer back Alarm	-	-	-	-	-	-	-	Yes(*2)
Password ON Alarm	-	-	-	-	-	-	-	-
Output High Limit (%)	-	-	-	-	-	-	-	-
Output Low Limit (%)	-	-	-	-	-	-	-	-
Output Scale High Limit (%)	-	-	-	-	-	-	-	-
Output Scale Low Limit (%)	-	-	-	-	-	-	-	-
Time to Chat-tering Recov-ery Notice	-	-	Yes	-	-	-	-	-
Upper Equip-ment Name	-	-	Yes	Yes	Yes	-	-	Yes
Switch Color Change Part	-	-	-	-	-	-	-	-

Continues on the next page

Table B7.1.5-6 Variable types and advanced setting items (1/2) (Table continued)

Setting item	Variable type (*1)							
	BOOL ECW_B	DINT REAL ECW_I ECW_R	ANLG_S ANLGI	VEL	ANN ANN_FUP	IO_REAL	IO_BOOL	GOV_B GOV_IB OVR_B OVR_IB
Operation Guard	-	-	-	-	-	-	-	-
Flashing when prompt for Acknowledgment	-	-	-	-	-	-	-	-
Color Change after Acknowledgment	-	-	-	-	-	-	-	-
Color Change Area	-	-	-	-	-	-	-	-
Use of Button	-	-	-	-	-	-	-	-
Button Label	-	-	-	-	-	-	-	-
Button Color (Normal)	-	-	-	-	-	-	-	-
Button Color (Resetting)	-	-	-	-	-	-	-	-
Operation Guard Color	-	-	-	-	-	-	-	-

*1: Yes: Can be set
-: Setting item not available
*2: For GOV_B and GOV_IB, no setting is required.

Table B7.1.5-7 Variable types and advanced setting items (2/2)

Setting item	Variable type (*1)							
	OVR_I OVR_R OVR_IR	PASSWD	SCI_B SCO_B	SCI_I SCO_I SCI_R SCO_R PNI_I PNI_R PSI_I PSI_R	MOB_11 MOB_21	MOB_RS	MOA	HSDTR GASDTR
Tag Mark	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Alarm Level	Yes	Yes	-	-	Yes	Yes	Yes	Yes
Upper Window	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Help	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scale Reverse	-	-	-	-	-	-	-	Yes
Scale-division	-	-	-	-	-	-	-	Yes
Double Authenti-cation	Yes	Yes	-	-	Yes	Yes	Yes	Yes
Alarm in Overriding	Yes	-	-	-	-	-	-	-
Answer back Alarm	Yes	-	-	-	Yes	Yes	-	-
Password ON Alarm	-	Yes	-	-	-	-	-	-

Continues on the next page

Table B7.1.5-7 Variable types and advanced setting items (2/2) (Table continued)

Setting item	Variable type (*1)							
	OVR_I OVR_R OVR_IR	PASSWD	SCI_B SCO_B	SCI_I SCO_I SCI_R SCO_R PNI_I PNI_R PSI_I PSI_R	MOB_11 MOB_21	MOB_RS	MOA	HSDTR GASDTR
Output High Limit (%)	-	-	-	-	-	-	Yes	-
Output Low Limit (%)	-	-	-	-	-	-	Yes	-
Output Scale High Limit (%)	-	-	-	-	-	-	-(*2)	-
Output Scale Low Limit (%)	-	-	-	-	-	-	-(*3)	-
Time to Chattering Recovery Notice	-	-	-	-	-	-	-	Yes
Upper Equipment Name	Yes	Yes	-	-	Yes	Yes	Yes	Yes
Switch Color Change Part	-	-	-	-	-	-	-	Yes
Operation Guard	-	-	-	-	-	-	-	Yes
Flashing when prompt for Acknowledgment	-	-	-	-	-	-	-	Yes
Color Change after Acknowledgment	-	-	-	-	-	-	-	Yes
Color Change Area	-	-	-	-	-	-	-	Yes
Use of Button	-	-	-	-	-	-	-	Yes
Button Label	-	-	-	-	-	-	-	Yes
Button Color (Normal)	-	-	-	-	-	-	-	Yes
Button Color (Resetting)	-	-	-	-	-	-	-	Yes (*4)
Operation Guard Color	-	-	-	-	-	-	-	Yes

*1: Yes: Can be set
-: Setting item not available
*2: Fixed to 100.0. For display purpose only.
*3: Fixed to 0.0. For display purpose only.
*4: This setting item is applied only when HSDTR is used and is not applied when GASDTR is used.

Variable Name

To assign a tag name to a function block instance, enter the [instance name] as the variable name. From among the variables created in SCS Manager, specify the variable name you want to assign a tag name. A tag name can be defined regardless of the scope of the variable.
In case of a local variable, enter a scope name after "@."

In case of an internal variable of a user-defined function block, assign an instance name using Dictionary View of SCS Manager. The variable name is specified in the format of "[Instance Name].[Internal Variable Name]." Up to two nests are permitted in each variable to which a tag name is assigned.

Table B7.1.5-8 Examples of variable specification

Variable name (*1)	Scope	Description
VAR1	Global	Global variable
VAR2@PROG1	PROG1	Local variable of PROG1 function
FB01.VAR3	Global	Internal variable VAR3 of user-defined function block instance FB01
FB01.VAR3@PROG1	PROG1	Internal variable VAR3 of user-defined function block instance FB01 defined locally in PROG1 function
FB01.FB2.VAR3	Global	Internal variable VAR3 of user-defined function block instance FB2, which is used in user-defined function block instance FB01 (maximum limit of function block nesting)

*1: The variable name can contain up to 69 single-byte characters. Tag Name Builder also checks the following items:
- The variable name consists only of alphanumeric characters and "@," "." or "_". If any other character is used, an error will occur.
- The variable name begins with an alphabetic character or "_"; otherwise, an error will occur.
- Three or more nests in a variable will result in an error. The variables "FB01.VAR3" and "FB01.VAR3@PROG1" have one nest, while "FB01.FB2.VAR3" has two nests.

Tag Name

A name used to access each application logic variable from HIS. A tag name can contain up to 16 single-byte alphanumeric characters including "_" and "-". Note that tag names cannot begin with "_" or "-". All characters are converted to uppercase as they are entered. Tag names must be unique within the CENTUM project .

Tag Comment

A comment assigned to a tag name. It can be defined within 24 single-byte characters.

Annunciator Message

A message notifying the process error. You can define any string within 80 single-byte characters.

Default: None

Unit

A symbol indicating the engineering unit of data such as flow rate and pressure. A unit can be defined within 6 single-byte characters .

Default: %

Low Limit

A low limit (SL) is the lowest point of engineering data scale. It can be defined using up to seven digits including a sign and decimal point. This setting is referenced by HIS only for display purposes and not used in calculation or alarm processing of the SCS.

Default: 0.0

High Limit

A high limit (SH) is the highest point of engineering data scale. It can be defined using up to seven digits including a sign and decimal point. This setting is referenced by HIS only for display purposes and not used in calculation or alarm processing of the SCS.

Default: 100.0

Label

A display format applied to the switch position label displayed on each button on the instrument faceplates of HIS. Two label formats are available: Direct and Reverse. Either type can be specified.

Table B7.1.5-9 Label

Number	Description
1	Direct
2	Reverse

Default: Direct

Button 1/Button 2

A button color can be specified for each button on the instrument faceplates of HIS.

Select a button color from one of the following 16 colors:

R: Red N: Black G: Green Y: Yellow B: Blue M: Magenta C: Cyan W: White SB: Steel Blue PK: Pink SG: Spring Green OR: Orange YG: Yellow Green VO: Violet DB: Deep Sky Blue GR: Gray

When each button (switch) is pressed, the button color will change to the specified color.

Default: Red

Button Top/Button Bottom

Each button on the instrument faceplates of HIS can be divided into the top and bottom sections and its color can be specified for each section. Sixteen colors are available, corresponding to the colors shown in "Button 1/Button 2" above, except for "N: Black," which is substituted by "N: Background color."

Level

Variables can be classified according to their priorities. Eight levels from 1 to 8 are available, and the security level increases as the number increases. The operation and monitoring privileges on the HIS with respect to each data item will change depending on the function constraint level. Enter a number between 1 and 8.

Default: 4

SEE ALSO For more information about levels, refer to:

- 3.4, "Function Block Security" in the CENTUM VP Engineering Reference Vol. 1 (IM 33J10D10-01EN)
- 3.4, "Function Block Security" in the CENTUM VP Engineering Reference Vol. 1 (IM 33K03G21-50E)

Switch Position Label

A label displayed on each button on the HIS instrument faceplates. Switch position labels 1 to 4 can be defined using up to eight single-byte or four double-byte characters. However, the following characters cannot be used:

, (comma), | (vertical bar), ' (single quotation), " (double quotation), \ (back slash), and #

Default: ON,,OFF,ON

Tag Mark

A tag mark indicating the tag name priority and process status. The following four tag name priorities are available:

- Important
- General
- Aux.1
- Aux.2

For each tag name, alarm confirmation mode can be set as either "with acknowledgement (with Ack)" or "without acknowledgement." You can select from the following eight types of combinations of priority levels and confirmation modes. Enter a number from 1 to 8.

Table B7.1.5-10 Tag marks

Number	Type	
1	Important with Ack.	Important tag with acknowledgement
2	General	General tag
3	Aux.1	Auxiliary tag 1
4	Aux.2	Auxiliary tag 2
5	Important	Important tag
6	General with Ack.	General tag with acknowledgement
7	Aux.1 with Ack.	Auxiliary tag 1 with acknowledgement
8	Aux.2 with Ack.	Auxiliary tag 2 with acknowledgement

Default: 2 (General)

In some function blocks, a reconfirmation dialog box always appears if you try to change an MV.

SEE ALSO For more information about reconfirmation dialog box, refer to:

"● Reconfirmation dialog box" on page B8-13

Alarm Level

Define a processing level on an HIS for each alarm generated with respect to a given tag name. You can specify an alarm priority and display color for all alarms generated in relation to the tag name. You can select an alarm processing level from the 16 levels listed in the following table: The alarm levels 1 to 4 are fixed. Enter the number using single-byte characters.

Table B7.1.5-11 Alarm processing levels

Level	Type	Description
1	High	High-priority alarm
2	Medium	Medium-priority alarm
3	Low	Low-priority alarm
4	Logging	Logging alarm
5 … 16	User (5) … User (16)	These types are defined in the CENTUM Alarm Processing Table Builder. Equalize to the setting from the Alarm Processing Table Builders on CENTUM.

Default: 1 (High)

Upper Window

An upper window is a window that is called when the graphic button in a toolbox or graphic key on the operation keyboard is operated on HIS while a tag name is selected. The upper window can be specified for each tag name.

Default: None

Help

You can specify a number for each help message displayed on HIS. The user can define desired help messages using CENTUM Help Builder and specify a number between HW0001 and HW9999 for each of these messages. Specify the applicable number to display the help dialog box showing the corresponding help message.

Default: HW000 (No help message)

Scale Reverse

This display method causes the top of the scale shown on the instrument faceplates of HIS to become the low limit, and its bottom the high limit. Specifying "Yes" will activate reverse display. Either "Yes" or "No" can be selected.

Default: No

Scale-division

You can select 1, 2, 3, 4, 5 or 7 divisions for the scale on the instrument faceplates of HIS. You can also set "AUTO" to let the system determine the division number automatically.

Default: AUTO

Double Authentication

Use this function if you want to grant operation permission based on approvals of two users--the logged-in user and another user--when operating important tag names from an HIS. When the use of double authentication is defined, the reconfirmation dialog box with double authentication appears. Specifying "Yes" will enable double authentication. Either "Yes" or "No" can be selected.

Default: No

Alarm in Overriding

Specify whether or not to generate a process alarm to notify that a grouping override function block or an override function block is overriding. Specifying "Yes" will cause an applicable process alarm to be generated. Either "Yes" or "No" can be selected.
Default: Yes

SEE ALSO For more information about overriding alarm, refer to:

"■ Process alarm" on page B4-6

Answer-back Alarm

Specify whether the process alarm is to be generated when the Override Operation or Manual Operation from HIS does not work properly. For example, a process alarm can be generated when the Manual Operation Function Block detects discrepancy between the output signal to a valve and the answerback input value from the limit switch of the valve. You can select "Both" (answerback error on both the ON and OFF sides), "ON", "OFF" or "No".
Default: Both

Table B7.1.5-12 Option for answer-back alarm

Variable type	OVR_B, OVR_I, OVR_R, OVR_IR, OVR_IB, MOB_RS(*1)	MOB_11, MOB_12
Option	0: No 1: Both (Default)	0: No 1: Both (Default) 2: ON 3: OFF

*1: For GOV_B, GOV_IB, and PASSWD, no setting is required.

SEE ALSO For more information about answerback error alarm, refer to:

"■ Process alarm" on page B4-6

● Password ON Alarm

Specify whether or not to generate a process alarm when the PASSWD function block is outputting 1 as the result of overriding by HIS. Specifying "Yes" will cause an applicable process alarm to be generated. Either "Yes" or "No" can be selected.
Default: Yes

SEE ALSO For more information about password ON alarm, refer to:

"■ Settings in the Tag Name Builder" on page B4-21

● Output High Limit

Specify the upper output limit within the range 0.0% to 100.0%.
Default: 100.0%

● Output Low Limit

Specify the lower output limit within the range 0.0% to 100.0%
Default: 0.0%

● Output Scale High Limit

Fixed to 100.0 %.

● Output Scale Low Limit

Fixed to 0.0%.

● Time to Chattering Recovery Notice (s)

This items is used to suppress the chattering alarm.

Set the time by which to delay the display of the process alarm indicating recovery from an error of the input open (IOP). Upon recovery from an error during the alarm suppression period, the SCS monitors whether the normal status persists for the time set for this item. Alarm suppression is continued if an error occurs within the set time, and a process alarm for recovery from an error is displayed if an error does not occur.

Setting this time to 0 disables the chattering alarm suppression function.

Setting range: 0 to 120 seconds

Default: 0

IMPORTANT

- This item cannot be set to function blocks other than ANLG_S, HSDTR, and GASDTR.
- This item can be used with SCS projects created using an SENG of R4.03.00 or later where the CENTUM Integration Package is activated.

Upper Equipment Name

Specify the upper equipment name set on the CENTUM.
Default: Blank

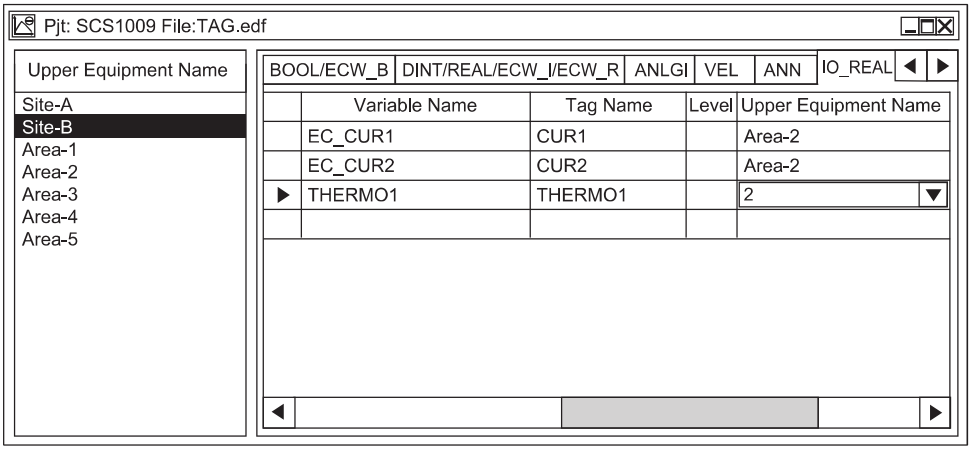


Figure B7.1.5-3 Setting of upper equipment names

Switch Color Change Part

This setting item can be specified with HSDTR and GASDTR function blocks.

Specify the parts where the display colors will change. Either Background or Characters can be selected.

Default: Background

Operation Guard

This setting item can be specified with HSDTR and GASDTR function blocks.

Specify the style for the ruled lines of the operation guard and the frame of acknowledgment. Either Dashed Line or Solid Line can be selected.

Default: Dashed Line

Flashing when prompt for Acknowledgment

This setting item can be specified with HSDTR and GASDTR function blocks.

Specify whether or not the area specified with Color Change Area will flash upon acknowledgment. Either Yes or No can be selected.

Default: Yes

Color Change after Acknowledgment

This setting item can be specified with HSDTR and GASDTR function blocks.

Specify whether or not the area specified with Color Change Area will change color upon acknowledgment. Either Yes or No can be selected.

Default: Yes

Color Change Area

This setting item can be specified with HSDTR and GASDTR function blocks.

Specify the areas that will flash and/or change color upon acknowledgment. Switch, Frame, or Both can be selected. When Switch is selected, the setting will follow the specification of Switch Color Change Part.

Default: Switch

Use of Button

This setting item can be specified with HSDTR and GASDTR function blocks.

Specify whether or not to use buttons. Either Yes or No can be selected.

Default: Yes

Button Label

This setting item can be specified with HSDTR and GASDTR function blocks.

Specify the string to be displayed in the button. This item can be defined within 8 single-byte characters or 4 double-byte characters. However, the following characters cannot be used:

, (comma), | (vertical bar), ' (single quotation), " (double quotation), \ (back slash), and #

Default: RESET

Button Color (Normal)

This setting item can be specified with HSDTR and GASDTR function blocks.

Specify the color of the button during the normal status. Select a button color from one of the following 16 colors:

R:Red N:Black G:Green Y:Yellow B:Blue M:Magenta C:Cyan W:White SB:Steel Blue PK:Pink SG:Spring Green OR:Orange YG:Yellow Green VO:Violet DB:Deep Sky Blue GR:Gray

Default: White

Button Color (Resetting)

This setting item can be specified with the HSDTR function block.

Specify the color of the button during the reset status. The colors that can be specified are the same as those for Button Color (Normal).

Default: Red

Operation Guard Color

This setting item can be specified with HSDTR and GASDTR function blocks.

Specify the color of the operation guard. The colors that can be specified are the same as those for Button Color (Normal) with the exception of Black.

Default: Red

B7.1.6 Engineering for overriding from HIS

When overriding from an HIS, use one of the following two types of function blocks:

- Grouping Override Function Blocks
- Override Function Blocks

These types of function blocks include function blocks that should be selected according to the data type of the variable to override. To manage multiple override function blocks as a group, use the grouping override function block.

SEE ALSO For more information about override using override function blocks, refer to:

I1.1, "Utilizing the forcing and override functions during maintenance" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Engineering for overriding from HIS

The engineering procedure for performing an override is as follows:

Grouping override function blocks

1. Define the grouping override function block instance.
2. Insert the grouping override function block instance that you have defined into the application logic.
3. Connect the input value for normal operation to the IN terminal. This value is output when override is not performed. Specify the value to be output during override for the VAL terminal.
4. Set the Group number of this instance in a fixed value for the GRP terminal.
5. Connect the input that permits or prohibits override to the SW terminal.

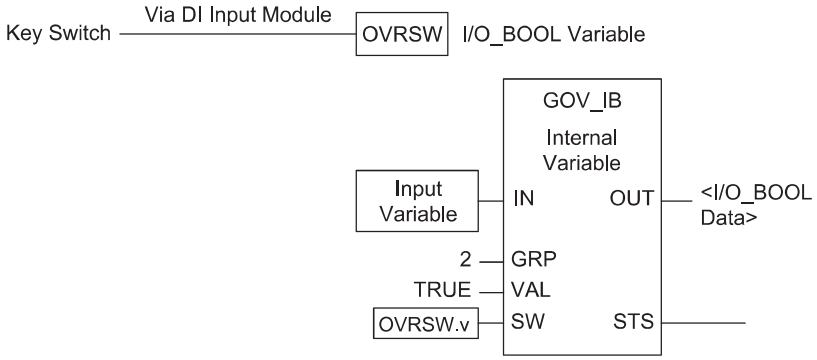


Figure B7.1.6-1 Example of grouping override function block

6. Define a tag name for the grouping override function block instance.
   You can use the tag name to perform grouping override from an HIS.

Override function blocks

1. Define the override function block instance.
2. Insert the override function block instance that you have defined into the application logic.
3. Connect the input value for normal operation to the IN terminal. This value is output when override is not performed. Specify the value to be output during override for the VAL terminal.
4. Connect the input that permits or prohibits override to the SW terminal.

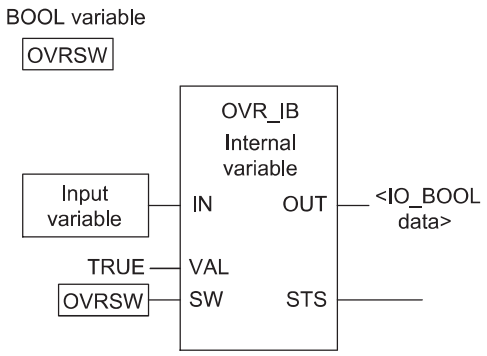


Figure B7.1.6-2 Example of override function block

5. Define a tag name for the override function block instance.
   You can use the tag name to perform override from an HIS.

Engineering for overriding using a password function block

Combining a password function block with an override function block will allow you to enable or disable override operations from an HIS using a password. The engineering procedure for connecting a password function block to a created override function block is as follows:

1. Define the password function block instance.
2. Insert the password function block instance that you have defined into the application logic.
3. Define a password string you need to enter for operation from an HIS for the password function block.
4. Search for the override function block instance to which this password function block is connected.
5. Connect the output parameter OUT of the password function block to the input parameter SW of the override function block.

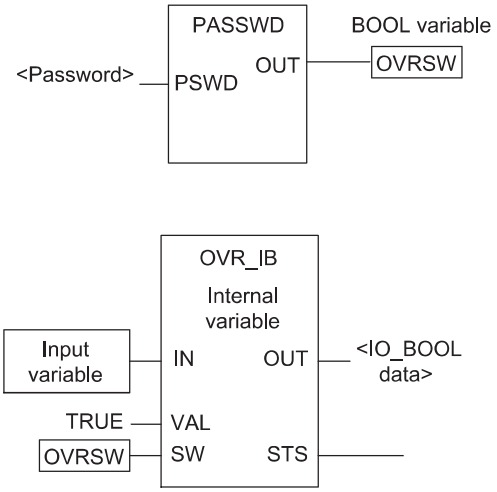


Figure B7.1.6-3 Example where a password function block is used to permit override

6. If necessary, set a password for the POU that contains the created password function block.
   This will restrict the reference to and printing of the password function block by opening the POU and prevent an unauthorized user from referencing a password.
7. Specify a tag name for the password function block instance.

SEE ALSO For more information about engineering for the password function block, refer to:

11.11, “SYS_PSWD (password function blocks management)” in POU Reference Manual (IM 32P03B20-01EN)

B7.1.7 Settings for exchanging data between FCS and SCS

For setting data from FCS to SCS, use SCS link transmission or external communication function block. The SCS link transmission allows data exchanges between FCS and SCS.

SEE ALSO For more information about SCS link transmission function, refer to:

- A6.1, “Overview of the SCS link transmission” on page A6-2
- A6., “SCS link transmission” on page A6-1

For more information about data setting from FCS, refer to:

B6., “Data setting using external communication function blocks” on page B6-1

For more information about overview of external communication function blocks, refer to:

10., “External communication function blocks” in POU Reference Manual (IM 32P03B20-01EN)

SCS link transmission

To exchange data between SCS and FCS, APCS, or GSGW, communications data must be assigned to the SCS link transmission function block. You can define the assignment using SCS Link Transmission Builder.

The engineering flow for enabling data exchanges using the SCS Link Transmission is as follows:

SEE ALSO For more information about how to use SCS Link Transmission Builder, refer to:

A6.3, “SCS link transmission definition” on page A6-11

Engineering flow for sending data from SCS to FCS

1. Open the SCS Link Transmission Builder, select SCS Link Transmission Definition, and set Send to [Yes] on the Self Station tab.
2. Define the LTSND (link transmission data output) function block.
3. In the SCS Link Transmission Builder, select the Data Wiring Definition and then the Self Station number.
   Define the LTSND function block for the bit number (bit No).
4. Place the LTSND function block in the application logic.

Engineering flow for receiving data from FCS

1. Select SCS Link Transmission Definition in the SCS Link Transmission Builder. Configure the settings as follows in the Self Station tab:
   - In the tab, set [Receive] to [Yes].
   - In the Other Stations tab, select the station number of FCS and set [Type] to [2: FCS].
2. Define the LTFCS (interference-free link transmission data input) function block.
3. In the SCS Link Transmission Builder, select the Data Wiring Definition and then the FCS station number.
   Define the LTFCS function block for the bit number (bitNo).
4. Place the LTFCS function block in the application logic.

External communication function blocks

Engineering flow

The engineering procedure for setting data using an external communication function block is as follows:

1. Define the external communication function block instance.
2. Insert the external communication function block instance defined in step 1 into the application logic.
3. Define a tag name for the instance defined in step 1.

IMPORTANT

Do not set data periodically to SCSs from PID, MLD and other regulatory control blocks or CALCU and other arithmetic/logic calculation blocks using the inter-station data link blocks (ADLs) of FCSs. Doing so can result in a writing error.

SEE ALSO For more information about data setting through a tag name interface, refer to:

B., “CENTUM integration” on page B-1

B7.1.8 Accessing subsystem's data from CENTUM

CENTUM can access the subsystem data after the names of the communication input function blocks and the communication output function blocks are defined. Moreover, CENTUM can set data to the subsystem through the external communication function blocks (ECW_*).

Reading subsystem's data by CENTUM

CENTUM can read data in the subsystem through a tag name interface.

You need to assign tag names to the instances of the function blocks for subsystem communication in advance.

The communication data read by CENTUM are logical data.

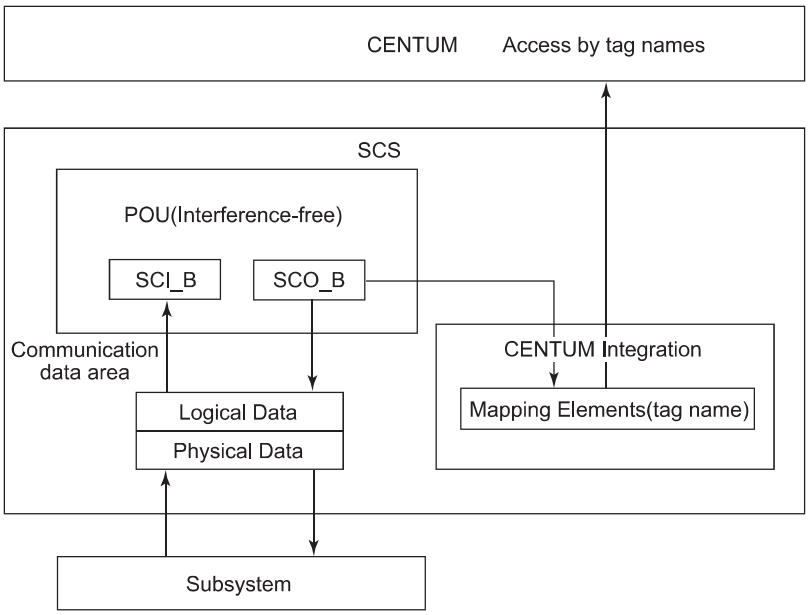


Figure B7.1.8-1 Reading subsystem's data by CENTUM

Setting subsystem's data by CENTUM

Through the external communication function block (ECW_*), CENTUM can set data in the subsystem through a tag name interface. The logic between the external communication function blocks and the subsystem communication output function blocks needs to be created.

IMPORTANT

Do not frequently set data from CENTUM to the subsystem through the external communication function blocks using tag name interfaces. Doing so can result in a writing error.

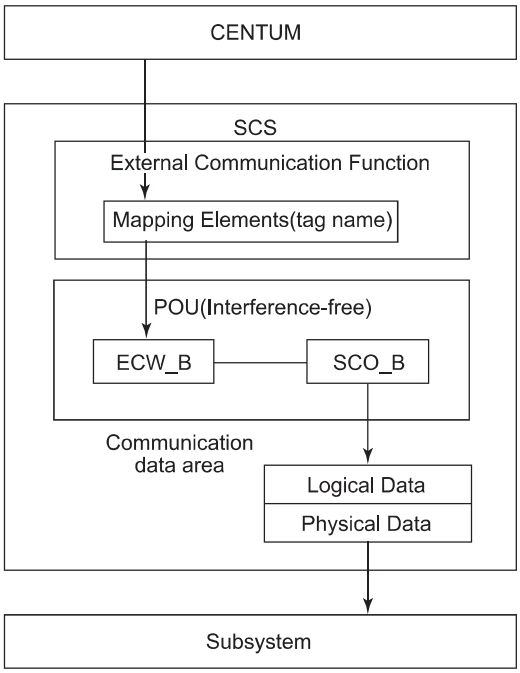


Figure B7.1.8-2 Setting subsystem's data by CENTUM

SEE ALSO

For more information about data setting using tag names, refer to:

"■ Limitations on the number of data setting requests via tag name interfaces" on page B2-2

For more information about external communication function blocks, refer to:

10., "External communication function blocks" in POU Reference Manual (IM 32P03B20-01EN)

B7.1.9 Plant hierarchy

The Plant hierarchy shows the equipment and devices on a control system in a hierarchical structure conforming to the physical model specified in the ISA S88.01. Function blocks named from the Tag Name Builder on the ProSafe-RS can be registered as equipment objects in the Plant hierarchy on the Control system. HIS is capable of filtering process alarms based on the plant hierarchy and of displaying process alarms for any equipment object.

Plant hierarchy

The mapping blocks and elements assigned with tag names can be handled as the equipment objects in CENTUM plant hierarchies. By specifying the tag names of the SCS, the process alarm filtering and security settings for operation and monitoring can be performed on HIS according to the plant hierarchy definition.

SEE ALSO For more information about plant hierarchy, refer to:

- 3, "Plant Hierarchy" in the Human Interface Stations Reference Vol. 2 (IM 33J05A11-01EN)
- 3, "Plant Hierarchy" in the Human Interface Stations Reference Vol. 2 (IM 33K03F22-50E)

Relationship of SCS tag data and SCS with plant hierarchy

An SCS and the plant hierarchy have the following relationships.

- It is possible to define upper level equipment names of an SCS at registering the SCS in System View of CENTUM.
- An equipment name which is defined in the CENTUM Plant Hierarchy Builder can be used as the upper level equipment name of the mapping block or element.
- Define the upper level equipment names when defining tag names of mapping blocks and mapping elements in the Tag Name Builder of the SENG. The upper level equipment names are managed as UAIDs (User Application IDs) within the SCS.
- The UAID of mapping blocks/elements whose upper level equipment name is not defined in the Tag Name Builder is set to 0 and the upper level equipment is set to the local SCS.

Changing UAID

- The upper level equipment names of mapping blocks and mapping elements can be changed via online change download as well. UAIDs of mapping blocks and mapping elements newly added via online change download take the values corresponding to the upper level equipment names defined in the Tag Name Builder.
- UAIDs managed by the SCS can be changed via operations from an HIS, SEBOL of FCS, and OPC.
- UAIDs cannot be changed from an SCS's application logic.

Precautions when UAIDs are changed from HIS and FCS

After changing UAID from HIS, FCS or OPC for the SCS tag name, if you perform the following operations, the inconsistency of the UAID between HIS and SCS will occur.

- Execute offline download to the SCS
- Reset and restart the SCS (when the SCS is reset and restarted, UAIDs of function blocks take the values specified by the Tag Name Builder)
- Reset and restart the HIS (when the HIS is reset and restarted, UAIDs of the tag list maintained on the HIS take the values specified by the Tag Name Builder)

IMPORTANT

If UAIDs do not match between the HIS and SCS, the security management on the HIS and process alarm filtering according to the plant hierarchy definitions no longer function correctly. If UAIDs are set from an HIS, FCS or OPC, be sure to set the UAIDs again from the HIS, FCS or OPC after SCS offline download or resetting and restarting the HIS and/or SCS.

Plant hierarchy engineering

1. Setting upper equipment names for SCS station
   When a new SCS is defined from the System View on the CENTUM ENG, the equipment object of SCS is automatically registered in the Plant hierarchy.

   Open the SCS Properties from the System View on the CENTUM ENG to specify the name of the upper equipment name than SCS.

2. Setting upper equipment name for SCS tag name
   The upper equipment name for each Mapping Block/Element on SCS can be specified from the Tag Name Builder. The specifiable upper equipment names are limited to those (Custom equipment name) defined from the Plant Hierarchy Builder on the CENTUM. You cannot specify the default equipment name.

3. Defining upper equipment
   Use the Plant Hierarchy Builder on the CENTUM ENG.

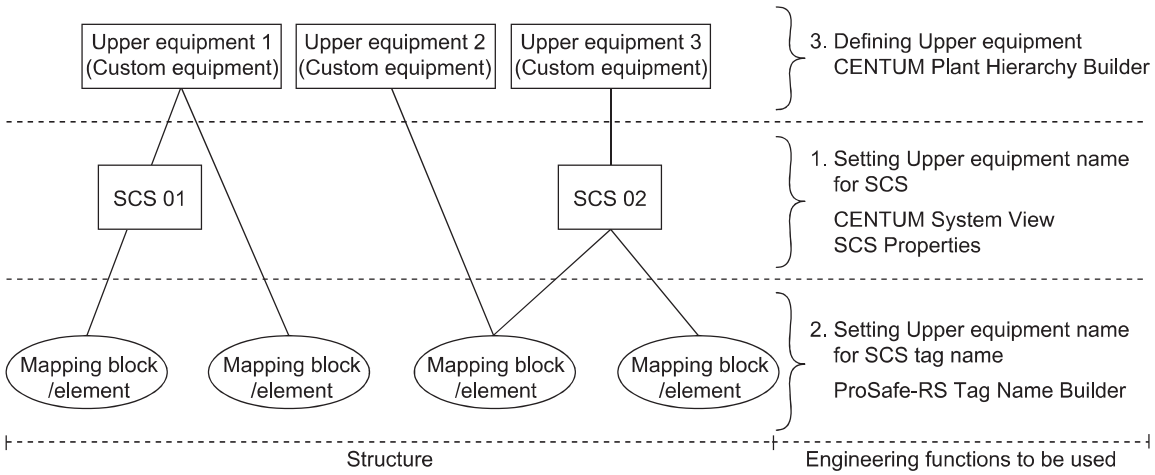


Figure B7.1.9-1 Example of SCS plant hierarchy

SEE ALSO

For more information about the plant hierarchy engineering, refer to:

- 3.2, "Plant Hierarchy Engineering" in the Human Interface Stations Reference Vol. 2 (IM 33J05A11-01EN)
- 3.2, "Plant Hierarchy Engineering" in the Human Interface Stations Reference Vol. 2 (IM 33K03F22-50E)

B7.1.10 Saving and downloading operation marks

The operation marks set for the mapping blocks or mapping elements of an SCS can be saved in an SENG. The saved operation marks can be downloaded to an SCS.

Save operation marks

The operation marks for the tagged elements and annunciators can be saved.

The operation marks can be saved by SCS Manager at any time. The dialog box that prompts for saving the operation marks will be displayed before Offline Download, Master Database Offline Download and SCS Restart. On the dialog box, choose Yes, then the operation marks will be saved.

Procedure of saving operation marks

1. On SCS Manager, choose [Tools] > [Controller] >[Save Operation Marks].
   A dialog box appears, asking you whether you want to save the operation marks.
2. Click [Yes], then saving will start with a progress bar.

Download operation marks

- The saved operation marks of the tagged data and annunciators can be downloaded.
- Only the saved operation marks of the tag names that are consistent with the tag names in the SCS can be downloaded. If the tag names are modified after saving the operation marks, the operation marks of the inconsistent tag names will not be downloaded.

IMPORTANT

- The operation marks in the SCS are initialized when you perform an Offline Download, Master Database Offline Download, or SCS manual restart, or when the SCS automatically restarts after power failure. When performing the above operations (except SCS auto restart after power failure), a dialog box will be displayed, prompting you to save the operation marks.
- For Offline Download or Master Database Offline Download, set a security password first and then download the operation marks after the SCS shifts to Waiting mode.
- For SCS Restart, download the operation marks after the SCS shifts to Waiting mode.

Procedure of download operation marks

1. On SCS Manager, choose [Tools] > [Controller] > [Download Operation Marks] to start.
   A dialog box appears, asking you whether you want to download the operation marks.
2. Click [Yes], then download will start with a progress bar.

B7.2 Engineering on the CENTUM side

This section describes engineering tasks performed on the CENTUM side, one of the tasks required to connect an SCS project and a CENTUM project.

B7.2.1 SCS creation

To connect each SCS project to a CENTUM project, a corresponding SCS must be created in CENTUM System View first.

Creating an SCS

Create SCSs on CENTUM System View. The procedure is explained in the following section:
Select [File] > [Create New] > [SCS (E)] in System View. The New Station dialog box appears.

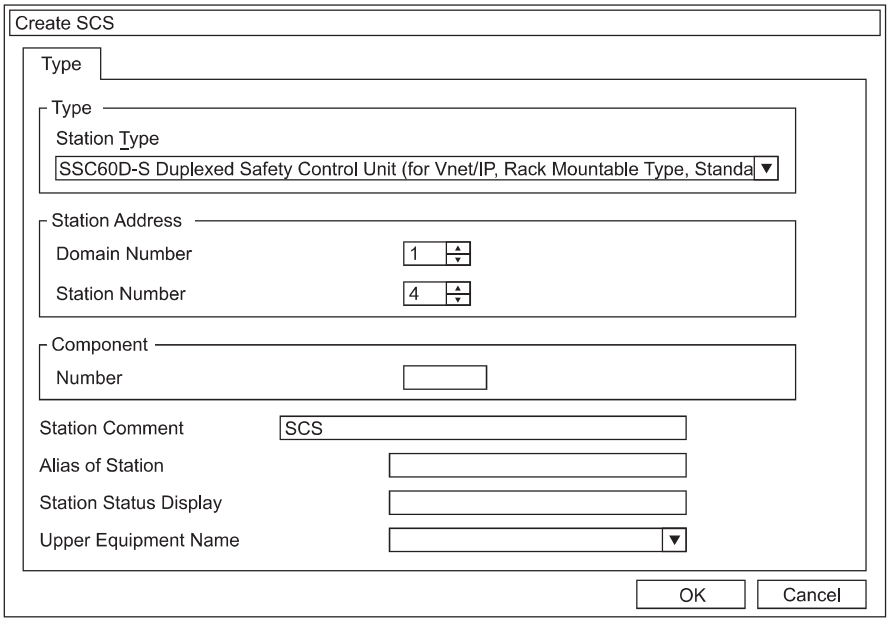


Figure B7.2.1-1 Example display of the Create SCS dialog box (Type tab)

TIP

Do not select "SCS01 Safety Control Station" as the station type.

The following section describes the items defined in each tab sheet:

Definition items in the Type tab

The following describes the items defined in Type tab. The station type and station address are mandatory.

Station Type

You can select the station type from the following choices:

Table B7.2.1-1 Station type list

Station Type
[S2SC70D-S Duplexed Safety Control Unit (for Vnet/IP and N-IO/FIO, Rack Mountable Type, Standard Type)]
[S2SC70D-F Duplexed Safety Control Unit (for Vnet/IP and N-IO/FIO, Rack Mountable Type, Wide Range Temperature Type)]
[S2SC70S-S Safety Control Unit (for Vnet/IP and N-IO/FIO, Rack Mountable Type, Standard Type)]
[S2SC70S-F Safety Control Unit (for Vnet/IP and N-IO/FIO, Rack Mountable Type, Wide Range Temperature Type)]

Continues on the next page

Table B7.2.1-1 Station type list (Table continued)

Station Type
[L1SC70D-S SIL2, Duplexed Safety Control Unit (for Vnet/IP, for FIO, Rack Mountable Type, Standard Type)]
[L1SC70D-F SIL2, Duplexed Safety Control Unit (for Vnet/IP and FIO, Rack Mountable Type, Wide Range Temperature Type)]
[L1SC70S-S SIL2, Safety Control Unit (for Vnet/IP and FIO, Rack Mountable Type, Standard Type)]
[L1SC70S-F SIL2, Safety Control Unit (for Vnet/IP and FIO, Rack Mountable Type, Wide Range Temperature Type)]
[SSC60D-S Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)]
[SSC60D-F Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)]
[SSC60S-S Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)]
[SSC60S-F Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)]
[SSC50D-S Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)]
[SSC50D-F Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)]
[SSC50S-S Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)]
[SSC50S-F Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)]
[SSC10D-S Duplexed Safety Control Unit (for Vnet, Rack Mountable Type, Standard Type)]
[SSC10D-F Duplexed Safety Control Unit (for Vnet, Rack Mountable Type, Wide Range Temperature Type)]
[SSC10S-S Safety Control Unit (for Vnet, Rack Mountable Type, Standard Type)]
[SSC10S-F Safety Control Unit (for V net, Rack Mountable Type, Wide Range Temperature Type)]

Station Address

Set the station address. A station address consists of a domain number and a station number. Although any domain number from 1 to 31 can be set for a ProSafe-RS station, set only a value between 1 and 16 when the station is used in the CENTUM integration structure. The default domain number is the number set in the project. The station number should be set from 1 to 64. The default station number is the next available blank number found in a search in ascending order from 1. Once a station address is set, it cannot be changed. The only way to change the station address is to delete the existing station and then create a new one with new address.

Component Number

You can set a component number between 0 and 9999. The setting of component number may be omitted.

Station Comment

You can set a comment for the station. The setting of station comment may be omitted. Set the comment using up to 24 single-byte or 12 double-byte characters.

Alias of Station

You can set an alias for the station.
When an alias is set, all names of the station displayed on an HIS will be replaced by the alias. Set the alias using up to eight single-byte alphanumeric characters.

Station Status Display

Set the name of the window you want to display on an HIS in place of the Station Status Display view. The name of the Station Status Display view is set using up to 16 single-byte al-

phanumeric characters. Double-click the SCS icon in the System Status Overview view to display the window set here.

Upper Equipment Name

Specify the name of the equipment located in a level above the station.
The upper equipment name should use the corresponding equipment name set in Plant Hierarchy Builder.

When a new SCS is defined, an SCS equipment object is registered in the plant hierarchy automatically. Different equipment can be specified for each Mapping Blocks/Elements of the SCS.

SEE ALSO For more information about plant hierarchy builder, refer to:

- 3.2.2, "Registering Custom Equipment (Other than Unit Equipment)" in the Human Interface Stations Reference Vol. 2 (IM 33J05A11-01EN)
- 3.2.2, "Registering Custom Equipment (Other than Unit Equipment)" in the Human Interface Stations Reference Vol. 2 (IM 33K03F22-50E)

Downloading the project common

In the CENTUM integration structure, the project common is used to build a system for operating and monitoring SCSs from HISs. So, download the project common.

In the engineering of HISs and FCSs in a CENTUM project, the common items in the project are defined as the project common (COMMON). The definitions in the project common are shared by all HISs and FCSs in the same CENTUM project. Accordingly, modifying the project common will also modify the corresponding HIS/FCS definitions.

TIP Changing the project common of a CENTUM project will not affect SCS applications.
Therefore, reengineering is not required on an SENG after the project common has been changed.

B7.2.2 SCS taglist generation

To access mapping blocks/elements on an SCS from an HIS using the corresponding tag names defined in ProSafe-RS Tag Name Builder, a taglist for the SCS must be generated on the CENTUM side. CENTUM taglists are generated using the Taglist Generation Function included in the CENTUM Engineering Function.

Generating SCS taglist on CENTUM

Launch Taglist Generation Function from System View.

1. In System View, select the SCS you want to generate a taglist for.
2. Select [Tools] > [SCS Taglist Import] from the menu.
   An HIS taglist is generated.

Taglist Generation Function generates an HIS taglist based on the corresponding SCS taglist file generated in the Engineering Function of the ProSafe-RS. If the CENTUM project is the current project, the taglist is downloaded to the HIS. The result of Taglist Builder operation appears in the message area of System View.

Engineering unit symbol and switch position label

Keep the engineering unit symbol and switch position label modes to AUTO while generating a SCS taglist.

When an SCS taglist is generated in the MANUAL model, if engineering unit symbols and switch position labels not present in the CENTUM project are included in the engineering information (taglist, etc.) of the SCS, they will not be registered in the CENTUM project, and a warning message appears as a result. In this case, register the engineering unit symbols and switch position labels that generated the warning message in the respective builders, and then generate a taglist again.

SEE ALSO For more information about mode of the engineering unit symbol and switch position label, refer to:

- 2.2, "Creating a New Project" in the CENTUM VP Engineering Reference Vol. 1 (IM 33J10D10-01EN)
- 2.2, "Creating a New Project" in the CENTUM VP Engineering Reference Vol. 1 (IM 33K03G21-50E)

Downloading a taglist

Each generated taglist can be downloaded to an HIS that requires it. Taglists can be downloaded using the TagList Down Load dialog box called from System View.

Taglist download operation

1. Select [Load] > [Download Tag-List] in System View.
   The TagList Down Load dialog box appears.

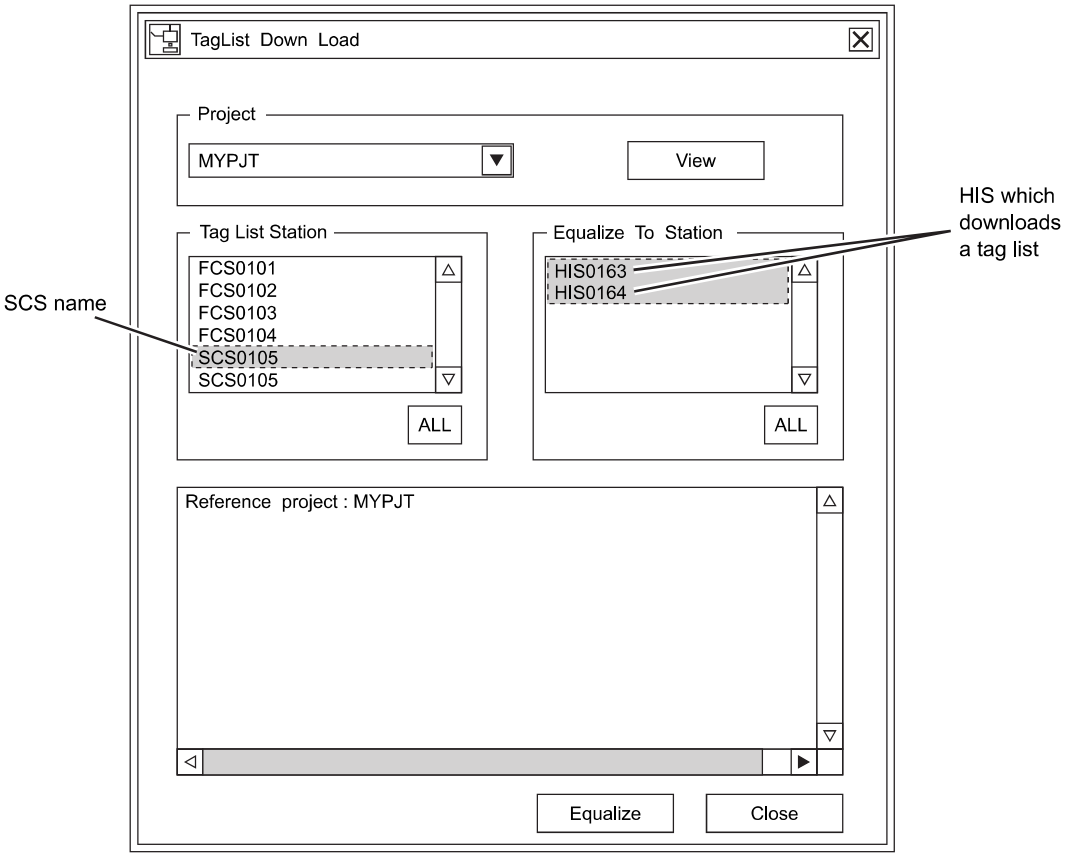


Figure B7.2.2-1 Example of the TagList Down Load dialog box

2. Select the desired project, and then click the [View] button.
   A list of stations appears.
3. Select the SCS, and the HIS you want to download the taglist to, and then click the [Equalize] button.
   The generated taglist is downloaded to the selected HIS.

Cautions after downloading database

In the CENTUM integration structure, if a database is downloaded (offline or online-change) from the SENG to SCS, be sure to generate a SCS Tag List from the System View on the CENTUM ENG. Otherwise, databases on HIS or Exaopc conflict, and trigger a system alarm message prompting you to equalize the database in the startup process of HIS or Exaopc.

B7.2.3 Other builders

To connect an SCS project with a CENTUM project, the following builders and viewer are required:

- Operation Mark Builder
- Plant Hierarchy Builder
- Plant Hierarchy Viewer
- FCS Constants Builder

Operation Mark Builder

Setting operation marks using Operation Mark Builder of the CENTUM ENG allows the assignment of tag with comment in the instrument faceplate or the change of operation privileges over mapping blocks/elements.

The definitions set in Operation Mark Builder are used commonly by all FCSs, HISs and SCSs in the CENTUM project.

If an operation mark is added or modified in Operation Mark Builder, the action of the operation mark on HISs will change once the addition/modification is downloaded to the HISs.

IMPORTANT

- The initial value of operation marks for mapping blocks/elements is 0 (no operation mark). When the SCS is restarted, the setting of operation marks will return to the initial value.
- An offline download (or master database offline download) to the SCS will cause the setting of operation marks to return to the initial value.
- Values cannot be specified for operation marks for mapping blocks/elements using the ProSafe-RS Engineering Function.
- Operation mark values cannot be changed using the SCS application logic.

SEE ALSO

For more information about operation marks, refer to:

- 3.5, "Operation Mark" in the CENTUM VP Engineering Reference Vol. 1 (IM 33J10D10-01EN)
- 3.5, "Operation Mark" in the CENTUM VP Engineering Reference Vol. 1 (IM 33K03G21-50E)

For more information about operation marks tab sheet, refer to:

- 4.3.10, "Operation Mark Tab" in the CENTUM VP Human Interface Stations Reference Vol. 1 (IM 33J05A10-01EN)
- 4.3.10, "Operation Mark Tab" in the CENTUM VP Human Interface Stations Reference Vol. 1 (IM 33K03F21-50E)

Plant Hierarchy Builder

Use the Plant Hierarchy Builder for registering Custom equipment. To activate the Plant Hierarchy Builder, in the System Engineering function, bring up the System View. In the List view, double click [Common] > [Custom Plant].

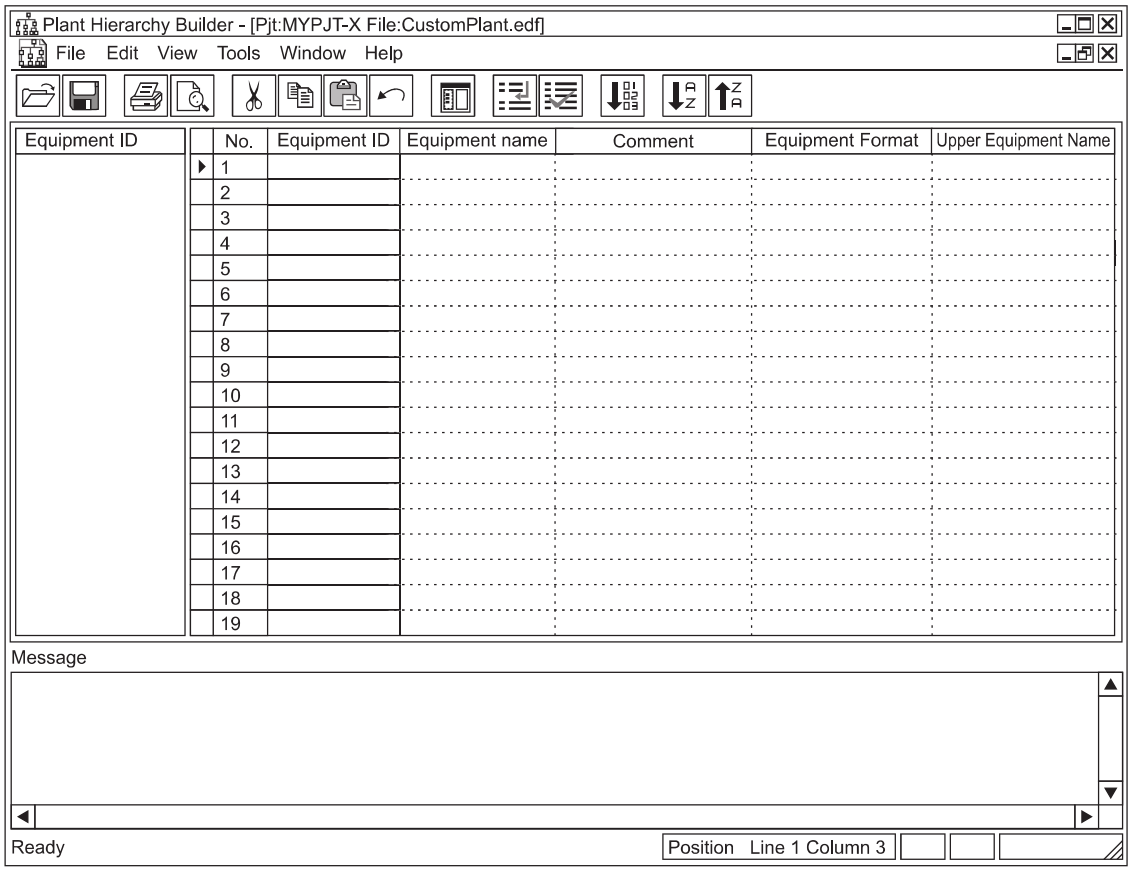


Figure B7.2.3-1 Plant Hierarchy Builder

Plant Hierarchy Viewer

In the Plant Hierarchy Viewer, you can confirm the custom equipment name registered from the Plant Hierarchy Builder. The Plant Hierarchy Viewer shows the plant hierarchy of the entire projects.
From the menu on the System View window on the CENTUM ENG, select [Tool] > [Plant Hierarchy Viewer]. SCS tags are shown in the Plant Hierarchy Viewer window.

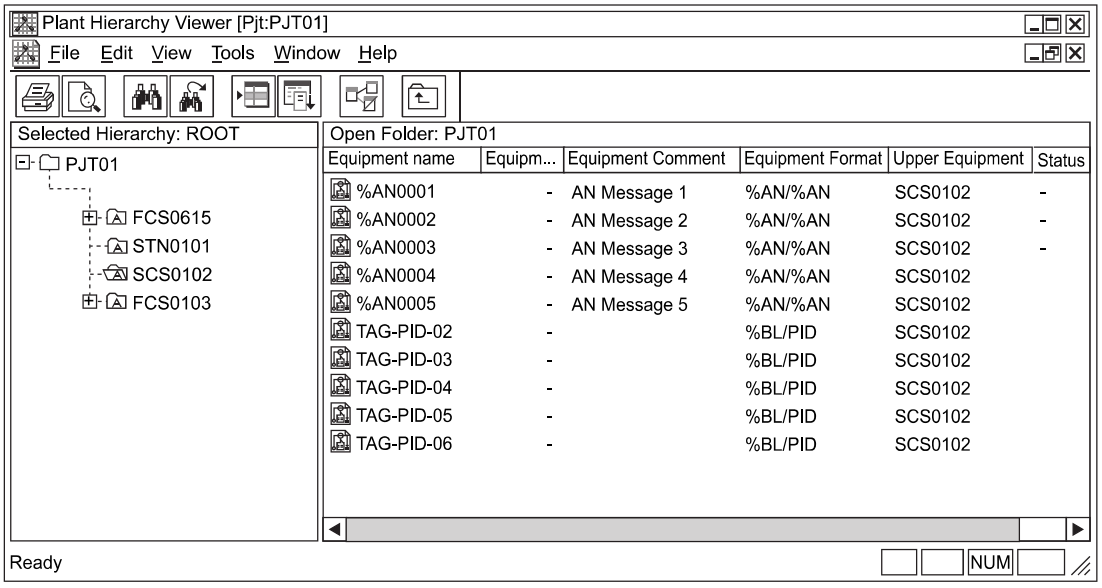


Figure B7.2.3-2 Example of Plant Hierarchy Viewer in R3.08 or later

SEE ALSO For more information about plant hierarchy viewer, refer to:

- 3.3, "Plant Hierarchy Viewer" in the Human Interface Stations Reference Vol. 2 (IM 33J05A11-01EN)
- 3.3, "Plant Hierarchy Viewer" in the Human Interface Stations Reference Vol. 2 (IM 33K03F22-50E)

FCS Constants Builder

If SCS exchanges data with FCS using the SCS link transmission, set present station definition and station definition of scan transmission definition.

The SCS data that can be referenced at FCS are %GS001 to %GS128.

SEE ALSO For more information about scan transmission definition settings in the FCS Constants Builder, refer to:

- "Scan Transmission Definitions" in A4.2, "Global Switch" in the Field Control Stations Reference (IM 33J15A10-01EN)
- "Scan Transmission Definitions" in A4.2, "Global Switch" in the Field Control Stations Reference (IM 33K03E10-50E)

B7.2.4 Items to note on CENTUM engineering

This section describes the items to be noted in CENTUM engineering.

■ Software I/Os supported on SCS

Among the various software I/Os of CENTUM FCS, common switches and annunciators can be used on SCS.

● Common switches

The SCS common switches having an element number between %SW0001 and %SW0400 are system common switches. The system common switches are elements having a predefined purpose, such as identification of SCS status. All common switches of SCSs are system common switches.

Tag names cannot be defined for SCS common switches. Also, values cannot be set in common switches.

SEE ALSO For more information about details of each SCS common switch element number, refer to:

"■ Software inputs/outputs" on page B1-2

● Annunciators

Annunciators are used as mapping elements for ANN and ANN_FUP function blocks. Each message can be defined using up to 80 single-byte or 40 double-byte characters.

Annunciators are either with or without tag names.

- Annunciators
  Annunciators can display a message of up to 80 single-byte or 40 double-byte characters.
- Annunciators with tag names
  Annunciators with tag names can display a message of 24 single-byte characters and tag names.

The user can decide the first number of an annunciator with a tag name. In the Tag Name Builder, the numbers that precede the first number define the area assigned to annunciators, while the first number and all the numbers that follow the first number define the area assigned to annunciators with tag names.

TIP An annunciator with tag names can be used in SCS projects that are created in ProSafe-RS R4.01 or later.

■ Data setting from FCS to SCS

Using SFC (Sequential Function Chart) can set data from FCS to SCS.

All the SCS data are accessible by assigning the tag names to the mapping elements on the Tag Name Builder of SENG. And the SCS data can be written from FCS by assigning the data to the external communication function blocks.

SEE ALSO For more information about data setting from FCS, refer to:

- B7.1.7, "Settings for exchanging data between FCS and SCS" on page B7-32
- B6.1, "Confirmation of setting data" on page B6-2
- "■ Functions in CENTUM integration structure" on page B2-1

The first number of annunciator message with tag name

You can assign annunciators and annunciators with tag names in the annunciator message storage area.

To assign area to annunciator messages and annunciator messages with tag names, you need to set the first number of annunciator message with tag name (%AN). The number from the first number that is set to the largest number of annunciator message can be used for an annunciator message with tag name.

Setting range: 0 to 1000 (SCSP1/SCSU1), 0 to 2000 (SCSP2/SCSP3/SCSL2)

Initial setting: 0

IMPORTANT

If the first number is 1 or greater, then that number and all the following numbers will be used as annunciator messages with tag names.

If the first number is 0, the entire message can be used as an annunciator message.

SEE ALSO For more information about configuring the annunciator message with tag name, refer to:

"● The first number of annunciator messages with tag name" in "■ Settings with the Communication Tab" in C1.2.6, "SCS Constants Builder" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Precautions on Annunciators with tag names

- Maximum 80 single-byte characters can be recorded as an annunciator message with tag name, while the first 24 characters are output as message. If your message is longer than 24 characters, you need to use an annunciator message.
- If the 24th character of a single-byte string is a double byte character, the first 23 characters are displayed.
- To use an existing annunciator message as an annunciator with tag name, you need to specify "The first number of the annunciator message with tag name (%AN)", and execute the build. The messages with the specified number and higher numbers get converted to annunciator messages with tag names.
- When using iDefine, mixed use of annunciator messages and annunciator messages with tag name is not allowed. You must define all annunciators as either annunciator messages or annunciator messages with tag name.
- Even if you are defining annunciator messages with tag name by using iDefine, you must specify "The first number of the annunciator message with tag name (%AN)."

Precautions when integrated with CENTUM or connected with Exaopc

In a CENTUM Integration environment, a communication error (No. 0301 control bus communication error) may be alerted with CENTUM HIS after the SCS starts up until the operating mode transitions to Waiting Mode. Similarly, a communication error may be alerted with an OPC server on which Exaopc or Exaopc OPC Interface Package (for HIS) is installed.

This alarm is alerted until the transition to Waiting Mode because the SCS does not respond to communication from other stations. As this is merely a transitional alarm alerted upon starting the SCS, you do not need to respond to this alarm.

B8. Overview of safety system operation and monitoring using HIS

In the CENTUM integration structure, HIS can operate and monitor SCS data through tag names in the same interface as that of FCS data. Because SCS application logic is created with IEC 61131-3 language, it is necessary to define mapping blocks/elements in the SCS and assign tag names with Tag Name Builder to realize the tag name interface. In addition, it is possible to monitor the SCS status and alarms by HIS standard windows.

SEE ALSO For more information about mapping blocks/elements, refer to:

B3., “Tag name interfaces for CENTUM” on page B3-1

Overview of safety system operation and monitoring using HIS

The following outlines the operation and monitoring of an SCS by an HIS in the CENTUM integration structure.

- Operate and monitor SCS data using tag names via the same interface used for operating and monitoring FCS data. Data can be referenced using the instrument faceplate, and SCS data can be displayed in the Graphic view.
- Monitor in HIS's Process Alarm view both occurrence and recover of process alarms and annunciators detected by SCSs.
- Monitor in HIS's System Alarm view all system alarms occurred on SCS.
- Display in HIS's SCS Station Status Display view the operating status of SCS.
- Override the application logic variables from HIS.
- Set the outputs of the application logics form HIS.

Windows used for operation and monitoring of SCS

The following windows are mainly used for operation and monitoring of SCSs from an HIS:

Table B8-1 Windows used for operation and monitoring of SCS

Window name	Description
System Alarm view	Check system alarms generated on SCSs
Process Alarm view	Check process alarms and annunciator messages generated on SCSs
SCS Station Status Display view	Monitor the operating status of SCSs
Instrument faceplate	Operate and monitor SCSs using the instrument faceplates of mapping blocks/elements
Graphic view	Monitor the data of mapping blocks/elements

The following functions can be implemented from an HIS using the above windows:

- Learn SCS alarms in real time
- Check the status of each SCS controller
- Perform maintenance override of SCSs from an HIS

Notes on online change

While operating a grouping override function block, override function block, or password function block from an HIS, do not perform online change download.

Even if the function blocks and mapping blocks that are not the targets of online change are operated from HIS, an error may occur during operation of the grouping override function block, override function block, or password function block from HIS. In this case however, the online change communication is not affected. Wait for the communication for online change to end, and then operate the grouping override function block, override function block or password function block again.

Error notification method

If an operation from HIS generates an error while online change download is running, you are notified in the following ways:

- Notification by a system alarm
- Notification by answerback error alarm (if notification of answerback error alarm is enabled in the detailed definitions for the tag)

SEE ALSO For more information about definitions of answerback errors in Tag Name Builder, refer to:

"■ Setting items" on page B7-14

B8.1 Windows used for operation and monitoring of SCS

This section describes the primary windows used in the operation and monitoring of SCSs from an HIS.

B8.1.1 System Alarm view

The System Alarm view displays a list of diagnostic information messages that notify hardware and communication errors in the system as system alarm messages. The system alarm messages are predefined in the system.

SEE ALSO For more information about System Alarm view, refer to:

- 4.2, "System Alarm View" in the Human Interface Stations Reference Vol. 1 (IM 33J10D10-01EN)
- 4.2, "System Alarm View" in the Human Interface Stations Reference Vol. 1 (IM 33K03F21-50E)

Overview of the System Alarm view

The System Alarm view displays and manages the system alarm information notified by SCSs and FCSs as system alarm messages. Both SCS and FCS system alarm messages can be displayed in the same window.

When an SCS detects an error by its diagnostic functions, the SCS issues a system alarm message. When the error is recovered, a recovery message is issued. Each SCS also issues a system alarm as a confirmation of an operation performed to the SCS, such as security level change or forcing of variables. The System Alarm view displays these messages as system alarms. The following is an overview of the System Alarm view:

- When an alarm has occurred in SCS, the [SCS Alarm occurrence Notification] button on the toolbar changes to notify the occurrence of an SCS alarm. When the button is clicked, the message is displayed after being filtered by the Safety Control Station filter.
- Once the operator acknowledges the system alarm, the system alarm message will stop flashing.
- When the system alarm is cleared, the corresponding system alarm message is deleted from the window.
- The corresponding alarm class information managed by the SCS is displayed together with each system alarm.
- System alarm messages generated on SCSs can be filtered into a separate group for display. This function allows for easy distinction of SCS alarms from FCS alarms even when a large number of system alarm messages have been generated on FCSs.
- If SCS alarms are present, calling the System Alarm view will automatically filter the alarm messages by the Safety Control Station filter before the window is displayed.

Selection of display items

Call the Window Setting dialog box from the applicable tool button in the System Alarm view. When this dialog box is first opened, the Display Item name check box is unchecked. Checking this box will enable the selection of items you want to display in the System Alarm view.

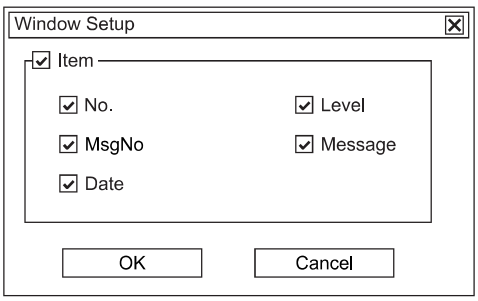


Figure B8.1.1-1 Window Setup dialog box

The following table shows the default display items in the System Alarm view and items that can be displayed or hidden.

Table B8.1.1-1 Display items in the System Alarm view

Display item name	Default window setting	Selection
Item	Displayed	Yes
MsgNo	Displayed	Yes
Date	Displayed	No
Level(*1)	Not displayed	Yes
Message	Displayed	No

*1: The displayed level corresponds to the SCS alarm class (1 to 4).

Split display

The System Alarm view can be displayed into two frames.

When a filter is set, the view is split horizontally, with the messages matching the filter condition displayed in the top frame and all messages displayed in the bottom frame.

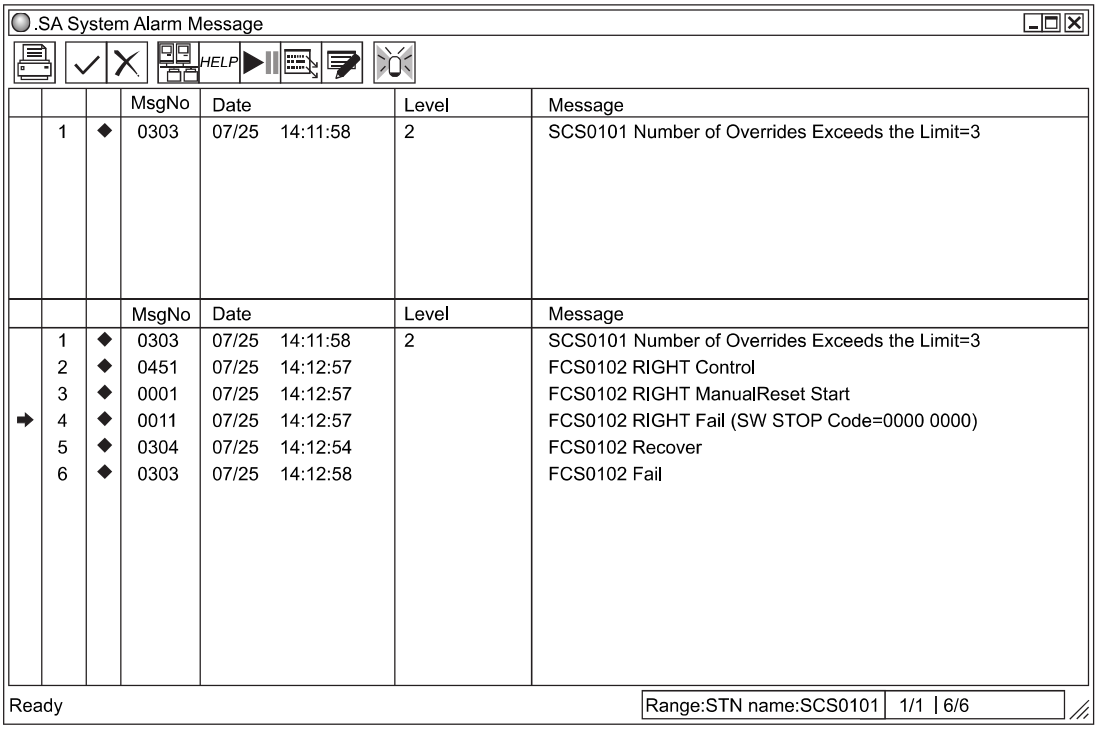


Figure B8.1.1-2 Split display of the System Alarm view

SEE ALSO For more information about split display of the System Alarm view, refer to:

- "Splitting System Alarm View" in 4.2.3, "Filter and Display System Alarm Messages" in the Human Interface Stations Reference Vol. 1 (IM 33J10D10-01EN)
- "Splitting System Alarm View" in 4.2.3, "Filter and Display System Alarm Messages" in the Human Interface Stations Reference Vol. 1 (IM 33K03F21-50E)

Specification of system alarm filters

The following filters can be specified in the System Alarm view:

- All

All system alarm messages are displayed.

- Station Name
  System alarm messages generated in the selected station are displayed.
- Current Station
  Alarm messages generated in the current station are displayed.
- Safety Control Station
  System alarm messages generated on SCS are displayed.

  All ProSafe-RS SCSs become the target of filtering.

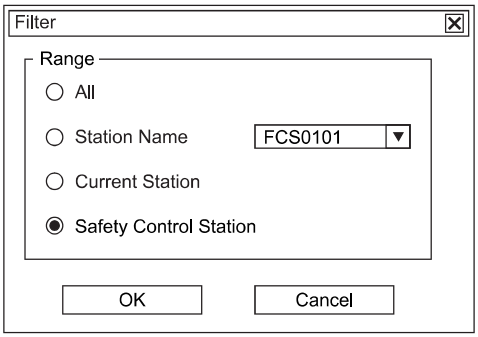


Figure B8.1.1-3 System alarm filter setting dialog box

B8.1.2 Process Alarm view

The Process Alarm view displays process alarms including annunciator messages.

SEE ALSO For more information about Process Alarm view, refer to:

- 3.6, "Process Alarm View" in the Human Interface Stations Reference Vol. 1 (IM 33J10D10-01EN)
- 3.6, "Process Alarm View" in the Human Interface Stations Reference Vol. 1 (IM 33K03F21-50E)

Overview of the Process Alarm view

The Process Alarm view displays and manages the process alarm information notified by SCSs and FCSs as process alarm messages and annunciator messages.

- When a process alarm has occurred in SCS, the [SCS Alarm occurrence Notification] button display on the toolbar changes to notify the occurrence of an SCS alarm. When the [SCS Alarm Occurrence Notification] button is clicked, the message is displayed after being filtered by the [Safety Control Station] filter.
- SCS process alarms can be acknowledged and deleted in the Process Alarm view. Acknowledging or deleting an SCS process alarm on an HIS will change the corresponding process alarm information managed on the SCS.
- Process alarm messages occurred in SCSs can be filtered into a separate group for display. This function allows for easy distinction of SCS alarms from FCS alarms even when a large number of process alarm messages have been generated on FCSs.
- If SCS alarms are present, calling the Process Alarm view will automatically filter the alarm messages using the [Safety Control Station] filter before the window is displayed.

Selection of display items

Call the Window Setting dialog box from the applicable tool button in the Process Alarm view. When this dialog box is first opened, the Display Item name check box is unchecked. Checking this box will enable the selection of items you want to display in the Process Alarm view.

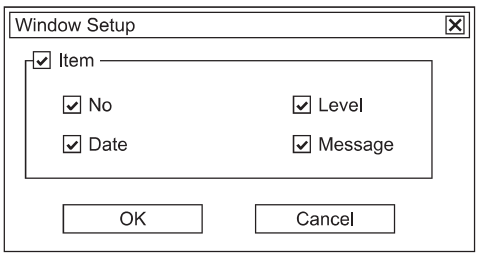


Figure B8.1.2-1 Window Setup dialog box

The following table shows the default display items in the Process Alarm view and items that can be displayed or hidden.

Table B8.1.2-1 Display items in the Process Alarm view

Display item name	Default window setting	Selection
Item	Displayed	Yes
Date	Displayed	No
Level(*1)	Not displayed	Yes
Message	Displayed	No

*1: The displayed level corresponds to the alarm priority level.

Split display

The Process Alarm view can be displayed into two frames.

When a filter is set, the view is split horizontally, with the messages matching the filter condition displayed in the top frame and all messages displayed in the bottom frame. However, if an alarm priority filter is selected in the Alarm tab on the HIS Setup window, both the top and bottom frames display only the messages of the specified priorities.

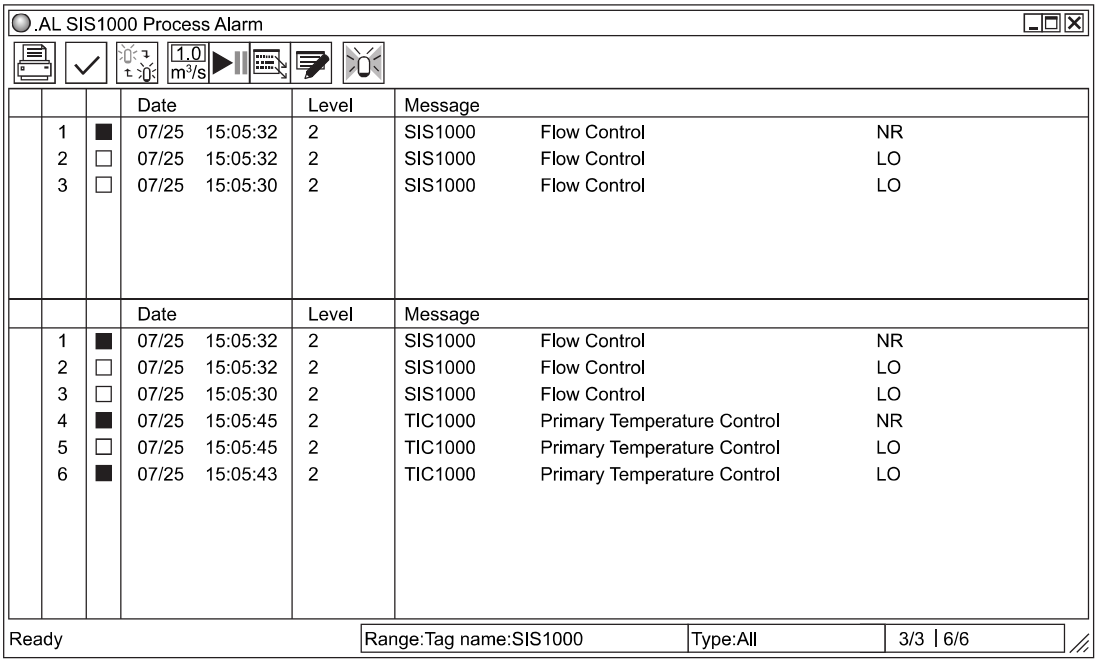


Figure B8.1.2-2 Split display of the Process Alarm view

SEE ALSO For more information about Split display of the Process Alarm view, refer to:

- "Splitting Process Alarm View" in 3.6.3, "Filter and Display Process Alarm Messages" in the Human Interface Stations Reference Vol. 1 (IM 33J10D10-01EN)
- "Splitting Process Alarm View" in 3.6.3, "Filter and Display Process Alarm Messages" in the Human Interface Stations Reference Vol. 1 (IM 33K03F21-50E)

Search and display of process alarm messages

Process alarm messages and annunciator messages can be searched for using the following keywords:

Search range specification

- All
  All process alarm messages and annunciator messages are displayed.
- FCS Name
  Process alarm messages and annunciator messages generated in the selected control station are displayed.
- Plant Hierarchy Name
  Process alarm messages and annunciator messages generated in the selected control drawing name or unit instrument tag name are displayed.
- Tag Name

Process alarm messages and annunciator messages relating to the specified function block are displayed.

- Batch ID
  Process alarm messages and annunciator messages relating to the specified batch ID are displayed.
- Safety Control Station
  Process alarm messages and annunciator messages generated on SCSs are displayed.

  All ProSafe-RS SCSs become the target of filtering.

Search types

- All
  Process alarm messages and annunciator messages are displayed.
- Function Block Only
  Only process alarm messages are displayed.
- Annunciator Only
  Only annunciator messages are displayed.

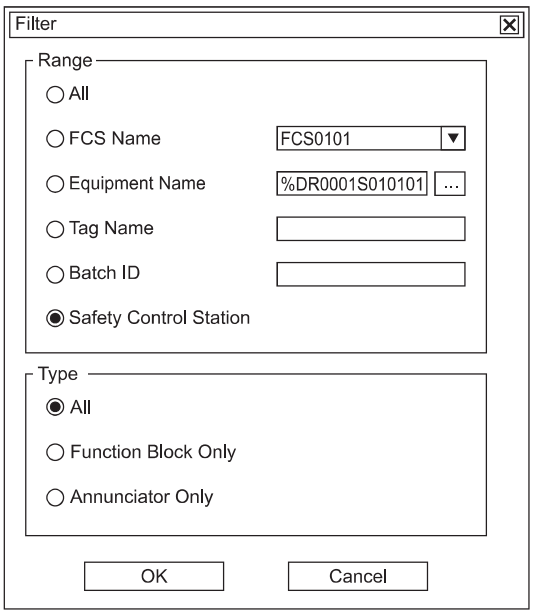


Figure B8.1.2-3 Alarm filter setting dialog box

B8.1.3 Instrument faceplates

Instrument faceplates display statuses and data of function blocks, mapping blocks, and elements assigned on the Tag Name Builder. Instrument faceplates of SCS and FCS are distinguished by the color of the mark in the bottom of the faceplate.

IMPORTANT

The operator must utilize the SCS instrument faceplate mainly for monitoring.

Follow the predefined procedure to operate an SCS instrument faceplate.

Instrument faceplate display

Mapping blocks can be called from an HIS as the instrument faceplate.

The function block types are as follows (the corresponding mapping block types are shown after the colon ":"):

- BOOL/ECW_B, DINT/ECW_I, REAL/ECW_R, IO_REAL, SCI_B, SCO_B, SCI_I, SCO_I, SCI_R, SCO_R : %WB
- PSI_I, PSI_R, PNI_I, PNI_R : %XB
- IO_BOOL : %Z, %Y
- ANN, ANN_FUP : %AN
- ANLG_S : S_ANLG_S
- ANLGI : S_ANLGI
- VEL : S_VEL
- OVR_B, OVR_I, OVR_R, OVR_IB, OVR_IR : S_OVR_B, S_OVR_I, S_OVR_R, S_OVR_IB, S_OVR_IR
- PASSWD : S_PASSWD
- HSDTR : S_HSDTR
- GASDTR : S_GASDTR

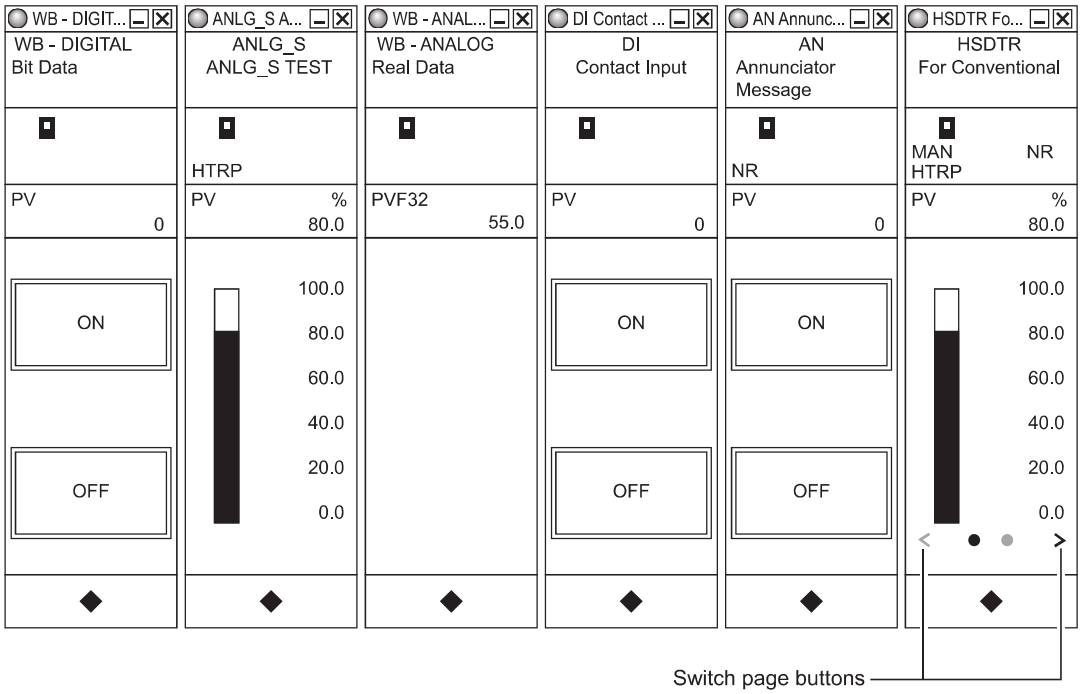


Figure B8.1.3-1 Image of instrument faceplate display

- GOV_B, GOV_IB : S_GOV_B, S_GOV_IB
- MOB_21 : S_MOB_21
- MOB_11 : S_MOB_11
- MOB_RS : S_MOB_RS
- MOA : S_MOA

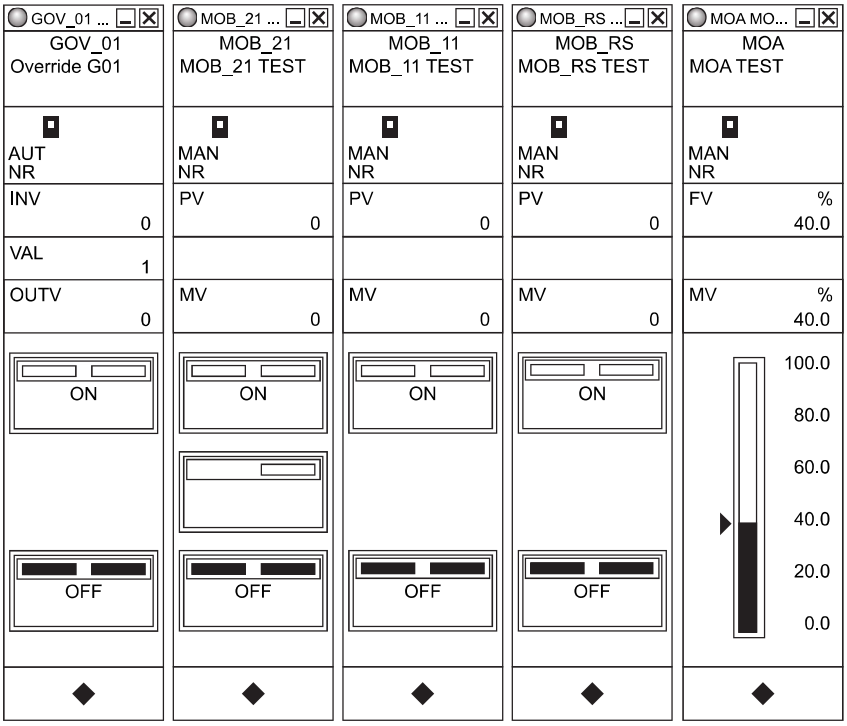


Figure B8.1.3-2 Image of instrument faceplate display

SEE ALSO For more information about instrument faceplates, refer to:

- 2, "Instrument Faceplate" in the Human Interface Stations Reference Vol. 2 (IM 33J05A11-01EN)
- 2, "Instrument Faceplate" in the Human Interface Stations Reference Vol. 2 (IM 33K03F22-50E)

Operation of password function blocks and manual operation blocks

- PASSWD, MOB_21, MOB_11, MOA
  If you set values of MV, enter the password in the password dialog box.

  If you enter the wrong password, MV values are reset to the previous values before the change.
- MOA
  To close the INC/DEC dialog box, click anywhere outside the dialog box. If no action is made, the dialog box closes in about 30 seconds.

Instrument faceplate

On the instrument faceplates of SCS and FCS, the mark in the bottom is displayed in different colors.

Table B8.1.3-1 Color of the mark in the bottom of faceplates

Station	mark color
FCS	Dark Blue
SCS	Orange

TIP Related builders cannot be called using a tag name.

Operation marks

The settings for operation mark provide the function to notify the operator of various statuses of equipment, such as under maintenance, out of order or operation prohibited. When an operation mark is set, a tag with comment is set in the instrument faceplate. By assigning an operation mark, the operation privileges over the instrument faceplate can be changed temporarily.

SEE ALSO For more information about settings for the Operation marks, refer to:

- "Toolbar of Tuning View" in 3.3.1, "Components of Tuning View" in the Human Interface Stations Reference Vol. 1 (IM 33J10D10-01EN)
- "Toolbar of Tuning View" in 3.3.1, "Components of Tuning View" in the Human Interface Stations Reference Vol. 1 (IM 33K03F21-50E)

Two-step operation setting for switch faceplates

Operation of the instrument faceplate buttons in the following function blocks is always in two steps, regardless of the settings in the instrument faceplate operation definition tab in the HIS constants builder.

- Grouping Override Function Block (GOV_*)
- Override Function Block (OVR_*)
- Password Function Block (PASSWD)
- Data Manual Operation with Answerback Function Block (MOB_*)
- Auto-reset Data Manual Operation Function Block (MOB_RS)

SEE ALSO For more information about two-step operations, refer to:

- "Two-Step Operation" in 2.5, "Operation Type on Instrument Faceplate" in the Human Interface Stations Reference Vol. 2 (IM 33J05A11-01EN)
- "Two-Step Operation" in 2.5, "Operation Type on Instrument Faceplate" in the Human Interface Stations Reference Vol. 2 (IM 33K03F22-50E)

Reconfirmation dialog box

When operating the following data items of the mapping block in the instrument faceplate or data input dialog box, the reconfirmation dialog box always appears regardless of the tag mark setting. You cannot disable the reconfirmation dialog box by the tag mark setting.

Table B8.1.3-2 Data items of mapping block for which the reconfirmation dialog box appears

Function block	Data items of mapping blocks
Grouping Override Function Block (GOV_*)	MV
Override Function Block (OVR_*)	MV
Password Function Block (PASSWD)	MV
Data Manual Operation with Answerback Function Block (MOB_*)	MV
Auto-reset Data Manual Operation Function Block (MOB_RS)	MV
Analog-type Data Manual Operation Function Block (MOA)	MV
Analog input function block for smoke and heat detectors (HSDTR)	MV01
Analog input function block for gas and flame detectors (GASDTR)	MV01

Reset operation of device

Follow these steps to reset a device from an instrument faceplate corresponding to HSDTR or GASDTR.

TIP The switch page buttons are not displayed when the instrument faceplate is in the compact view. For this reason, the page on which the reset button is displayed cannot be displayed either. Run the reset operation after switching to the normal view.

1. Click the switch page button on the right.
   The display will switch to the page with a reset button.

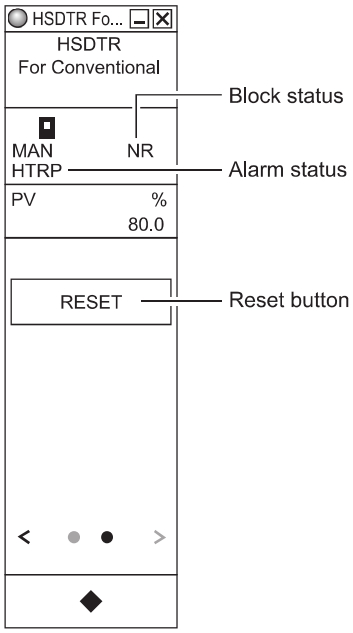


Figure B8.1.3-3 Display of instrument faceplate on 2nd page (example of HSDTR)

2. Click the reset button.
   The reconfirmation dialog box appears.

TIP

The reset button cannot be operated when an operation guard is displayed over the reset button.

3. Click [OK] on the reconfirmation dialog box.
   The reset operation will be run. Operations in an instrument faceplate corresponding to HSDTR or GASDTR are not two-step operations.

   With HSDTR, [RST] appears for the block status during the reset status.

4. Click the switch page button on the left.
   The display will switch to that of the process variable bar. The reset operation is complete when the alarm status switches to [NR].

B8.1.4 SCS Station Status Display view

The SCS Station Status Display view displays the operating status of each SCS, such as scan period and security level.

IMPORTANT

SCSs cannot be started or stopped from the SCS Station Status Display view, regardless of the roles assigned to the operator on the HIS.

TIP

In this manual, the safety control unit is referred to as CPU node and the safety node unit is referred to as FIO node.

System Status Overview view

The System Status Overview displays the status of the system over the control bus, including SCS, HIS and FCS. SCS icons are the same as FCS icons and are shown in orange frames.

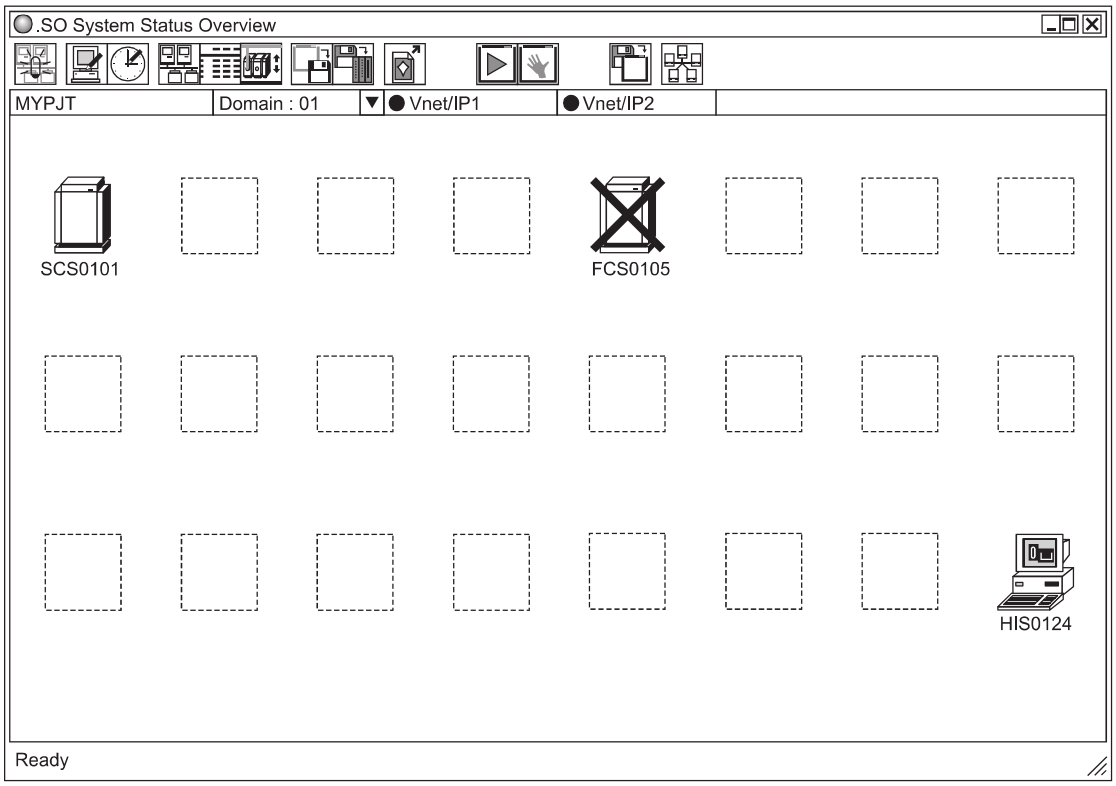


Figure B8.1.4-1 System Status Overview view

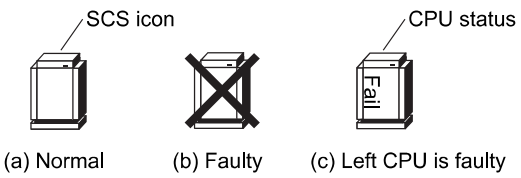


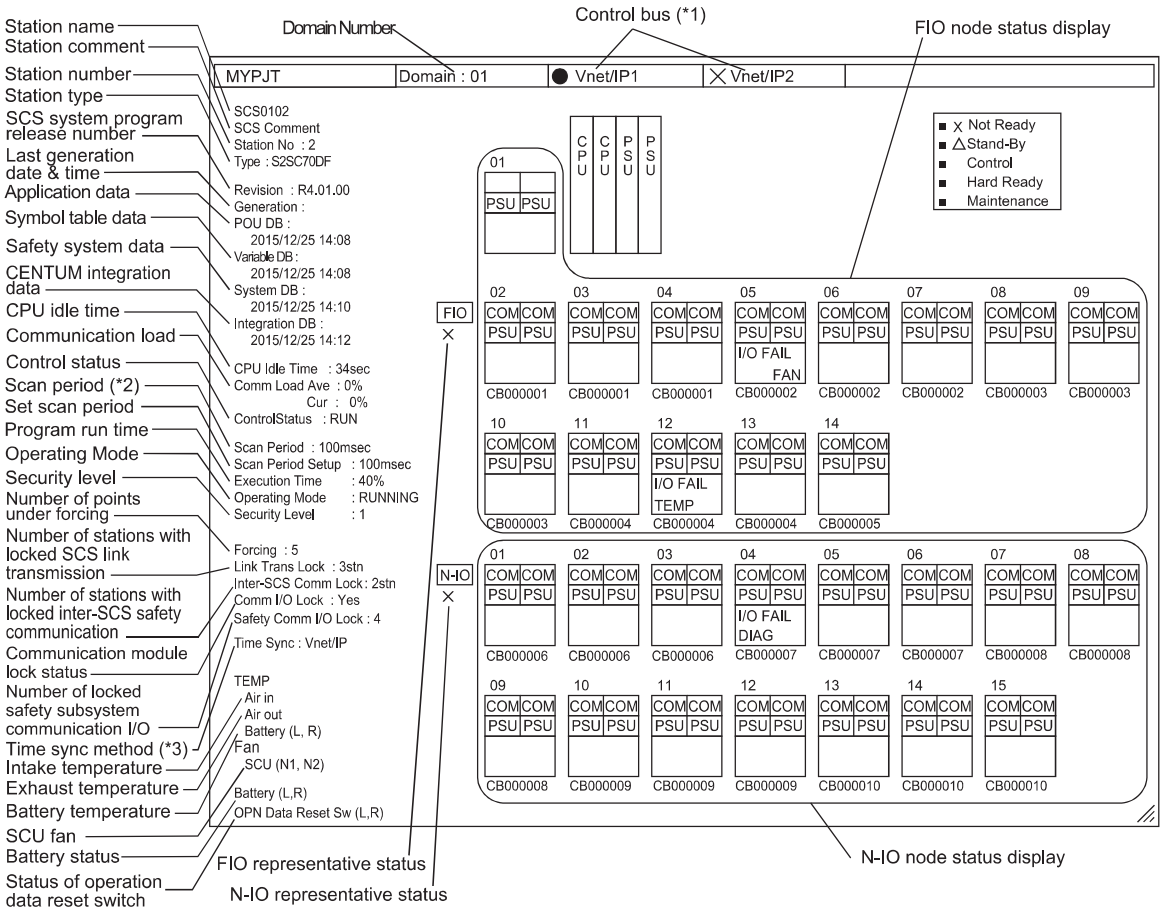
Figure B8.1.4-2 SCS icons

SCS Station Status Display view

The SCS Status Display shows the status of an SCS in detail. Operating mode, scan period and security level are shown in this window. In this window, whether or not the operating status and connection status of CPU and I/O modules is normal is shown in different colors.

IMPORTANT

The HIS' s SCS Station Status Display view displays the information that has been read from each SCS. However, the Diagnostic Information Operating dialog box in SCS Maintenance Tool cannot be opened from this window.



*1: When V net is used, “V net1” and “V net2” are displayed instead of “Vnet/IP1” and “Vnet/IP2,” respectively.
*2: For SCS with system program R2.02 or earlier, the set scan period is displayed.
*3: When V net is used, the “IRIG-B : Ready” is displayed instead of “Time Sync : Vnet/IP.”

Figure B8.1.4-3 SCS Station Status Display view

Toolbar of the SCS Station Status Display view

The following operations can be performed from the toolbar in the SCS Status Display view:



Selecting this button will call the System Alarm view where alarm details can be checked. If a system alarm message is present, the button will flash in red.



Selecting this button will call the HIS Setup window.



Selecting this button will call the Adjust Time dialog box.



Selecting this button will call the System Status Overview view.



The SCS report dialog box to show the station information.

The contents in the dialog box can be printed out or exported into a file.

Station information display

The following information is displayed in the SCS information:

- Station name
- Station comment
- Station number
- Station type
- SCS system program revision
- Last generated date/time
  The date and time of the last download to the SCS is displayed for each of the following DBs:
  - POU DB (application data)
  - Variable DB (symbol table data)
  - System DB (safety system data)
  - Integration DB (CENTUM integration data)
- CPU idling time (seconds)
  The CPU idling time per minute is displayed.
- Communication load (%)
  The Vnet/IP communication load against CPU load of the safety control station is displayed in percentage. The displayed values are current load and the moving average load against minute.
- Control status
  [RUN] is displayed when the SCS is running, and [STOP] is displayed when the SCS is stopped, both in cyan color.
- Scan period (milliseconds)
  This is the actual scan period of the SCS. Note that the set scan period is displayed for SCS with system program R2.02 or earlier.
- Set scan period (milliseconds)
  The set scan period for the SCS is displayed.
- Program execution time (%)
- Operating mode
  [RUNNING] is displayed when the SCS in the running mode, [WAITING] is displayed when the SCS is in the waiting mode, and [INITIAL] is displayed when the SCS is in the initial mode.
- Security level
- Number of points under forcing

- Number of stations locked in SCS Link Transmission
- Communication module lock status
  [Yes] is displayed in cyan when the communication I/O data is locked, and [No] is displayed in cyan when the communication I/O data is not locked.
- Number of stations locked in Inter-SCS Safety Communication
- Number of locked safety subsystem communication I/O
  The number of locks is displayed in cyan.

  This is only displayed for SCSP3. If S2LP131 is not defined, 0 is displayed.
- IRIG-B connection status
  This item is displayed if IRIG-B time synchronization is specified.
- Time synchronization method
  This is displayed only when the control bus is Vnet/IP. If the SCS is synchronized with SNTP server, [SNTP] is displayed; if it is not synchronized with SNTP server, [Vnet/IP] is displayed.

SEE ALSO For more information about the actual and set scan period, refer to:

A7.2, “Automatic extension function for scan period of the application logic execution function” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Station status display

The following statuses are displayed in the SCS station status: The character string representing each item is displayed in green if the status is normal, or red if faulty. If the status is faulty, the × mark indicating fault is displayed.

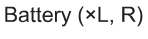


Figure B8.1.4-4 The mark stands for abnormal (battery temperature abnormal)

- Intake temperature
- Exhaust temperature
- Battery temperature
- SCU Fan
  This item is displayed for the station type that supports wide temperature ranges (S2SC70S-F, S2SC70D-F, L1SC70S-F, L1SC70D-F, SSC60S-F, SSC60D-F, SSC50S-F, SSC50D-F, SSC10S-F, SSC10D-F).
- Battery status
- Status of the operation data reset switch
  - This status is displayed on HIS in CENTUM VP R6.07.00 or later if the station type is SSC60 or S2SC70. If the CPU module is S2CP471, the status that the operation data is maintained is displayed in green, and the status that the operation data is cleared is displayed in red. If the CPU module is other than S2CP471, the maintained status is displayed.
  - This status is displayed on HIS in CENTUM VP R6.08.00 or later if the station type is L1SC70. The status that the operation data is maintained is displayed in green, and the status that the operation data is cleared is displayed in red.

Station configuration display

The following statuses are displayed in the SCS station configuration:

- CPU Status

The character string is displayed in green, red, yellow or blue when the CPU is normal, faulty, on standby or hardware ready, respectively. When a program is being copied, the character string [COPY] will flash in white. While FLASH memory is being written, [FLASH] will flash in white.

- Power Supply Status
  Displayed in green if the power supply is normal, or red if faulty.

ESB bus status display

Displayed in green if the ESB bus is normal, or red if faulty. But the status of the Optical ESB Bus Repeater modules is not displayed.

Display of the representative node status

The representative status is displayed under the N-IO and FIO node labels that indicate the N-IO and FIO nodes.

- For N-IO nodes
  If any N-IO node has an error, a red [X] is displayed. If a node is under maintenance, a cyan box is displayed. If a maintenance port of a node interface unit (NIU) is enabled in a node, a magenta opened padlock mark is displayed.



Figure B8.1.4-5 Opened padlock mark

If a node has various mixed status, the status is displayed in the following precedence:

1. Red [X]
2. Cyan box
3. Magenta opened padlock mark

- For FIO nodes
  If any FIO node has an error, a red [X] is displayed. When only SEC40x or L1EC40x is defined for FIO Node 1, the power status of the CPU Node is not reflected in the FIO representative status.

FIO node status display

In the FIO node configuration of the control station, the following status is displayed. When you click on the display area of the node configuration, the node status display dialog box appears.

- Node number
- Communication status
  The communication status of nodes is displayed in character string [COM]. It is displayed in green if the power supply is normal, or red if faulty. Nothing is displayed in node 1.
- Power supply status
  The power supply status of nodes is displayed in character string [PSU]. It is displayed in green if the power supply is normal, or red if faulty. When only SEC40x or L1EC40x is defined for FIO Node 1, the power status of the CPU Node is not reflected in the power status of FIO Node 1.
- Input module status
  It displays whether the input module is faulty. If it is faulty, [I/O FAIL] is displayed in red. Nothing is displayed while it is normal.
- Component number

N-IO node status display

In the N-IO node configuration of the control station, the following status is displayed. When you click on the display area of the node configuration, the node status display dialog box appears.

- Node number
- Communication status
  The communication status of nodes is displayed in character string [COM]. It is displayed in green if the power supply is normal, red if faulty, or in cyan if it is under maintenance.
- Power supply status
  The power supply status of nodes is displayed in character string [PSU]. It is displayed in green if the power supply is normal, or red if faulty.
- Input unit status
  It indicates the status of the input unit. If it is faulty, [I/O FAIL] is displayed in red. Nothing is displayed while it is normal.
- Node diagnosis
  If the node interface unit (NIU) notifies the abnormality of the node temperature or error information from an external diagnostic device, [DIAG] is displayed in red. Nothing is displayed while it is normal.
- Node status
  The node status is displayed with the frame enclosing the display area of the node configuration. It is displayed in green if normal, red if faulty, and cyan if both nodes are under maintenance. It is displayed in green dotted lines if node status is normal and the NIU maintenance port is enabled.

  If a node has various mixed status, the status is displayed in the following precedence:

  1. Abnormal
  2. Under maintenance
  3. If node status is normal and the NIU maintenance port is enabled
  4. Normal
- Status of the NIU maintenance port
  If enabled, a magenta opened padlock mark is displayed on the upper right of the node configuration.
- Component number

SCS Report dialog box

The SCS Report dialog box showing the status of each SCS can be called from the SCS Station Status Display view. To call the SCS Report dialog box, use the following button on the toolbar:



The following figure shows an example of the SCS Report dialog box:

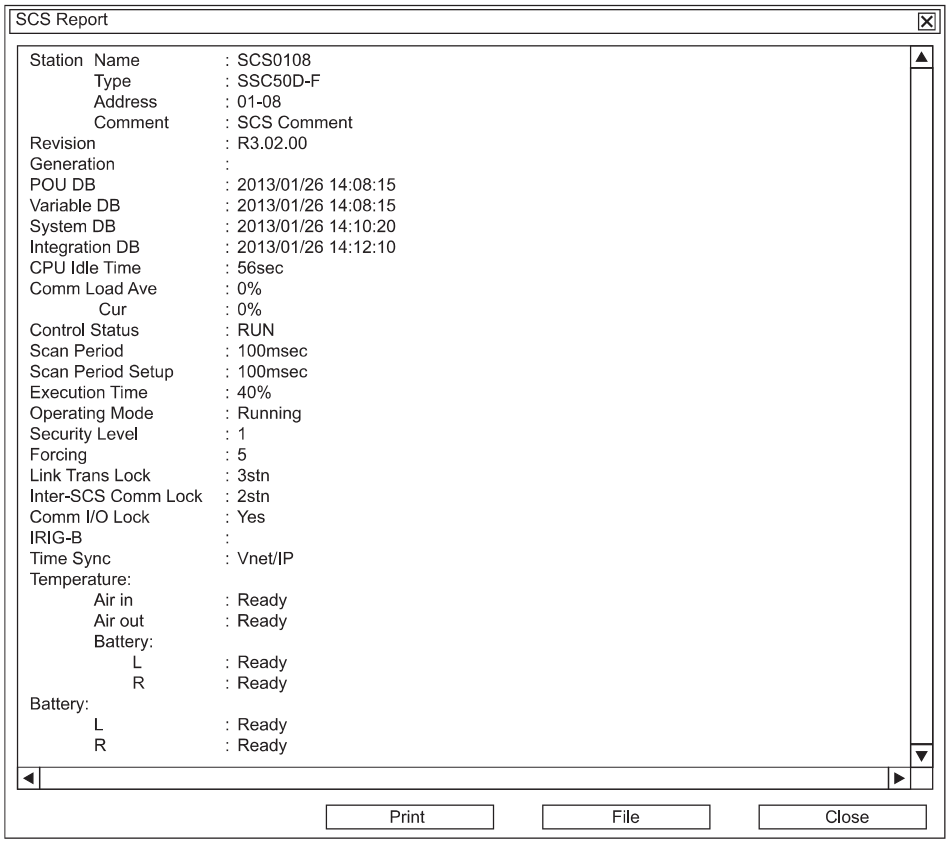


Figure B8.1.4-6 SCS Report dialog box

- Print
  Clicking this button prints the content currently displayed in the SCS Report dialog box. The displayed content will be output to the printer specified in the HIS Setup window.
- File
  Clicking this button saves the content currently displayed in the SCS Report dialog box to a FDC. The default name of the save file is "SCSRevInf.txt."
- Close
  Clicking this button closes the SCS Report dialog box.

SCS Node Status Display dialog box

The SCS Node Status Display dialog box is used to display the node status of each SCS in detail. The following figure shows an example of the SCS Node Status Display dialog box:

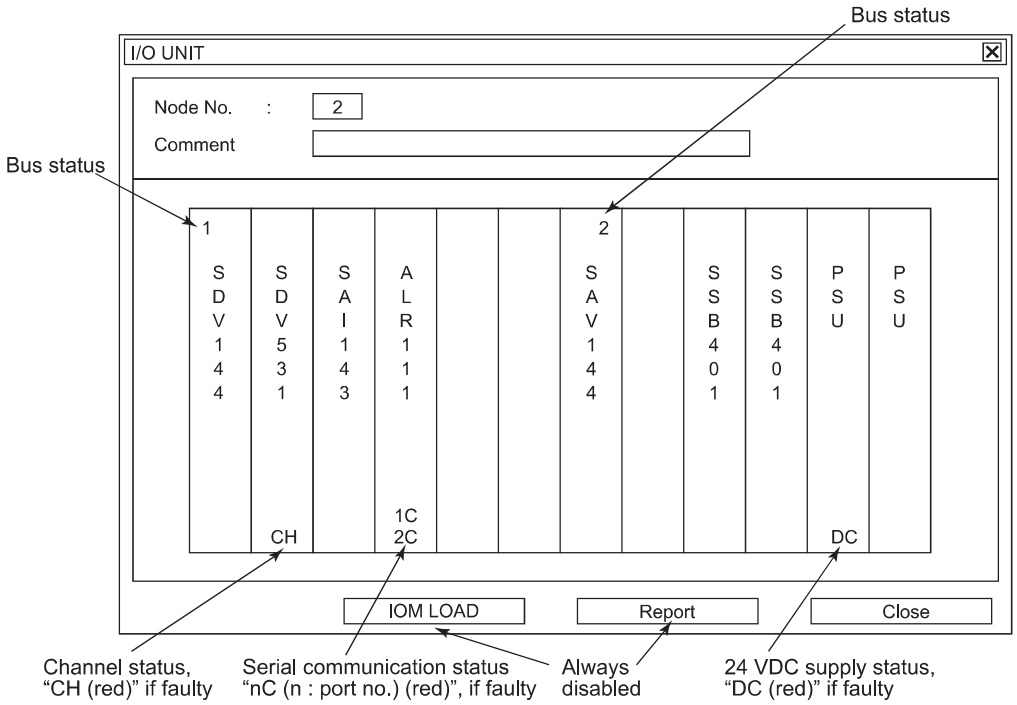


Figure B8.1.4-7 SCS node status display dialog box (for FIO nodes)

TIP

But the status of the Optical ESB Bus Repeater modules is not displayed.

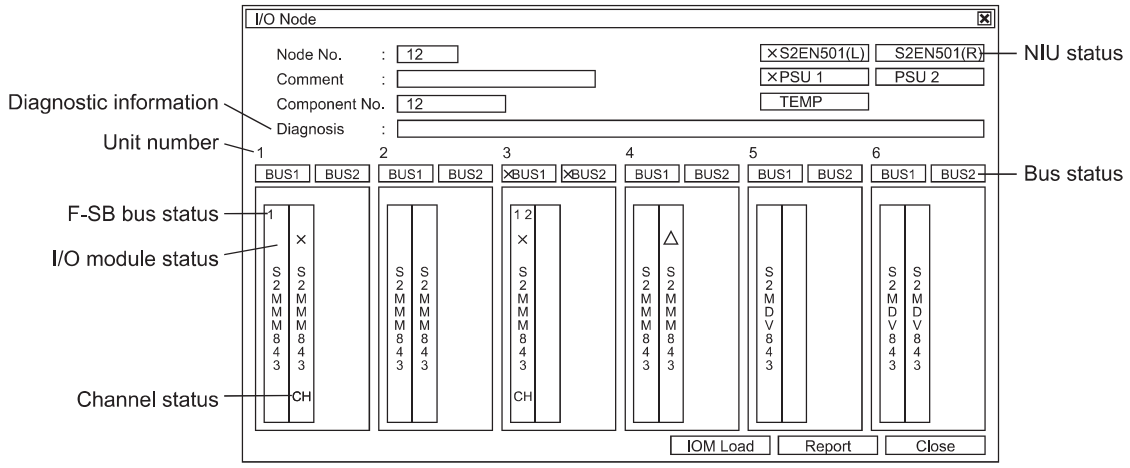


Figure B8.1.4-8 SCS node status display dialog box (for N-IO nodes)

FIO node status display

The communication status and power supply status of FIO nodes are displayed.

- Power supply status
  The character string [PSU] is displayed in green if the node is normal, or red if faulty.
- 24 VDC supply status
  [DC] is displayed in red if the power supply status is abnormal.
- SSB401/L1SB401 status
  The color of SSB401/L1SB401 changes to green if the unit is normal, and red if faulty. When the status is faulty, a mark is displayed.
- Bus status

Nothing is displayed while the buses are normal. If a bus is faulty, the bus number appears in red.

- I/O module status
  The color of the I/O module varies with module status. Green indicates Normal. Red indicates Abnormal. Blue indicates Ready and yellow indicate Standby. The bus status is also displayed by a red-colored number.

  The "-" in the I/O module name is not displayed.
- Channel status
  [CH] is displayed in red if any assigned channels are faulty.
- Communication module status (Subsystem communication)
  [nC] (n: port number) is displayed in red if communication with the subsystem fails.

N-IO node status display

The diagnosis information, NIU status, power supply status, temperature status, and node communication status of the N-IO nodes are displayed.

- Diagnosis information
  If NIU notifies the node temperature is abnormal or error information from an external diagnostic device, all of these contents are displayed. Multiple information are separated by commas.
- NIU status
  The communication status of NIU is displayed. If the communication status is normal, the NIU type is displayed in green. If it is faulty, an [×] and the NIU type are displayed in red or in cyan if it is under maintenance.
- Power supply status
  The power supply status of the node is displayed. If normal, [PSU + number] is displayed in green. If faulty, [×] and [PSU + number] are displayed in red.
- Temperature status
  The temperature status of the node is displayed. If normal, [TEMP] is displayed in green. If faulty, [×] and [TEMP] are displayed in red.
- Bus status
  The bus status is displayed. If normal, [BUS + number] is displayed in green. If faulty, [×] and [BUS + number] are displayed in red. If it is not defined, nothing is displayed.
- I/O module status
  The status of the I/O module is displayed. If the module is normal, the I/O module name is displayed in green. If the module is faulty, [×] and I/O module name are displayed in red. If the module is on dual-redundant standby status, [△] and the I/O module name are displayed in yellow.
- F-SB bus status
  The communication status of F-SB bus (the node bus) is displayed. If it is faulty, character string [1] or [2] that indicates the bus position is displayed in red. Nothing is displayed while it is normal.
- Channel status
  The communication status of the I/O module channel signal is displayed. If it is faulty, the character string [CH] that indicates the representative channel is displayed in red. Nothing is displayed while it is normal.
- Status of the NIU maintenance port
  If it is enabled, a magenta opened padlock mark is displayed on the right side of the [Node No.] column, and [Maintenance Port Enabled] is displayed. Nothing is displayed while it is disabled.

Channel status display dialog box

When you double-click on the display area of the I/O module in the SCS node status display dialog box of N-IO, the channel status display dialog box appears.

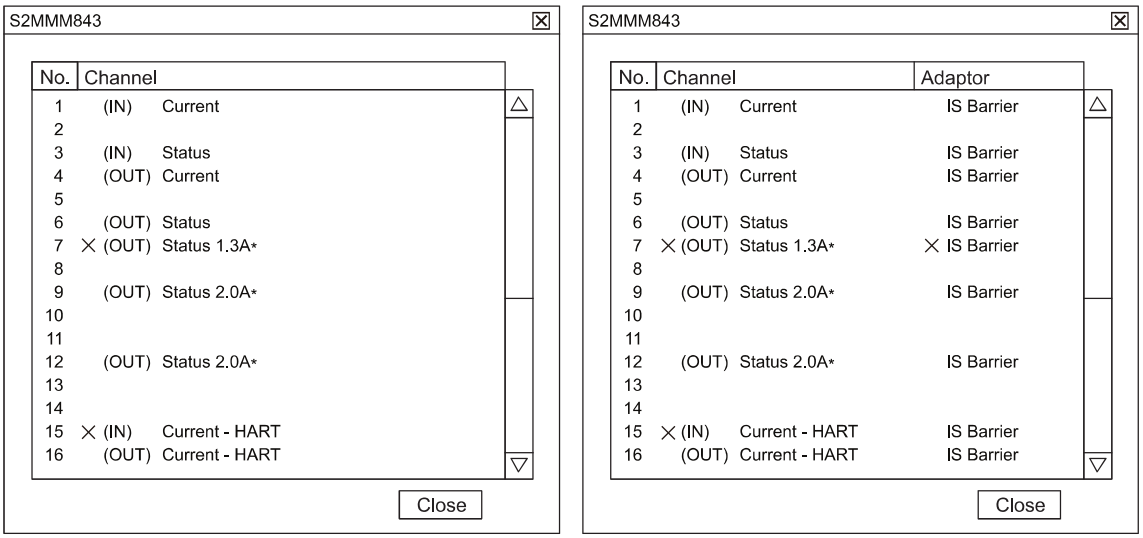


Figure B8.1.4-9 Channel status display dialog - normal configuration (left) and intrinsic safety barrier configuration (right)

The channel status display dialog box shows the signal type and communication status that are assigned to each channel of the I/O module. If the channel communication status is normal, the channel information in the channel column is displayed in green. If the channel communication status is faulty, the channel information in the channel column is displayed in red with [x] placed at the head. If the channel is not defined, nothing is displayed.

Only the primary channel is displayed for high current output. Non-primary channels are not displayed.

If you are using an intrinsic safety barrier, "IS Barrier" is displayed in the Adaptor column. If normal, it is displayed green. If it is faulty, [×] is placed in front and is displayed in red.

Table B8.1.4-1 Display character strings for channel signal types

Channel column display	Signal type
(Blank)	Not used (Not defined)
(IN) Current	Current input
(IN) Current - HART	Current input (HART)
(IN) Status	Status input
(OUT) Current	Current output
(OUT) Current - HART	Current output (HART)
(OUT) Status	Status output
(OUT) Status 1.3A *	Status output (1.3A output)
(OUT) Status 2.0A *	Status output (2A output)

B8.1.5 Adjust Time dialog box

You can set or change the system date and time in the Adjust Time dialog box.

Time setting from an HIS

You can change the current network time from an HIS using the time setting function.

- Vnet/IP
  Network time on the Vnet/IP (including V net router) is synchronized with the time set on HIS. Therefore, the time on the following stations is synchronized with the time set on HIS:
  - SCS (CPU module and digital input module (SDV144/L1DV144))
  - SENG, FCS, HIS

  If the time synchronization is based on an SNTP server, the time set on HIS is ignored.
- V net
  The network time in one V net domain and other V net domains, where Transfer/Receive System Time is specified for BCV/CGW, is synchronized with the time set on HIS. Therefore, the time on the following stations is synchronized with the time set on HIS:
  - SCS (CPU module and digital input module (SDV144))
  - SENG, FCS, HIS

  However, the network time of the Vnet/IP domain is not synchronized if the domain is connected through a V net router (AVR10D) of Style S2 or earlier. Even with a V net router of Style S3 or above, the network time is not synchronized if the V net domain is not configured as the clock master. SCS time with IRIG-B time synchronization is unaffected by the time change on the HIS.

SEE ALSO For more information about Time synchronization of SCS, refer to:

A3., “Time synchronization” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about Adjust Time dialog box, refer to:

- 4.4, "Adjust Time Dialog Box" in the Human Interface Stations Reference Vol. 1 (IM 33J10D10-01EN)
- 4.4, "Adjust Time Dialog Box" in the Human Interface Stations Reference Vol. 1 (IM 33K03F21-50E)

B8.1.6 Software for Managing the Alarms

CENTUM VP has the following dedicated alarm management software:

- UACS (Unified Alarms & Conditions Server)
- CAMS for HIS (Consolidated Alarm Management Software for HIS)

IMPORTANT

Although it is possible to suppress less important alarm messages so as to make important alarms more noticeable, do not suppress messages from SCS.

This section provides an overview of these software.

SEE ALSO

For more information about UACS, refer to:

UACS Alarm Management Reference (IM 33J05A22-01EN)

For more information about CAMS for HIS, refer to:

A1., "CAMS for HIS Overview" in the Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

Overview of UACS

UACS is an ANSI/ISA-18.2 compliant alarm management system. It provides the function to manage alarm messages generated in the plant according to the functions required by alarm management standards and guidelines.

UACS has a default filter for filtering system alarms and process alarms from SCS.

Overview of CAMS for HIS

When CAMS for HIS is enabled in HIS, the System Alarm and Process Alarm views for displaying and managing the system alarms and process alarms are integrated in the CAMS for HIS window.

CAMS for HIS Message Monitor has a default filter for filtering system alarms and process alarms from SCS.

B8.2 Other functions used for operation and monitoring of SCS

Override is available as an operation from HIS. In addition, equalizing and trend recording are available as HIS functions that can be used in the operation and monitoring of SCS. This section also describes the CENTUM Security Function, Alarm Inhibition, and Chattering Alarm Suppression.

SEE ALSO For more information about override from HIS, refer to:

I1.1.1, “Override” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

B8.2.1 Equalizing

The [SCS Taglist Import] command, which is run on System View, generates a taglist database from the information defined using the ProSafe-RS's Engineering Function and the generated taglist database is downloaded to each HIS in the system. As a result, taglist databases on the SCS and HIS are equalized.

IMPORTANT

When you have added or changed any tag definitions using the Tag Name Builder on the SENG and downloaded the changes to the SCS, there will be inconsistencies between the databases in the SCS and HIS. To equalize the database, go to the System View and run the [SCS Taglist Import] command.

SEE ALSO For more information about how to run [SCS Taglist Import] from System View, refer to:

"■ Generating SCS taglist on CENTUM" on page B7-43

■ SCS monitoring

Each HIS function communicates with SCSs based on the equalized information.

SCSs are handled in the following manner on the HIS:

- SCSs are not included in the number of FCS units operated and monitored.
- SCS tags are included in the tag monitoring points.

B8.2.2 Trend recording

SCS tag names can be assigned for trend data recording. However, since SCSs do not support high-speed (1-second) trend recording, assigning an SCS tag name to a high-speed trend recording block will not display data. Do not assign SCS tag names to high-speed trend recording blocks.

B8.2.3 Security function of CENTUM

The CENTUM provides a security function that changes access privileges with respect to FCS data according to the account of the operator working on each HIS. This function can be utilized for SCSs in the same manner.

These access privileges can be restricted further using the Security Function of the CENTUM. For example, an HIS account permitted to write data assigned to external communication function blocks and an HIS account not permitted to write such data can be set up using the Security Function of the CENTUM.

- The Security Function of the CENTUM is completely independent of the security levels of SCSs. SCS security levels cannot be manipulated from HISs.
- The Security Function of the CENTUM is completely independent of the SENG' s Engineering Security Management Function.

B8.2.4 Alarm inhibition (AOF)

Alarm inhibition (AOF) is a function to suppress the display and beeping sounds of process alarm messages temporarily. It is useful when many process alarm messages are generated during the startup of SCS. System alarm messages cannot be suppressed.

How to activate/deactivate suppress alarm function

You can turn on the Alarm Inhibition function (AOF) from HIS or from FCS targeting the Mapping block/element on the SCS.

Every time the SCS is restarted, the Alarm Inhibition function (AOF) is turned off. The switch between activate and deactivate the Alarm Inhibition function is allowed only by applications on the FCS or on the HIS. Neither the applications on the SCS nor the applications on the SENG are allowed to do so.

SEE ALSO For more information about secifying alarm inhibition, refer to:

7.3.4, "Alarm Inhibition (AOF)" in the Human Interface Stations Reference Vol. 2 (IM 33J05A11-01EN)

For more information about specifying alarm inhibition, refer to:

7.3.4, "Alarm Inhibition (AOF)" in the Human Interface Stations Reference Vol. 2 (IM 33K03F22-50E)

Alarm inhibition from HIS

You can inhibit alarm for Tag data of SCS by using AOF button on Tuning view of HIS. The Tag mark color is shown in blue while the function is on.

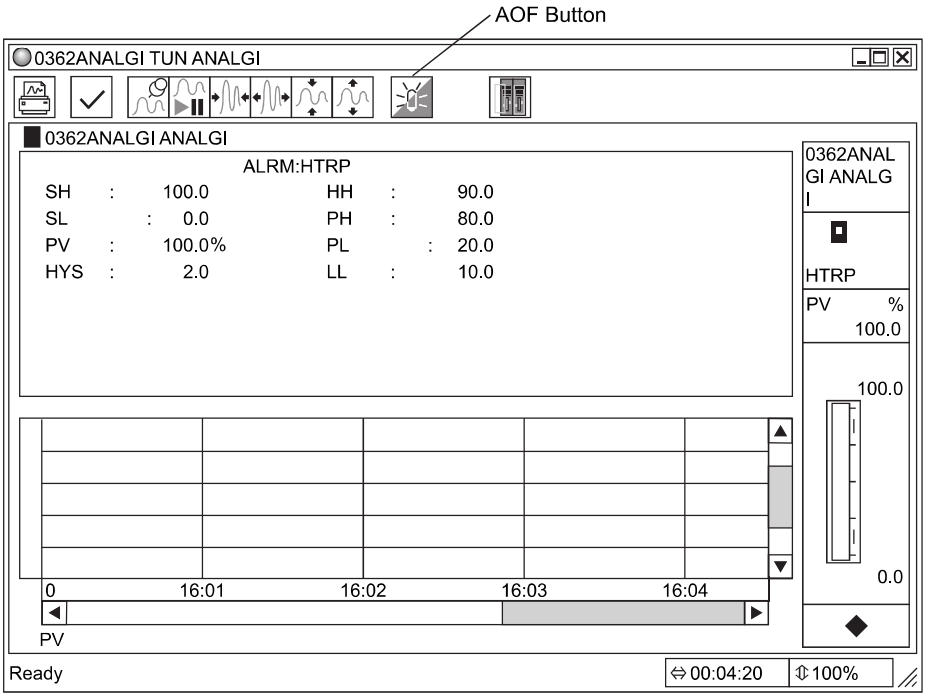


Figure B8.2.4-1 Suppress alarms in a Tuning view

TIP The AOF button only appears when the mapping block/element corresponding to the tag name has the data item of AOFS.

Outputting suppressed alarm messages

On releasing the Alarm Inhibition, the suppressed alarm messages can be output for the process alarms that are still raised. This means that you can confirm the suppressed messages for the process alarms occurred during Alarm Inhibition. The time stamp of a suppressed message shows the time when the message is output upon the release of Alarm Inhibition. Whether to output the suppressed alarm messages can be specified on the SCS Constants Builder.

SEE ALSO For more information about how to make settings required for outputting the suppressed messages, refer to:

C1.2.6, “SCS Constants Builder” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

B8.2.5 Chattering alarm suppression

While a plant is in operation, physical defects such as loosening of the connections of detector terminals and corrosion may lead to unstable input values and cause repeated notification of alarms indicating occurrence and recovery of input errors. As a result, a large number of alarms will appear in the operation and monitoring windows of HIS.

Error occurrence and recovery alarms repeatedly notified are referred to as chattering alarms.

This section explains the function for suppressing the message displays and buzzer sounds of chattering alarms.

Overview of chattering alarm suppression

The chattering alarm suppression function prevents certain system alarm messages and process alarm messages regarding errors detected by the SCS from being displayed in operation and monitoring windows of HIS such as System Message Banner. This function can be used with systems having a CENTUM integration structure.

Alarms for which the display can be suppressed with the chattering alarm suppression function are system alarms and process alarms that are notified upon occurrence and recovery of analog input errors. Specifically, applicable system alarms are channel error alarms, and applicable process alarms are input open (IOP) alarms.

SCS suppresses the display of alarms in the operation and monitoring windows of HIS. Even while the display of alarms is being suppressed, the SCS will still detect occurrence and recovery of errors. Suppression will not affect the operation of application logic, either.

Note that the diagnostic information window of SENG is not subject to alarm display suppression. Even while the SCS is suppressing the display of alarms, system alarms and diagnostic information messages for occurrence and recovery of channel errors will still be displayed in the diagnostic information window of SENG.

Note that this function will not affect the safety functions run by the SCS.

IMPORTANT

The chattering alarm suppression function can be used with combinations of ProSafe-RS R4.03 or later and CENTUM VP R6.04 or later. This function can also be used with databases created using a version of SENG that is R4.03 or later.

SEE ALSO For more information about the operation and monitoring windows of HIS subject to chattering alarm suppression, refer to:

"● Viewers of HIS for which display is suppressed" on page B8-39

Operation during alarm suppression

When an analog input error occurs, an error occurrence alarm is displayed in the operation and monitoring windows of HIS and the SCS enters the chattering alarm suppression period. Even if the error is recovered during the alarm suppression period, unless the recovered state persists for at least the time to chattering recovery notice set by the user, the SCS will continue to suppress the display of error occurrence and recovery alarms in the operation and monitoring windows of HIS.

TIP

The time to chattering recovery notice is the time by which the display of error recovery alarms are delayed. Even if an error is recovered and returned to the normal status during the alarm suppression period, the SCS will not immediately notify an error recovery alarm. Whether the normal status persists for the set time to chattering recovery notice will be monitored. If an error occurs during this time, the SCS will determine that chattering is occurring and continue to suppress alarms. If an error does not occur, the SCS will determine that the error has been recovered and notify an error recovery alarm.

The following figure shows the operation during suppression, which is common to system alarms and process alarms.

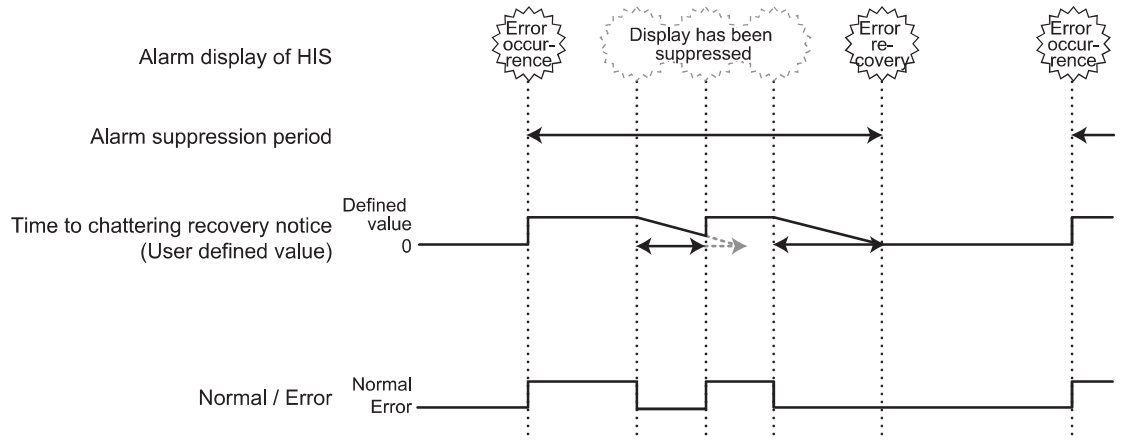


Figure B8.2.5-1 Operation during alarm suppression

Display suppression of channel error alarms

As system alarms, the display of channel error alarms that are notified when detecting the occurrence and recovery of a channel error of the analog input module will be suppressed.

System alarms subject to suppression

The display of the following system alarms can be suppressed with chattering alarm suppression:

- No. 4125 I/O module channel error occurred
- No. 4126 Recovery from I/O module channel error

The following string indicating that the suppression period has ended will be added to the error recovery alarm that is displayed when the alarm suppression period has ended:

(Chattering suppression is over)

Example:

SCS0101 IOM Channel Recover NODE 01 SLOT 02 CH 03 (Chattering suppression is over)

SCS0101 IOM Channel Recover N-IO NODE 01 UNIT 01 SLOT 02 CH 03 (Chattering suppression is over)

SEE ALSO

For more information about details of the diagnostic information messages, refer to:

Message Number 4126 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)

Channels subject to suppression

The channels that can be made subject to suppression of channel error alarms are the analog input channels.

The following table shows the modules and target channels for which channel error alarms can be suppressed.

Table B8.2.5-1 Modules and target channels for which channel error alarms can be suppressed

I/O	Type of module	Model	Target channel
FIO	Analog input module	SAI143/L1AI143, SAV144/ L1AV144, SAT145/L1AT145, SAR145/L1AR145	All channels
N-IO	Analog digital I/O module	S2MMM843	Next signal type channel • Current input • Current input (HART communication)

Operation during channel error alarm suppression

Even if a channel error is recovered after a channel error has occurred with an analog input channel, unless the recovered state persists for at least the time to chattering recovery notice set by the user, the SCS will continue to suppress the display of error occurrence and recovery alarms in the operation and monitoring windows of HIS.

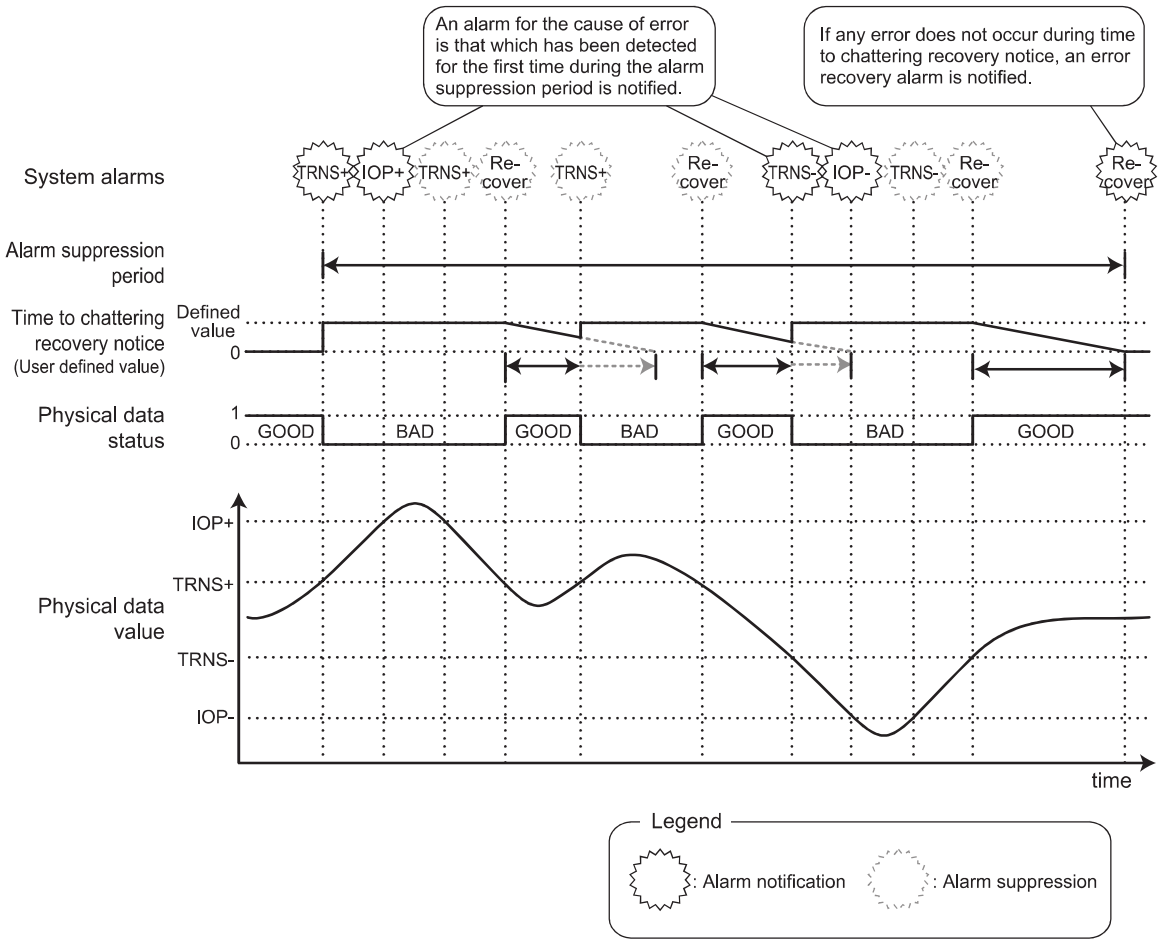


Figure B8.2.5-2 Operation of SCS during channel error alarm suppression

- In a state where alarms are not being suppressed, when a channel error occurs with an input channel, the SCS will notify a channel error occurrence alarm and enter the alarm suppression period. Also, a channel error occurrence alarm will appear in the operation and monitoring windows of HIS.
- If the cause of error is that which has been detected for the first time by the SCS during the alarm suppression period, a channel error occurrence alarm for the cause of error will

appear in the operation and monitoring windows of HIS. If the cause of error is that which has already been detected, the channel error occurrence alarm will not be displayed in the operation and monitoring windows of HIS.

- Even if a channel error is recovered, if a channel error occurs again before the elapse of the time to chattering recovery notice set by the user, the SCS will determine that chattering is occurring and continue alarm suppression. Channel error recovery and occurrence alarms will not be displayed in the operation and monitoring windows of HIS. However, if the cause of error of the channel error is a cause of error that has been detected for the first time during the alarm suppression period, a channel error occurrence alarm for the cause of error will appear in the operation and monitoring windows of HIS.
- If the set time to chattering recovery notice elapses while the channel error remains recovered, a channel error recovery alarm to which a string indicating that the suppression period has ended (Chattering suppression is over) is added will appear in the operation and monitoring windows of HIS.
- The physical data values and physical data status during the alarm suppression period will conform to actual input values.

Display suppression of input open (IOP) alarms

With process alarms, the following will occur. If a tag name has been defined for the instance of the function block entering the analog input (IN), the display of input open (IOP) alarms notified upon a change of the data status will be suppressed.

Process alarms subject to suppression

The display of the following input open (IOP) process alarms can be suppressed with chattering alarm suppression:

- No. 1101 Input process alarm generation
- No. 1102 Input process alarm recovery

Also, during alarm suppression, it is also possible to suppress the display of the following process alarms upon recovery to the NR status:

- No. 1106 Process alarm normal recovery

TIP

- HI and LO pre-alarms and HI and LO trip occurrence and recovery process alarms are not subject to alarm suppression.
- Rewarning alarms are not subject to alarm suppression.

The following string indicating that the suppression period has ended will be added to the error recovery alarm that is displayed when the alarm suppression period has ended:

(Chattering suppression is over)

No.1102

Message name	Input process alarm recovery
Printing example	`A0101A comment PV=4.8 KNM3/H IOP Recover (Chattering suppression is over)`

A0101A: Tag name

Comment: Tag comment

4.8: PV value

KNM3/H: Engineering unit symbol

IOP: Alarm status

Meaning	The alarm display suppression period has ended because the function block indicated by the printed content has been recovered from the alarm status and the time to chattering recovery notice has elapsed.

No.1106

Message name	Process alarm normal recovery
Printing example	`FIC100A comment NR (Chattering suppression is over)`
Meaning	The alarm display suppression period has ended because the function block indicated by the printed content has been recovered from the alarm status and the time to chattering recovery notice has elapsed.

Function blocks with which the alarm suppression function can be used

Function blocks and corresponding mapping blocks with which the input open (IOP) alarm suppression function can be used are shown in the following table.

Table B8.2.5-2 Function blocks and corresponding mapping blocks with which the input open (IOP) alarm suppression function can be used

Function block	Mapping block	Description
ANLG_S	S_ANLG_S	Analog input function block with data status
HSDTR	S_HSDTR	Analog input function block for smoke and heat detectors
GASDTR	S_GASDTR	Analog input function block for gas and flame detectors

Operation during input open (IOP) alarm suppression

Even if the data status of an analog input (IN) of a targeted function block changes from BAD to GOOD, unless the GOOD state persists for at least the time to chattering recovery notice set by the user, the SCS will continue to suppress the display of input open (IOP) alarm occurrence and recovery in the operation and monitoring windows of HIS.

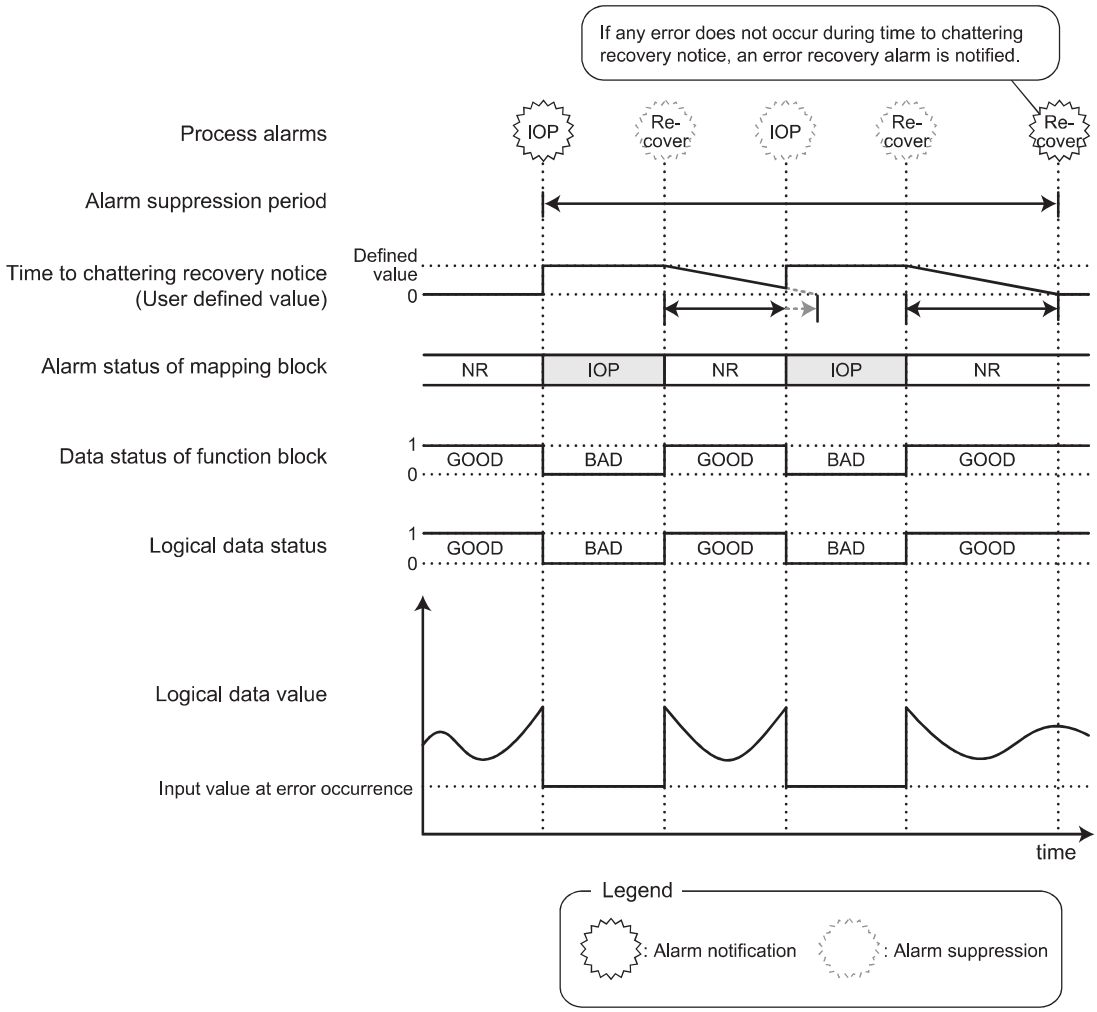


Figure B8.2.5-3 Operation of SCS during input open (IOP) alarm suppression

- In a state where alarms are not being suppressed, if the data status of an analog input (IN) of the function block becomes BAD, the SCS will notify an input open (IOP) alarm from the mapping block and enter the alarm suppression period. Also, an input open (IOP) alarm occurrence will appear in the operation and monitoring windows of HIS.
- Even if the data status of the analog input (IN) becomes GOOD during the alarm suppression period, if the data status becomes BAD again before the elapse of the time to chattering recovery notice set by the user, the SCS will determine that chattering is occurring and continue alarm suppression. Input open (IOP) alarm recovery and occurrence will not be displayed in the operation and monitoring windows of HIS. Process alarm normal recovery will not be displayed either even upon recovery to the NR status.
- If the set time to chattering recovery notice elapses while the data status of the analog input (IN) remains in GOOD, an input open (IOP) alarm recovery and a process alarm normal recovery to which a string indicating that the suppression period has ended (Chattering suppression is over) is added will appear in the operation and monitoring windows of HIS.
- Analog input values, the data status, and output of function blocks will conform to logical data values and the logical data status.

Operation during alarm inhibition (AOF)

The operation when alarm inhibition (AOF) is enabled during chattering alarm suppression with the SCS is as follows:

- While AOF is enabled, even if the data status of an analog input (IN) becomes BAD, the chattering alarm suppression function targeted at process alarms will not operate.
- The chattering alarm suppression function will be disabled when AOF is enabled during the alarm display suppression period for process alarms. After this, operation will follow that of AOF.
  Note that if in the normal status AOF is enabled during the alarm display suppression period based on this function, at this time the SCS will notify the error recovery alarm for the end of the suppression period. However, as process alarms will be suppressed by AOF, an error recovery alarm will not be displayed in the operation and monitoring windows of HIS.

TIP

The chattering alarm suppression function targeted at system alarms will not be affected by AOF.

Method of monitoring with HIS

This section explains the viewers of HIS for which display is suppressed when the chattering alarm suppression function is enabled along with how to confirm alarms that have been suppressed.

Viewers of HIS for which display is suppressed

The types of viewers and alarms of HIS for which display is suppressed with chattering alarm suppression are shown in the following table.

Table B8.2.5-3 Types of viewers and alarms of HIS for which display is suppressed

Viewers	Alarms subject to suppression
System message banner Message controls in graphic views UACS (Unified Alarms & Conditions Server) CAMS for HIS message monitor of consolidated alarm management	System alarms and process alarms
System alarm view Individual system alarm message acknowledgment window	System alarms
Process alarm view Individual process alarm message acknowledgment window	Process alarms

Confirming alarms for which display has been suppressed

The following display functions are not subject to chattering alarm suppression. By using the following display functions, even during chattering alarm suppression, it is possible to confirm the alarms for which display has been suppressed:

- Message monitor window
- Historical message display functions (such as the historical message report window)
- SOE viewer
- Diagnostic information window of SENG (*1)

*1: System alarms are subject to display. Process alarms cannot be confirmed.

TIP

With display functions not subject to chattering alarm suppression, suppressed error recovery alarms and the error recovery alarms for when the suppression period has ended are displayed continuously. Both of the error recovery alarms will have the same message number. A string indicating that the suppression period has ended (Chattering suppression is over) will be added to the error recovery alarm that is displayed when the alarm suppression period has ended.

Engineering

To enable the chattering alarm suppression function, set the time to chattering recovery notice with SENG.

Suppression of system alarms and suppression of process alarms are independent of each other. The time to chattering recovery notice needs to be set for each of the system alarms or process alarms to suppress.

To suppress the system alarms and process alarms for the occurrence and recovery of channel errors of a certain analog input, set the time to chattering recovery notice as the same value for each so that the alarm suppression period is the same for both.

Suppression of system alarms can be set with I/O Parameter Builder or Safety I/O Editor.

Suppression of process alarms can be set with Tag Name Builder or iDefine.

IMPORTANT

Set the time to chattering recovery notice upon considering an appropriate value with the alarm design of the plant. Necessary alarms may not be notified if the time to chattering recovery notice is not an appropriate value.

SEE ALSO

For more information about setting items of the I/O Parameter Builder, refer to:

"■ Time to Chattering Recovery Notice (s) (Time to Chattering Recovery Notice)" in Appendix 1.3.2, "Settings for the AI channel" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about setting items of the Safety I/O Editor, refer to:

"■ Setting items of the Safety I/O Editor" in D1.4.1, "Starting the Safety I/O Editor" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about setting items of the Tag Name Builder, refer to:

"● Time to Chattering Recovery Notice (s)" on page B7-26

Operation upon online change download

This section explains operation of the chattering alarm suppression function when an online change download is performed after the following operations:

- Changing the chattering alarm suppression function to enabled
- Changing the chattering alarm suppression function to disabled

● Changing the chattering alarm suppression function to enabled

If the chattering alarm suppression function is enabled while the targeted channel or function block is in a state of error, alarms will be suppressed in the following manner in the operation and monitoring windows of HIS:

- For system alarms
  If the chattering alarm suppression function is enabled while the targeted channel is in a state of error, display will be suppressed from the next error recovery alarm. If an error occurs again during the suppression period, operation will differ depending on the cause of error. An error occurrence alarm is displayed if the cause of error differs from that of the error occurrence alarm prior to enabling this function. If the cause of error is the same, an error occurrence alarm will not be displayed.

TIP

If this function is enabled while the targeted channel is in a state of error, the error occurrence alarm displayed prior to enabling this function will be the first error occurrence alarm.

- For process alarms
  If the chattering alarm suppression function is enabled while the targeted function block is in a state of error, display will be suppressed from the next error recovery alarm. If an error occurs again during the suppression period, an error occurrence alarm will not be displayed.

SEE ALSO

For more information about operation of system alarms when the chattering alarm suppression function is enabled while the target channel is in the normal status, refer to:

"● Operation during channel error alarm suppression" on page B8-35

For more information about operation of process alarms when the chattering alarm suppression function is enabled while the target function block is in the normal status, refer to:

"● Operation during input open (IOP) alarm suppression" on page B8-37

● Changing the chattering alarm suppression function to disabled

If the chattering alarm suppression function is disabled, depending on the status of the SCS and alarm suppression when the change is made, an alarm will be displayed at the following timing in the operation and monitoring windows of HIS:

- If the function is disabled when in the normal status and not during the alarm suppression period, display will be restored from the next occurrence of an error occurrence alarm.
- If the function is disabled when in the normal status and during the alarm suppression period, the error recovery alarm for when the suppression period has ended will appear immediately.
- If the function is disabled when in the error status, display will be restored from the next occurrence of an error recovery alarm.

■ Operation during unsteady state of SCS

If the SCS enters the following unsteady state during chattering alarm suppression, the elapsed time of the time to chattering recovery notice is reset:

- Initial cold start of the SCS
- Occurrence of a path error such as a node error, unit error, or IOM error

C. SOE OPC Interface

The SOE OPC Interface provides the functions of the OPC (OLE for Process Control) server that handles event information and diagnostic information that are acquired through the sequence of event recorder (SOER) function of SCSs. OPC clients can access this information by using the OPC Interface.

C1. Overview of SOE OPC Interface

By using the SOE OPC Interface (server) provided by ProSafe-RS, it is possible to access event information and diagnostic information of SCS from OPC applications (clients) on the host computer.

This section explains the specifications of ProSafe-RS SOE OPC Interface and compatibility with the OPC specifications. The OPC specifications can be obtained from the web site of the OPC Foundation.

TIP

OPC (OLE for Process Control) is an OLE (Object Linking and Embedding) specification, i.e., a method of standard communication between applications in Windows environments, which is specifically applicable to process control. OPC allows sending/receiving process data among multiple general-purpose Windows-compatible applications.

What is the SOE OPC Interface?

The SOE OPC Interface provided by ProSafe-RS consists of the OPC server and SOE cassette dedicated to ProSafe-RS.

- OPC server
  The OPC server notifies event information and diagnostic information that is acquired from SCSs to OPC clients. The OPC server consists of the Alarms & Events server (hereinafter referred to as A&E server), which accesses various data, and Historical Data Access server (hereinafter referred to as HDA server), which stores historical data.
- ProSafe-RS SOE cassette
  The SOE cassette dedicated to ProSafe-RS is incorporated in the cassette provided by the OPC Interface as communication interface.
- Function of the SOE cassette
  The SOE cassette provides communication functions for notifying SOE events and diagnostic information of SCS to the OPC server. By connecting to the OPC server equipped with this cassette, OPC clients can receive event messages (SOE events and diagnostic information) of SCS.

System configuration using the SOE OPC Interface

The SOE OPC Interface runs on a computer and reports SCS event information and diagnostic information to the host computer through the OPC Interface.

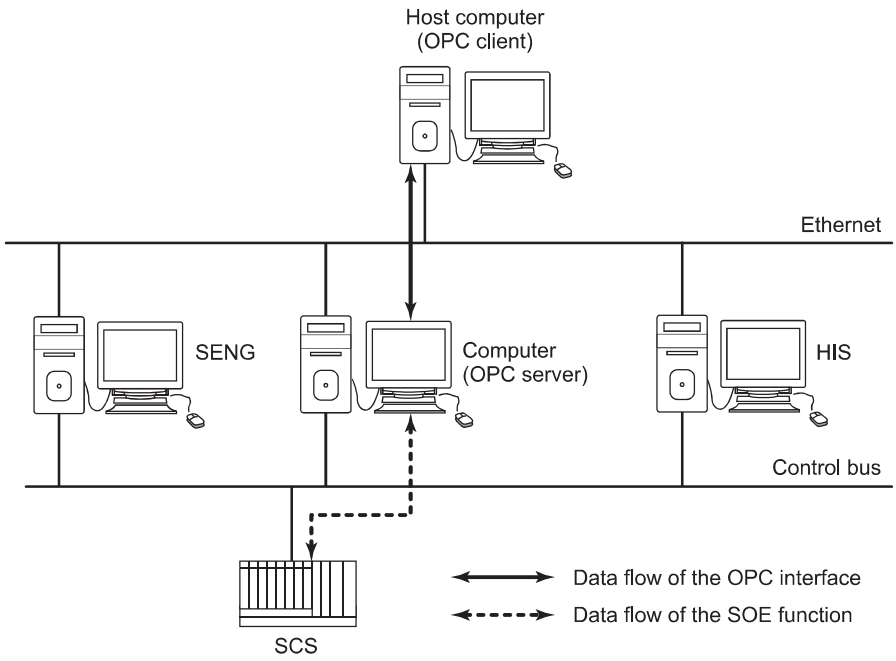


Figure C1-1 Example of system configuration using the SOE OPC Interface

Software configuration of the SOE OPC Interface

The SOE OPC Interface is comprised of the OPC server and the ProSafe-RS SOE cassette (hereinafter referred to as SOE cassette). The OPC server sends data to the OPC client. The SOE cassette is an interface used by the OPC server to acquire data from SCS. The following figure shows the software configuration for the SOE OPC Interface.

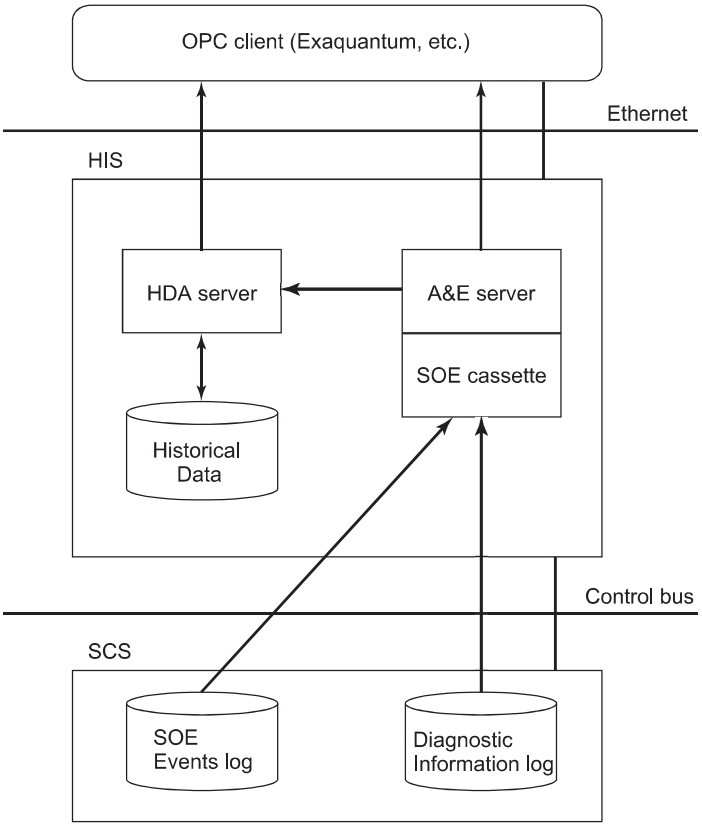


Figure C1-2 Software configuration and data flow

Details of the SOE OPC Interface

Particular items of the SOE OPC Interface are explained below, including parameters and control method required when constructing the system with the SOE OPC Interface.

OPC interface

The following OPC-compliant interface is provided:

- Alarms and Events (A&E)
  This interface notifies event messages, which are generated asynchronously by SCS, to the host computer. The SOE cassette reads the event log on SCS at regular intervals (the default is 10 seconds) and notifies changes (e.g., that new event messages are generated) to the client.

  The A&E server provides OPC A&E custom interfaces and OPC A&E automation interfaces.

- Historical Data Access (HDA)
  This interface stores event messages, which are generated asynchronously by SCS, in the historical database. This operation enables OPC clients to receive missed event messages.

Application capacity

The following table shows the application capacity limits.

Table C1-1 Application capacity

Item	Capacity
Maximum number of connected clients	100 clients
Maximum number of event registration objects (*1)	1000/OPC server
Maximum number of registered event generation sources (*2)	100/registration object

*1: It is the maximum number of event registration objects (subscription) that can be created in the CreateEventSubscription method.
*2: It is the maximum number of event generation sources that can be specified in subscription when setting up a filter in the event generation source. The maximum number of event generation sources (dwNumSources) in the SetFilter method is checked.

Server name (ProgID), type library name

The server name and type library name for the A&E server are as follows: The server name is used for custom interfaces. The type library name is used by the automation interfaces in applications such as Visual Basic and Excel.

- The custom interfaces
  Server name: Yokogawa.ExaopcAESCSSOE
- The automation interfaces
  Type library name: Yokogawa ProSafe-RS SCS Alarms & Events Automation Server

The server name and type library name for the HDA server are as follows:

- The custom interfaces
  Server name: Yokogawa.ExaopcHDASCSSOE
- The automation interfaces
  Type library name: Yokogawa ProSafe-RS SCS HDA Server

Event categories and event types

The following table shows support for event categories and event types for SOE cassettes. The event category of system alarms generated in the SOE cassette is "System alarms (101)."

Table C1-2 Event category and event type

Event category		Event type	Description
Name	Value		
System alarms	101	Simple(=1)	Diagnostic Information
Sequence of events	110	Simple(=1)	Event Information

Source (event generation sources)

This item contains the same reference as displayed in SOE Viewer. In the case of system alarms generated in the SOE cassette, the ProgID value (Yokogawa.Exaopc AESCSSOE) is stored in this item.

Time (event generation time)

This item contains the same time stamp (SCS time) as displayed in SOE Viewer. The time stamp is stored using UTC (Universal Time Coordinated).

The time stamp based on the computer time is stored using UTC in the case of system alarms generated in the SOE cassette.

Severity (event priority)

This item contains a value from 200 to 900 to indicate the severity of the alarm or event. 900 is stored in the case of system alarms generated in the SOE cassette.

Table C1-3 Event category and severity

Event category	Severity level	Description
Name		
System alarms	900	Diagnostic Information (class 1)
	500	Diagnostic Information (class 2)
	300	Diagnostic Information (class 3)
	200	Diagnostic Information (class 4)
Sequence of events	500	Event Information

Message

All SCS-generated event messages displayed in the SOE Viewer as the character string are stored, including all system alarm messages generated in the SOE cassette.

Event description and attributes

The following table summarizes SOE event attributes for events reported by the OPC interface.

Table C1-4 Event attributes of diagnostic information

Attribute name	OPC ID	VARIANT type	Remark
SOETimestamp	301	VT_DATE	Event Occurrence Date (Local)
TimestampM	302	VT_I2	Event Occurrence Time (Millisecond)

Continues on the next page

Table C1-4 Event attributes of diagnostic information (Table continued)

Attribute name	OPC ID	VARIANT type	Remark
Resource	303	VT_BSTR	The same as the corresponding information displayed in SOE Viewer (*1)
Type	304		
ID	305		
Quality	306		
Node	308	VT_I2	Node position, or 0
Slot	309	VT_I2	Slot position, or 0
Time_Diff	318	VT_BSTR	Time zone (-08:00, +00:00, +09:00, ...)

*1: Resource (computer name), Type (fixed to BSYS), ID/Quality (blank) SOETimestamp, TimestampM and Time_Diff (computer time) are stored in the case of alarms generated in the SOE cassette.

Table C1-5 Event attributes of event information

Attribute name	OPC ID	VARIANT type	Remark
SOETimestamp	301	VT_DATE	Event Occurrence Date (Local)
TimestampM	302	VT_I2	Event Occurrence Time (Millisecond)
Resource	303	VT_BSTR	The same as the corresponding information displayed in SOE Viewer
Type	304		
ID	305		
Quality	306		
Node	308	VT_I2	Node position (DI/DO event only), or 0
Slot	309	VT_I2	Slot position (DI/DO event only), or 0
Channel	310	VT_I2	Channel position (DI/DO event only), or 0
TripMark	313	VT_I2	True/false of tripping signal (1/0)
Time_Diff	318	VT_BSTR	Time zone (-08:00, +00:00, +09:00, ...)

Formats for system alarms generated in the SOE cassette

The SOE cassette generates a system alarm when access to SCS event logs fails. The system alarm is notified to the OPC client. The following example shows the message format for this system alarm.

- Event Category: 101 (System alarms)
- Event Type: 1 (Simple)
- Source: Yokogawa.ExaopcAESCSSOE
- Time: (Computer time)
- Severity: 900
- Message: Database Connection Error `ERR=0x80004005`
  Database Connection Recover
- SOETimestamp (Event Attribute): (Computer time) Event Occurrence Date (Local)
- TimestampM (Event Attribute): (Computer time) Event Occurrence Date (Millisecond)
- Resource (Event Attribute): (Computer name)
- Type (Event Attribute): BSYS
- ID (Event Attribute): (Blank)
- Quality (Event Attribute): (Blank)
- Node (Event Attribute): 0

- Slot (Event Attribute): 0
- Time_Diff (Event Attribute): (Computer time) Time zone (-08:00, +00:00, +09:00, ...)

SEE ALSO For more information about CPU load balancing for the SOE cassette, refer to:

C2.4, “Connection with host system computer via an OPC server” on page C2-10

Event notification interfaces

The SOE cassette notifies event information and diagnostic information of SCS to the A&E server. It also provides a function for filtering each event.

Available interfaces

The following tables show the custom interfaces available to A&E server clients, based on the functions that are installed on the SOE cassette.

Table C1-6 Custom interfaces

Object	Interface	Method	Description	Support(*1)
OPCEventServer	IOPCCommon	SetLocaleID	Locale ID setting	Yes
		GetLocaleID	Locale ID acquisition	Yes
		QueryAvailableLocaleIDs	Inquiry about supported locale IDs	Yes
		GetErrorString	Error character string acquisition	Yes
		SetClientName	Client name setting	Yes
	IOPCEventServer	GetStatus	Server status acquisition	Yes
		CreateEventSubscription	Generation of Event Subscription object	Yes
		QueryAvailableFilters	Inquiry about items that can be filtered	Yes
		QueryEventCategories	Inquiry about event categories	Yes
		QueryConditionNames	Inquiry about condition names	Yes
		QuerySubConditionNames	Inquiry about sub-condition names	Yes
		QuerySourceConditions	Inquiry about condition names corresponding to a source name	Yes
		QueryEventAttributes	Inquiry about event attributes	Yes
		TranslateToItemIDs	Item ID translation/acquisition	Yes
		GetConditionState	Acquisition of condition status	Yes
		EnableConditionByArea	Condition Enable for a specified area	No
		EnableConditionBySource	Condition Enable for a specified source	Yes
		DisableConditionByArea	Condition Disable for a specified area	No
		DisableConditionBySource	Condition Disable for a specified source	Yes
		AckCondition	Notification of condition acknowledgment	No
		CreateAreaBrowser	Generation of Event Area Browser object	No
		IOPCSecurityNT	Access control interface that uses NT credit information	Yes
		IOPCSecurityPrivate	Access control interface that uses private-defined user name/password	Yes
	IConnectionPointContainer	EnumConnectionPoints	Creation of enumerator that scans connection points	Yes
		FindConnectionPoint	Acquisition of interface pointers to connection points	Yes
	IConnectionPoint	Advise	Connection between connection point and sink	Yes
		Unadvise	Disconnection between connection point and sink	Yes

Continues on the next page

Table C1-6 Custom interfaces (Table continued)

Object	Interface	Method	Description	Support(*1)
OPCEventServer	IOPCSecurityNT	IsAvailableNT	Inquiry about availability of OPC security function by NT credit information	Yes (*2)
		QueryMinImpersonation-Level	Inquiry about impersonation level	No
		ChangeUser	Notification of user credit information changes	No
	IOPCSecurityPrivate	IsAvailablePriv	Inquiry about availability of OPC security function by private credit information	Yes
		Logon	Logon request by client user	Yes
		Logoff	Logoff request by client user	Yes
OPCEventAreaBrowser (option)	IOPCEventAreaBrowser	ChangeBrowsePosition	Change of browser position	No
		BrowseOPCAreas	Acquisition of area list	No
		GetQualifiedAreaName	Acquisition of Area name	No
		GetQualifiedSourceName	Acquisition of Source name	No
OPCEventSubscription	IOPCEventSubscriptionMgt	SetFilter	Event filter setting	Yes
		GetFilter	Acquisition of event filter	Yes
		SelectReturnedAttributes	Selection of event attribute	Yes
		GetReturnedAttributes	Acquisition of selected event attribute	Yes
		Refresh	Event refresh request	Yes
		CancelRefresh	Cancellation of refresh request	Yes
		GetState	Acquisition of the status of Event Subscription object	Yes
		SetState	Set the status of Event Subscription object	Yes
	IConnectionPointContainer	EnumConnectionPoints	Creation of enumerator that scans connection points	Yes
		FindConnectionPoint	Acquisition of interface pointers to connection points	Yes
	IConnectionPoint	Advise	Connection between connection point and sink	Yes
		Unadvise	Disconnection between connection point and sink	Yes
OPCEventSink	IOPCEventSink	OnEvent	Event notification	Yes
OPCShutdown	IOPCShutdown	ShutdownRequest	Server shutdown notification	Yes

*1: Yes: supported
No: Not supported
*2: The IsAvailableNT method of the IOPCSecurityNT interface always returns FALSE.

Filters

You can specify the following filtering conditions:

Table C1-7 Filtering conditions

Mask	Description
OPC_FILTER_BY_EVENT	Filtering by Event type

Continues on the next page

Table C1-7 Filtering conditions (Table continued)

Mask	Description
OPC_FILTER_BY_CATEGORY	Filtering by Event category
OPC_FILTER_BY_SEVERITY	Filtering by Alarm severity
OPC_FILTER_BY_SOURCE	Filtering by Source name

OPC A&E automation interfaces

The OPC Foundation released a draft version of the OPC A&E automation interfaces. YOKOGAWA provides the OPC A&E automation interfaces that comply with the draft specifications.

Error codes

The following tables show error codes handled by the SOE cassette. Each error code is set as a return value of a function of the SOE cassette interface or a data error value of each data.

OPC error codes

The following OPC error codes are used by the SOE cassette:

Table C1-8 COM error codes

COM error codes used by OPC server	Description
E_FAIL	General errors (without specific codes)
E_INVALIDARG	Invalid parameter
E_NOTIMPL	Unsupported function
E_OUTOFMEMORY	Insufficient memory

Table C1-9 OPC error codes

OPC error code	Description
OPC_E_BADRIGHTS	No access right
OPC_E_BADTYPE	Invalid request type
OPC_E_INVALIDITEMID	Invalid item ID
OPC_E_INVALID_PID	Invalid parameter ID
OPC_E_UNKNOWNITEMID	Undefined item ID specified

SOE cassette definition error codes

The following cassette definition error codes are used in the SOE cassette:

Table C1-10 SOE cassette definition error codes

Code (xxxx-x999)	Symbol (ZOT_XL_E_XXXX)	Description
0xC0042329	ZOC_AE_E_MAXSERVER	Excessive number of clients connected to the A&E server
0xC004232A	ZOC_AE_E_MAXSUBSCRIPTION	Excessive number of event registration objects of the A&E server

Error code bit assignment

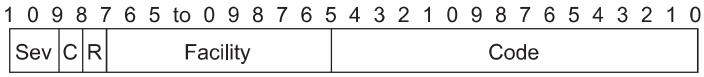
The bit assignment in the error codes is as follows:

Code:

0000 to 0200: For Microsoft

0200 to 7999: For OPC definition errors

9000 to 9999: For the A&E server



Sev - is the severity code
00 - Success
01 - Informational
10 - Warning
11 - Error
C- is the Customer code flag
R- is a reserved bit
Facility- is the facility code (=FACILITY_ITF)
Code- is the facility's status code

Figure C1-3 Bit assignment in error codes

C2. Setup for using the OPC server

Setup is required to connect the SOE OPC Interface server (hereinafter referred to as SOE OPC server) and OPC client products. This section describes the setting items of the SOE OPC Interface required to use the OPC server, setting procedures, and operations after the settings are completed.

C2.1 Settings of the SOE OPC Interface

You can configure operation parameters of the SOE cassette by using the operation parameter setting tool that is included in the SOE OPC interface. This section describes how to use this tool to configure the settings for connecting the SOE OPC server and OPC client products.

Settings of operation parameters

Use the operation parameter setting tool to configure the operation parameters for the A&E server and HDA server.

1. Start SOE OPC Parameter Setting.
   The SOE OPC Interface Settings dialog box appears.

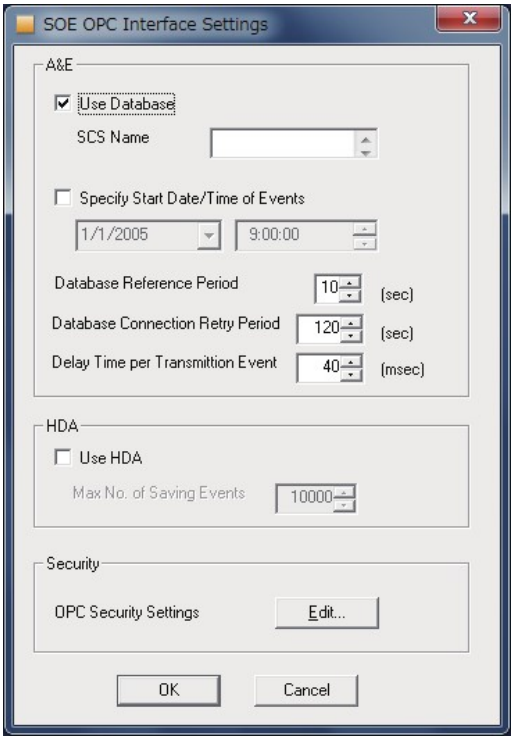


Figure C2.1-1 SOE OPC Interface Settings dialog box

2. Specify operation parameters for the A&E server and HDA (Historical Data Access) server.

SEE ALSO For more information about items set for the HDA server, refer to:

"● Items set for the HDA server" on page C2-3

● Items set for the A&E server

This section describes the setting items in the SOE OPC Interface Settings dialog box that relate to the A&E server.

- Use Database
  Always select this check box because the SOE OPC server is an A&E server.

  The check box is selected by default.

- SCS Name
  This field becomes enabled only if you select the [Use Database] check box. List the names of SCSs to be referenced (separated by space, comma or period).

Example:

SCS0101, SCS0102

The event logs of the SCSs selected here become the target of notification.

- Specify Start Date/Time of Events
  Select this check box to change the date/time of the first event to be acquired. If this box is selected, all events after the specified date/time are sent to the client. If the box is not selected, events after the computer time when restarting the SOE cassette are sent to the client.

  The check box is not selected by default.

- Date/Time Specification
  These fields become enabled only if you select the [Specify Start Date/Time of Events] check box. Specify the date and time of the first event.

  The time when you select the [Specify Start Date/Time of Events] check box is set by default.

- Database Reference Period
  Specify the period in units of seconds if you want to change the database reference period.

  A value in the range from 1 to 600 seconds can be specified. 10 seconds is set by default.

- Database Connection Retry Period
  Specify the time interval in seconds to retry reconnection to the database in case the connection to the database fails or the connection to the database is disconnected.

  A value in the range from 1 to 1800 seconds can be specified. 120 seconds is set by default.

- Delay Time Per Transmission Event
  This is the delay time for a single transmission event. Specify the time in units of milliseconds if you want to change the setting.

  A value in the range from 0 to 1000 milliseconds can be specified. 40 ms is set by default.

  Specify an appropriate value according to the load on the computer.

  - If you make the "Delay Time Per Transmission Event" longer, it takes more time to send events and the CPU load is reduced.
  - If you make the "Delay Time Per Transmission Event" shorter, it takes less time to send events and the CPU load is increased.

Items set for the HDA server

This section describes the setting items in the SOE OPC Interface Settings dialog box that relate to the HDA server.

- Use HDA
  Select this check box when the HDA functions should be used.

- Max No. of Saving Events
  This field becomes enabled only if you selected the [Use HDA] check box. Specify the maximum number of events that the HDA server should maintain. If more events than the maximum number of events saved are generated, events are overwritten starting from the oldest event. A value in the range from 1000 to 1000000 can be specified. 10000 is set by default.

IMPORTANT

Determine the maximum number of saving events based on the disk capacity and the search speed of the HDA server. An event uses approximately 500 bytes of disk space, which means that 10000 events use approximately 5 MB. When there are many events, file searches takes longer.

C2.2 Overview of product security settings

Product security settings are required to connect the SOE OPC server and OPC client products. This section describes the settings required on the SOE OPC server side.

You can configure the OPC product security and DCOM connection settings using the operation parameter setting tool that is included in the SOE OPC Interface.

Product security setting procedure

Follow these steps to configure the product security settings on the SOE OPC server:

1. Log on as a user with administrative rights. If the standard model of security settings are applied, log on as a user who belongs to the PSF_ENGINEER or PSF_ENGINEER_LCL group.
2. Start SOE OPC Parameter Setting.
   The SOE OPC Interface Settings dialog box appears.
3. Click the [Edit] button next to [OPC Security Settings].
   A dialog box to select the logon type for the OPC server appears.

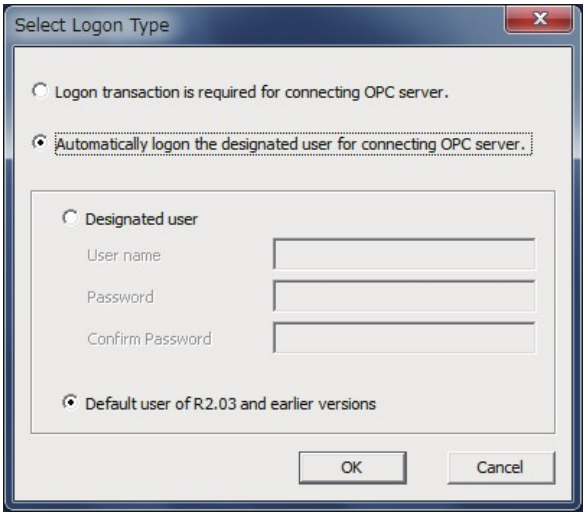


Figure C2.2-1 Select Logon Type dialog box

4. Configure the logon type settings for the OPC server according to the security level. The following table shows the setting items in the dialog box and precautions for setting the items.

Table C2.2-1 Setting items and precautions

Item	Description	Precautions
Logon transaction is required for connecting OPC server.	Select this option if you need to log on when connecting to the OPC server	Calls of Logon and SetUser methods on the OPC client are required to select this option. Do not select this option if the OPC client does not support the calls of Logon and SetUser methods.
Automatically logon the designated user for connecting OPC server.	Select this option to enable automatic logon when connecting to the OPC server	After the automatic logon is enabled, select one of the following logon methods. • Designated user • Default user of R2.03 and earlier versions

Continues on the next page

Table C2.2-1 Setting items and precautions (Table continued)

Item	Description	Precautions
Designated user	Select this option to designate a user for automatic logon	Specify the user name and password that is used for automatic logon. If periodic password change is required, you must respecify this password accordingly. This applies to the case of domain management in Windows authentication mode. Make sure to note the password expiration date.
Default user of R2.03 and earlier versions	Select this option to ensure compatibility with ProSafe-RS R2.03 or earlier.	This option is selected by default when automatic logon is enabled for connecting to the OPC server. Note that this setting may result in a reduced level of security.

TIP

To connect a computer that is installed with the SOE OPC interface package for ProSafe-RS R3.01 or later to Exaquantum or Exaquantum/SER as an OPC client, you need to set the items for product security in advance. When using Exaquantum, you must select [Default user of R2.03 and earlier versions].

SEE ALSO

For more information about security settings required when using Exaquantum as an OPC client, refer to:

D1.4.1, “ProSafe-RS SOE OPC Interface Package and Exaquantum PIMS Server” in Installation Guide (IM 32P01C50-01EN)

DCOM settings

In ProSafe-RS R3.02 or later, the IT security of the SOE OPC server is strengthened. Thus, depending on the OPC client used, the connection to the server may fail after R3.02 or later is installed. If the connection fails, configure the DCOM settings on the OPC server. You must restart the computer after you finish configuring the settings.

This section describes the DCOM setting procedures for different combinations of security models and user management methods.

DCOM setting procedure for legacy model

If the SOE OPC server security model is the legacy model, DCOM settings are configured by the IT security setting tool. No manual configuration is required.

DCOM setting procedure for the standard model under standalone management

This section describes the DCOM setting procedure when the SOE OPC server security model is the standard model and the user management method is standalone management. Follow these steps to configure if connection to OPC clients fails after ProSafe-RS R3.02 or later is installed:

1. Open the Control Panel.
2. Select [System and Security] > [Administrative Tools] > [Component Services].
   The Component Services window appears.
3. In the hierarchy tree, expand [Component Services] > [Computers] > [My Computer] > [DCOM Config].

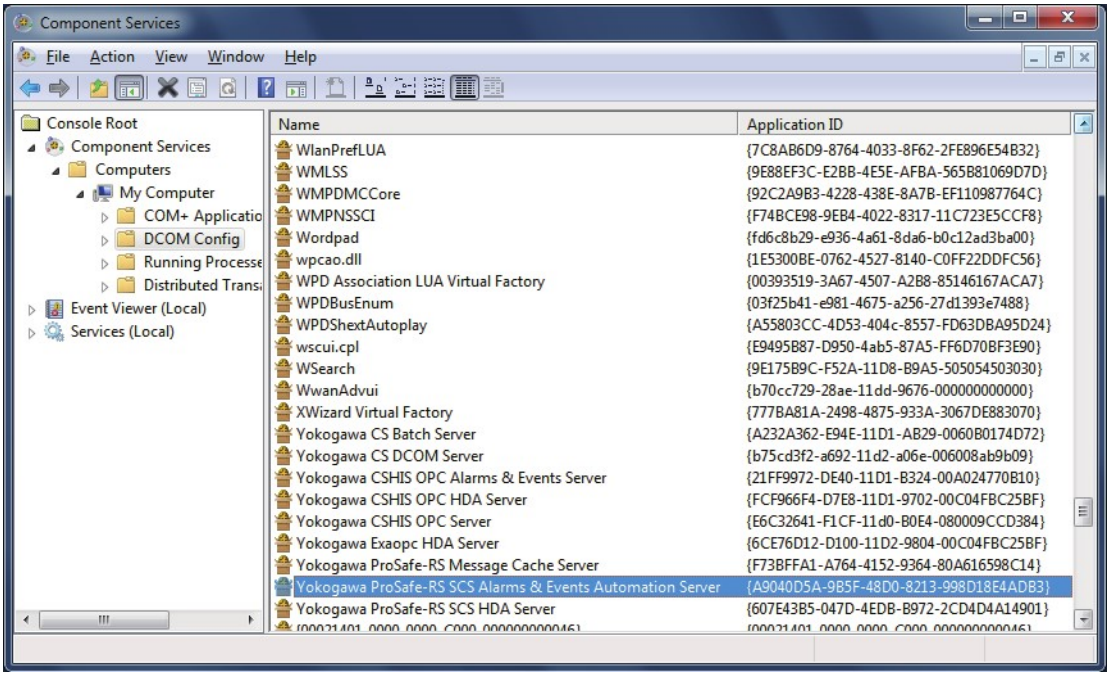


Figure C2.2-2 DCOM Config

4. Select Yokogawa ProSafe-RS SCS Alarms & Events Automation Server, and select [Properties] from the right-click menu.
   The Properties dialog box appears.

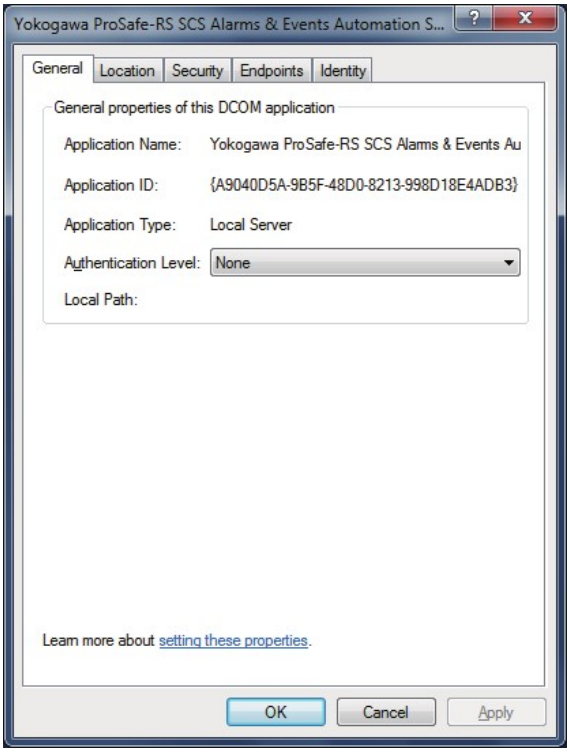


Figure C2.2-3 Yokogawa ProSafe-RS SCS Alarms & Events Automation Server Properties dialog box

5. Click the General tab, set the Authentication Level to [None], and click [OK].
6. Specify Yokogawa ProSafe-RS SCS HDA Server in Application Name, and select [Properties] from the right-click menu.
   The Properties dialog box appears.

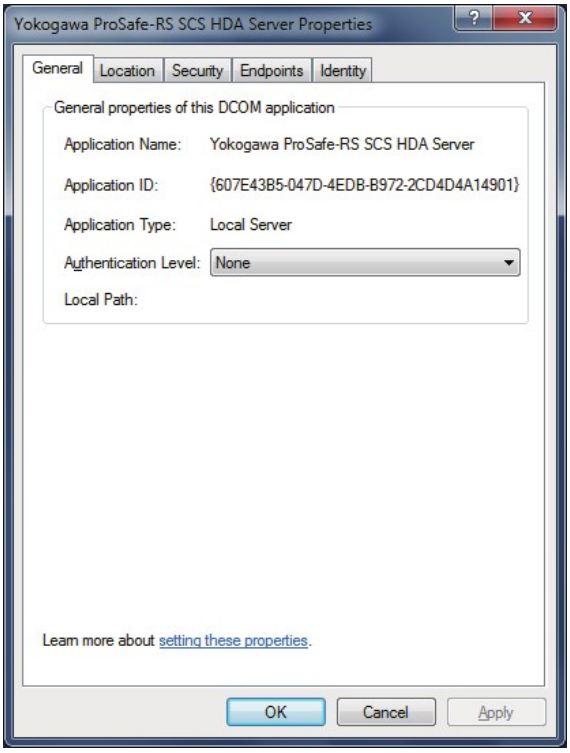


Figure C2.2-4 Yokogawa ProSafe-RS SCS HDA Server Properties dialog box

7. Click the General tab, set the Authentication Level to [None], and click [OK].
8. Restart the computer.

● DCOM setting procedure for standard model under domain management

The DCOM setting procedure when the SOE OPC server security model is the standard model and the user management method is domain management is the same as when the security model is the standard model and the user management method is standalone management.

SEE ALSO For more information about DCOM setting procedure for the standard model under standalone management, refer to:

"● DCOM setting procedure for the standard model under standalone management" on page C2-6

● DCOM setting procedure for standard model under combination management or linked domain management

The DCOM setting procedure when the SOE OPC server security model is the standard model and the user management method is either combination management or linked domain management is the same as when the security model is the standard model and the user management method is standalone management.

SEE ALSO For more information about DCOM setting procedure for the standard model under standalone management, refer to:

"● DCOM setting procedure for the standard model under standalone management" on page C2-6

C2.3 Operations after operation parameters are configured

This section describes how the SOE OPC Interface operates after the operation parameters are configured.

Operations when the operation parameter setting tool is launched

When the operation parameter setting tool is launched for the first time, all the items are set to their default values. When you launch the tool the next time, the tool displays all items according to the settings the user made last time.

The [Specify Start Date/Time of Events] check box is deselected when the SOE cassette starts to send events.

Operations when changing parameters

When using the operation parameter setting tool to change operation parameters for the SOE cassette, the SOE OPC interface restarts when you click the [OK] button in the operation parameter setting tool.

Events generated while the SOE OPC interface is restarting are not sent to the client. If you want to send events generated during the SOE OPC interface restart processing (approximately 1 to 2 minutes) to the client, specify the [Specify Start Date/Time of Events] setting item for the A&E server. The current time can be set by selecting/deselecting the [Specification of Head Event Date/Time] check box.

TIP

The same information will not be sent again if the SOE OPC interface is restarted with the same date/time as previously specified.
To resend the past events, check the [Specify Start Date/Time of Events] box and specify the date and time again.

C2.4 Connection with host system computer via an OPC server

ProSafe-RS connects with a host system computer via OPC interface. The following two OPC interfaces are available.

- Connection through SOE OPC interface package (RS4H2200)
  Enables OPC-compatible application (client) on the host system computer to access diagnostic data and event data (SOE) on SCS.
- Connection through Exaopc OPC interface (VP6H2411 for HIS, or NTPF100)
  Enables OPC-compatible application (client) on the host system computer to access various data such as process data and alarm messages on SCS in the same manner as data on the FCS.

This section primarily describes the SOE OPC Interface Function.

SEE ALSO For more information about Exaopc OPC interface, refer to:

NTPF100 Exaopc OPC Interface Package Guide Manual (IM 36J02A11-01E)

Overview of OPC Interface

The following figure shows the overview of the OPC Interface.

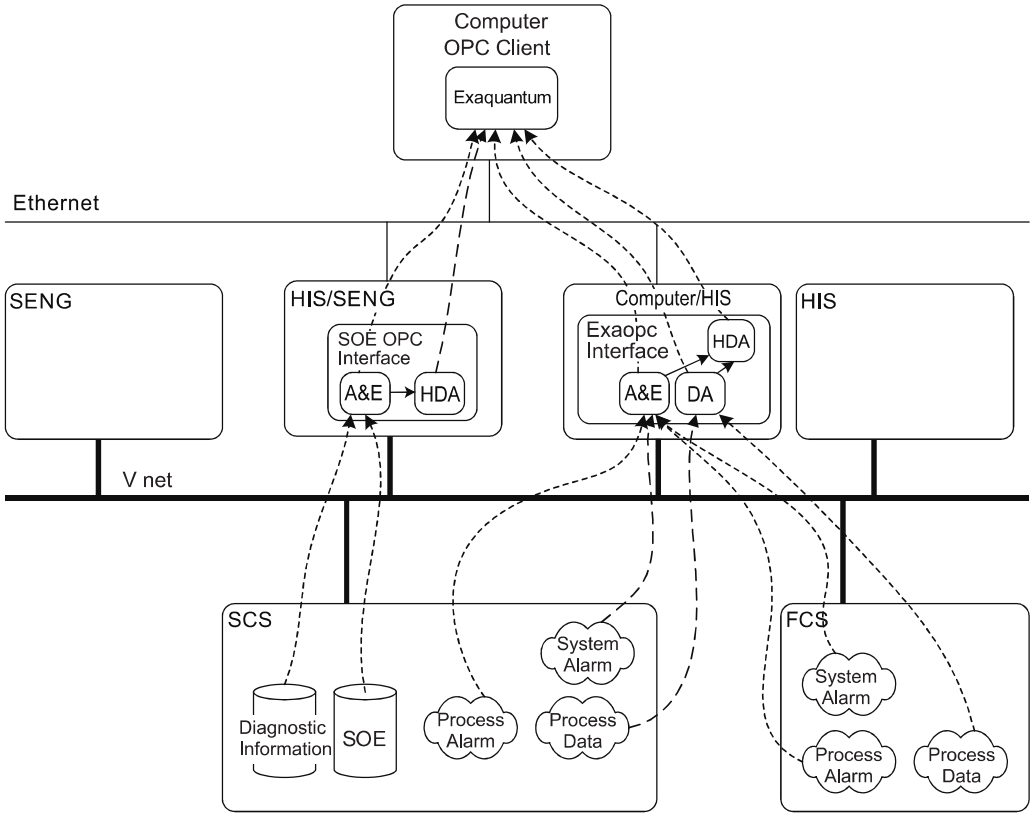


Figure C2.4-1 Overview of OPC Interface

SOE OPC interface (RS4H2200)

SOE OPC Interface package for ProSafe-RS notifies the client computer of diagnostic data and event data (SOE) on SCS via OPC A&E interface. The major OPC client is Exaquantum, but general-purpose OPC clients (provided by other manufacturers) can also be connected with SCS.

Together with Exaquantum, HDA interface becomes available.

SOE OPC Interface works on a PC. It also works on HIS. It consists of the OPC server, which sends data to clients, and an SOE-dedicated cassette of ProSafe-RS, with which SCS data is obtained (hereafter referred to as a cassette). The specifications for the OPC server are identical to the one for the A&E server, which is essentially part of Exaopc. The A&E server is a function which creates notifications in the occurrence of an event affecting the OPC client.

Exaopc OPC interface (VP6H2411 for HIS, or NTPF100)

Exaopc OPC Interface enables OPC client to access process data, alarms, and messages on SCS.

Exaopc OPC Interface supports the following three interfaces.

OPC DA Interface

Enables OPC client to access SCS process data.

OPC HDA Interface

Enables OPC client to access historical SCS process data kept by Exaopc OPC Interface.

OPC A&E Interface

Enables OPC client to access SCS alarms and messages such as process alarms and system alarms.

Precautions

This section provides the precautions for engineering the SOE OPC Interface.

Coexistence of SOE-dedicated OPC Server with Exaopc OPC Interface Package

Minimize the chance of coexistence of the SOE-dedicated OPC Server of ProSafe-RS with the HIS "Exaopc OPC Interface Package (for HIS)." Otherwise, this can cause lower performance of the SOE-dedicated OPC Server depending on the frequency of using the Exaopc OPC Interface Package. This problem can be avoided by distributing the load on several HISs.

CPU Load Distribution

To reduce the communication load and CPU load caused by sending a large amount of data to the client, the cassette has a function of distributing the CPU load by restricting the communication traffic to the client. The cassette computes the maximum number of events that can be sent simultaneously (1-1000) from the delay time per one transmit event (user defined value, the default is 40 ms) with the following expression and alternates transmission and delay.

- Maximum number of transmitted events = Maximum delay time (fixed at 2000 ms) /Event transmission delay time (ms)
- Delay time =Event transmission delay time (ms) x Number of transmit events (n)

The default is the repetition of 50 (2000/40) event transmissions and two second delays (40 x 50).

This case requires 40 seconds for transmitting 1000 events.

The default setting can be changed according to the performance of PC.

- Longer "event transmission delay time" causes delayed event transmission and lower CPU load.

- Shorter "event transmission delay time" causes faster event transmission and higher CPU load.

SEE ALSO For more information about host interface function of SOE, refer to:

C1., “Overview of SOE OPC Interface” on page C1-1

C3. Setup for using the OPC client

Setup of the OPC server and OPC client is required to connect to the SOE OPC server.

This section describes the settings using the setup tool, Windows account settings required to use the OPC client, and settings required on the OPC client.

C3.1 Settings using the setup tool and Windows account settings

You can configure the OPC client using required information which is collected from the OPC server using the setup tool.

After that, you can configure Windows accounts and settings required for the connection on the OPC server and client.

C3.1.1 Preparations on the OPC server

On the computer where the SOE OPC Interface is installed, you must get the information that is required to set up the OPC client and save it in a removable storage device.

TIP

To run a program file or SETUP.exe in Windows Vista or later, right-click the file, and then select [Run as Administrator].

1. Connect a formatted removable storage medium (such as USB memory stick) to the computer where the SOE OPC server is running.
2. In Windows Explorer, start the following program:
   `(ProSafe-RS installation drive):\(ProSafe-RS installation folder)\ProSafe-RS\YOKOGAWA\program\RHHCopyOPC.exe`

   The RHHCopyOPC dialog box appears.

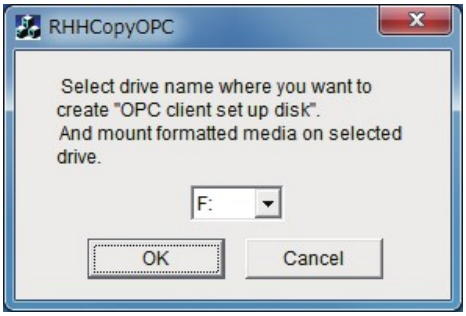


Figure C3.1.1-1 RHHCopyOPC dialog box

3. Select the connected removable storage medium and click [OK].
   The setup information that is required for the OPC client is saved on the removable storage medium.

C3.1.2 Operation procedure for the OPC client

On the computer where the OPC client runs, you must configure the setup information by using the setup tool and set up the user who will run the application on the OPC server.

TIP To run a program file or SETUP.EXE in Windows Vista or later, right-click the file and select [Run as Administrator].

1. Connect the removable storage medium that stores the setup information to the computer in which the OPC client is running.
2. Log on to the OPC client as an administrative user.
3. Insert the ProSafe-RS software medium into the drive, and run the following program contained in the medium.
   `(Media drive):\ProSafe-RS\vcredist_x86_2017\VC_redist.x86.exe`
4. Run the SETUP.EXE in the removable storage medium.
   The Command Prompt window appears, and the setting up of OPC client is performed.
   After the setup is complete, the Program Compatibility Assistant dialog box may appear.
   If it appears, click [This program installed correctly] to finish the installation.
5. Specify the user who will run the application on the SOE OPC server.
   If the SOE OPC server security model is the standard model
   a. Insert the ProSafe-RS software medium into the drive, start the command prompt window, and move to the following folder.
      `(Media drive):\ProSafe-RS\SECURITY`
   b. Run the following program.
      `ProSafe.Security.CreateProSafeProcess.exe`

      The "PSF_PROCESS" user is created on the client computer.
   c. Configure the security settings designated by the client application.

TIP If the client application is Exaquantum, add the "PSF_PROCESS" user to the QTM_OPC user group as designated by Exaquantum.

   If the SOE OPC server security model is the legacy model
   a. Create the following user on the client computer.
      Account name: EXAUSER (all in upper case)

      Password: EXAUSER (all in upper case)
   b. Configure the security settings designated by the client application.

C3.2 Security Settings

In order to connect the SOE OPC server and the OPC client products, set the security for the SOE OPC server and the OPC client according to the security model and user management method used on the SOE OPC server. If the client application coexists with the SOE OPC server, the configuration is not required.

You must configure the OPC client with administrator privileges.

IMPORTANT

If you have applied the Windows update programs to the SOE OPC server computer, be sure to apply the Windows update programs to the OPC client computers as well.

SEE ALSO For more information about the Windows update programs to apply, refer to:

B1.2, “Precautions for Setup” in Installation Guide (IM 32P01C50-01EN)

Settings for Standard Model

If the SOE OPC server security model is the standard model, the following settings are required. Be sure to restart the computer after you finish the configuration.

- Windows account settings on the SOE OPC server computer
- Firewall settings on the OPC client
- DCOM settings on the OPC client

This section describes the setting procedure for the Windows 10 operating system as an example.

Creating a Windows account on the SOE OPC server computer

Create a Windows account on the SOE OPC server computer or domain controller according to the user management method.

- For standalone management
  Add a user account with the same name as the local user who runs the client application on the OPC client computer to the SOE OPC server computer, and make it belong to the PSF_OPC group.
- For domain management or combination management
  Add a user account that runs the client application on the OPC client computer to the domain controller, and make it belong to the PSF_OPC group. If the user account running the client application is unable to support domain management, add a user account with the same name as the local user who runs the client application on the OPC client computer to the SOE OPC server computer, and make it belong to the PSF_OPC_LCL group.
- For linked domain management
  Add a user account that runs the client application on the OPC client computer to the domain controller, and make it belong to the PSF_OPC group. If the user account running the client application is unable to support domain management, add a user account with the same name as the local user who runs the client application on the OPC client computer to the SOE OPC server computer, and make it belong to the PSF_OPC group.

TIP If you add a user account with the same name as the local user to the SOE OPC server computer, make sure that the password is the same.

SEE ALSO For more information about how to create a user account in domain management, combination management, or linked domain management and make it belong to a group, refer to:

B2.4, “Creating Domain Users” in Installation Guide (IM 32P01C50-01EN)

Firewall settings on the OPC client

Configure firewall settings for the [File and Printer Sharing] service and the client application.

1. Open the Control Panel.
2. Select [System and Security] > [Windows Defender Firewall].
   The Windows Defender Firewall window appears.

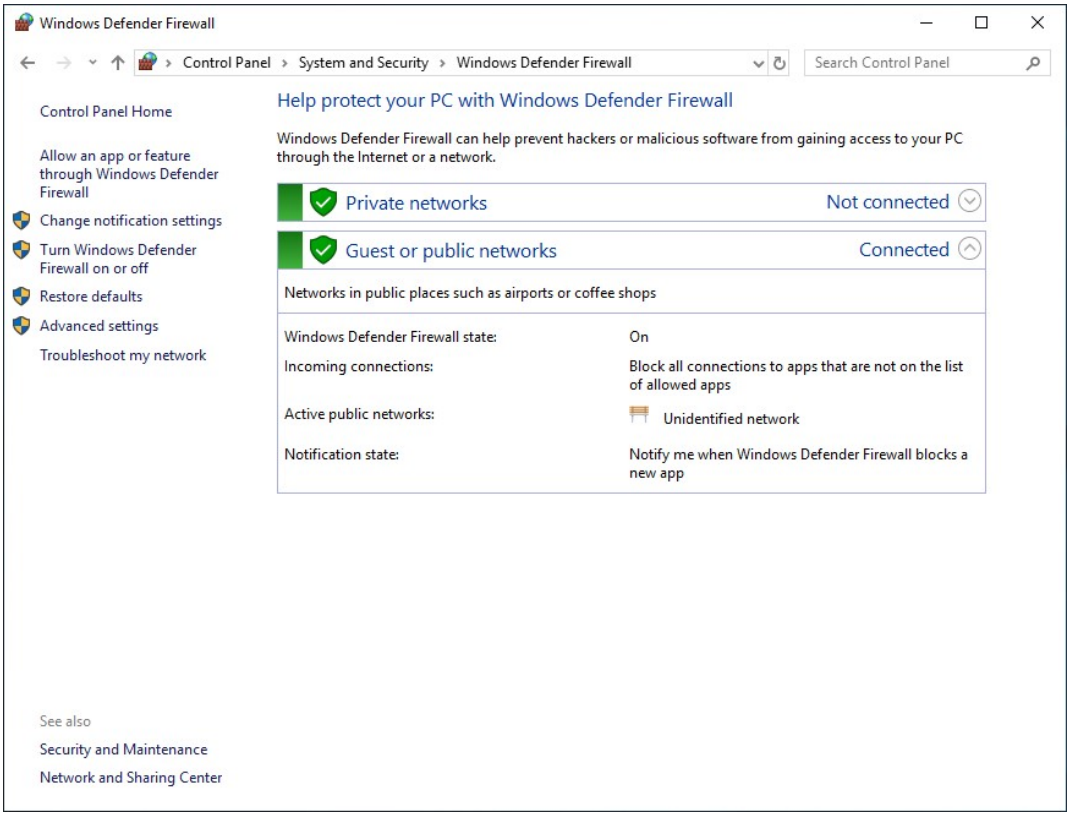


Figure C3.2-1 Windows Defender Firewall window

3. Click [Allow an app or feature through Windows Defender Firewall].
   The Allowed apps window appears.

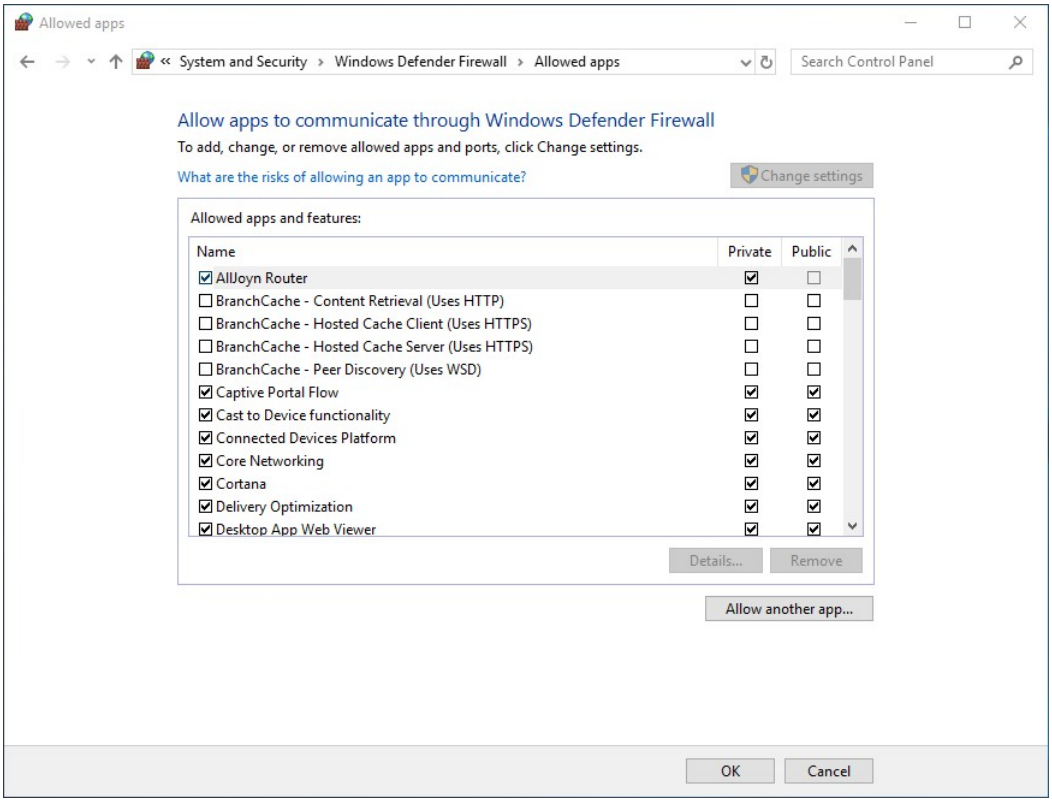


Figure C3.2-2 Allowed apps window

4. Click [Change settings].
5. In the Name column, select the check box for [File and Printer Sharing].
   Make sure all profiles (Private and Public) are selected.

TIP

For domain management, combination management, or linked domain management, [Domain] is displayed in addition to [Private] and [Public].

6. Click [Allow another app].
   The Add an app dialog box appears.
7. Select the client application from the Programs list and click [Add].
   Make sure that the selected client application is added to the Allowed apps window and that its check boxes in the Name and Public columns are selected.

DCOM settings on the OPC client

For DCOM, add the PSF_PROCESS user and configure "Access Permissions" and "Launch and Activation Permissions." After that, change the default authentication level.

1. Edit the Access Permissions settings for the PSF_PROCESS user.
   a. Open the Control Panel.
   b. Select [System and Security] > [Administrative Tools] > [Component Services].
      The Component Services window appears.

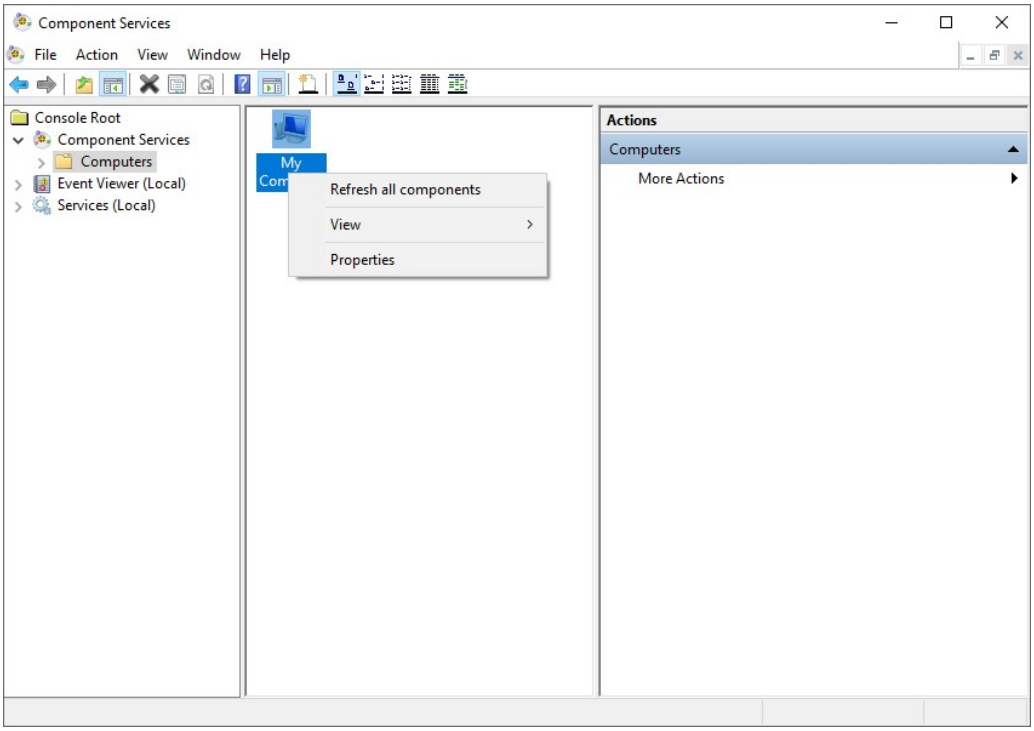


Figure C3.2-3 Component Services window

c. Right-click [Component Services] > [Computers] > [My Computer] and select [Properties].
The My Computer Properties dialog box appears.

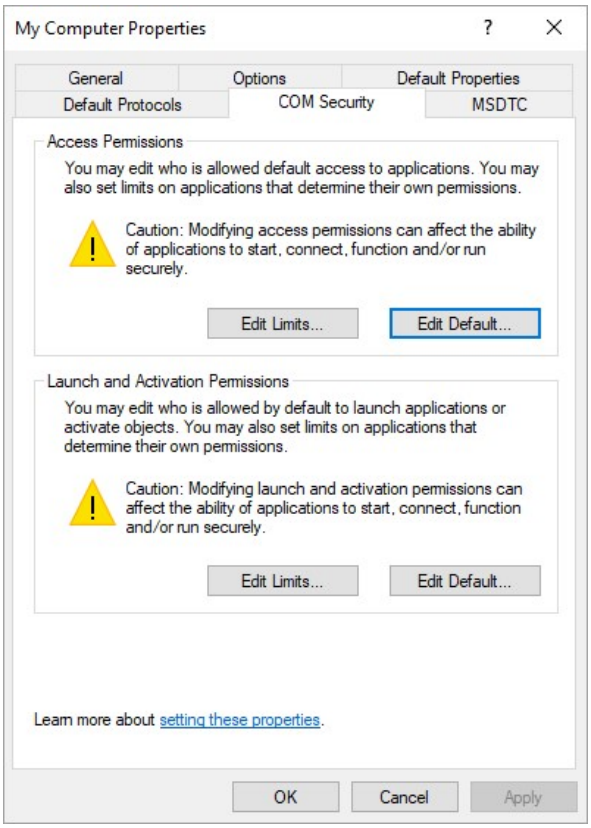


Figure C3.2-4 COM Security tab of the My Computer Properties dialog box

d. Click the COM Security tab and click [Edit Default] for Access Permissions.
The Access Permission dialog box appears.

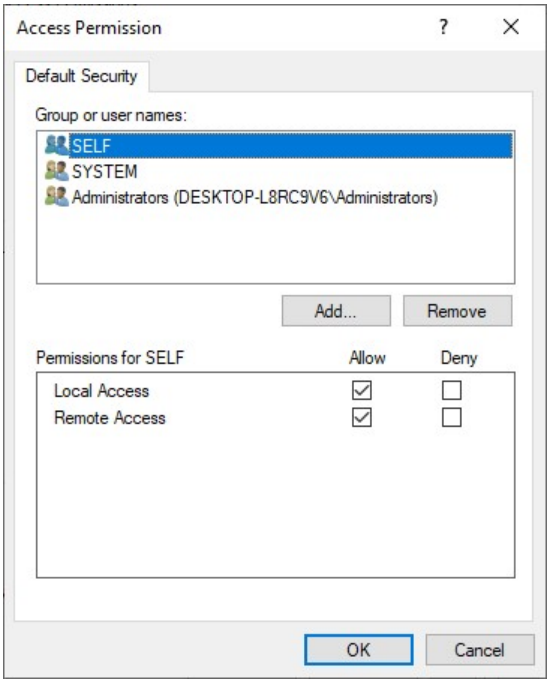


Figure C3.2-5 Default Security tab of the Access Permission dialog box

e. Click [Add].
The Select Users or Groups dialog box appears.

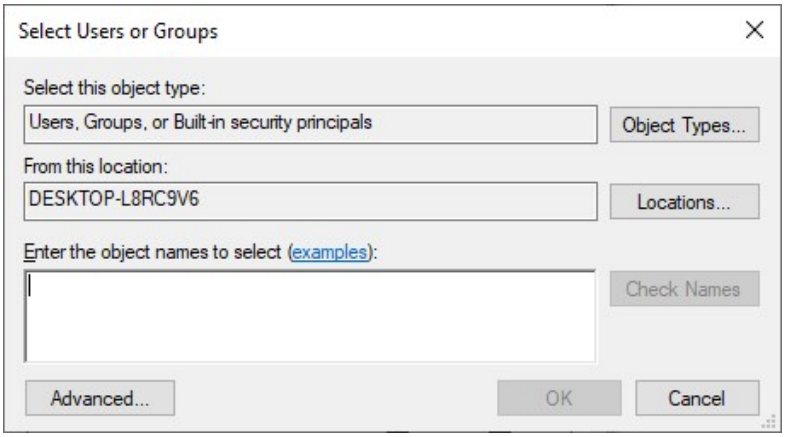


Figure C3.2-6 Select Users or Groups dialog box

f. Enter the `PSF_PROCESS` user created in the Operation procedure for the OPC client and click [OK].
The [PSF_PROCESS] user is added to the Access Permission dialog box.

g. Select [PSF_PROCESS], select the "Allow" check boxes for "Local Access" and "Remote Access," and click [OK].

2. Edit limits for Access Permissions

a. In the My Computer Properties dialog box, click the COM Security tab and click [Edit Limits] for Access Permissions.
The Access Permission dialog box appears.

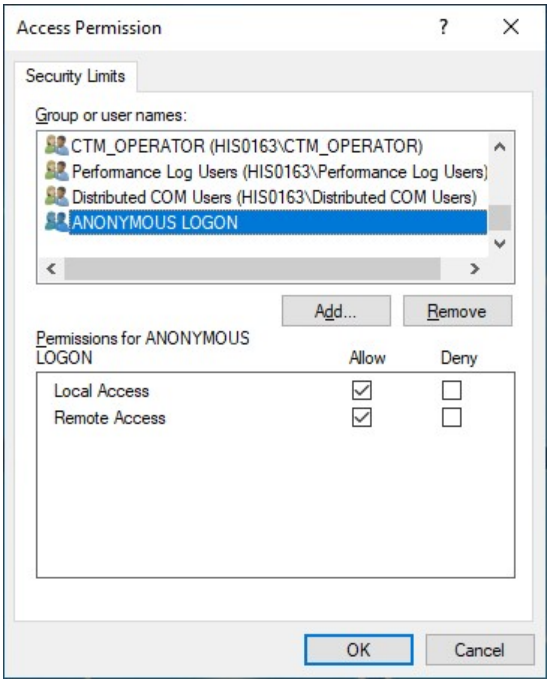


Figure C3.2-7 Security Limits tab of the Access Permission dialog box

b. Select [ANONYMOUS LOGON] in the Group or user names list, select the Allow check boxes for "Local Access" and "Remote Access," and click [OK].

3. Edit the default values of Launch and Activation Permissions

a. In the My Computer Properties dialog box, click the COM Security tab and click [Edit Default] for Launch and Activation Permissions.
The Launch and Activation Permission dialog box appears.

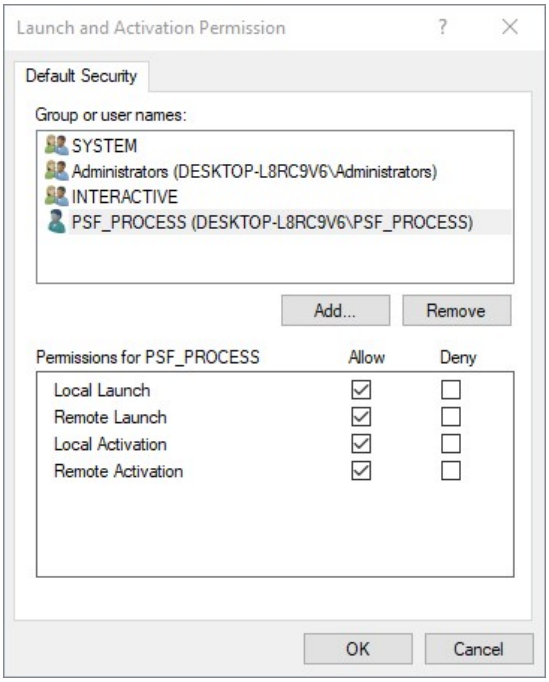


Figure C3.2-8 Default Security tab of the Launch and Activation Permission dialog box

b. Click [Add].
The Select Users or Groups dialog box appears.

c. Enter `PSF_PROCESS` for the user to select and click [OK].

The [PSF_PROCESS] user is added to the Launch and Activation Permission dialog box.

d. Select [PSF_PROCESS], select the Allow check boxes for "Local Launch," "Remote Launch," "Local Activation," and "Remote Activation," and click [OK].

4. Edit limits for Launch and Activation Permissions.

a. In the My Computer Properties dialog box, click the COM Security tab and click [Edit Limits] for Launch and Activation Permissions.
The Launch and Activation Permission dialog box appears.

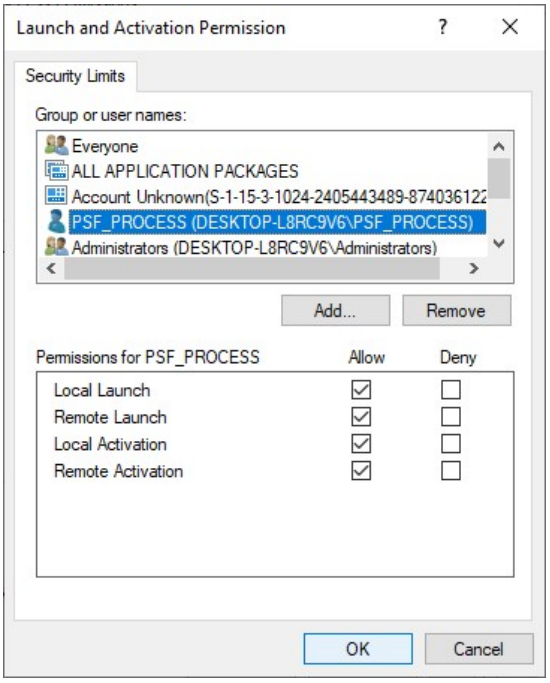


Figure C3.2-9 Security Limits tab of the Launch and Activation Permission dialog box

b. Click [Add].
The Select Users or Groups dialog box appears.

c. Enter `PSF_PROCESS` for the user to select and click [OK].
The [PSF_PROCESS] user is added to the Launch and Activation Permission dialog box.

d. Select [PSF_PROCESS], select the Allow check boxes for "Local Launch," "Remote Launch," "Local Activation," and "Remote Activation," and click [OK].

5. Edit the default properties.

a. In the My Computer Properties dialog box, click the Default Properties tab and select [Connect] for the Default Authentication Level, and click [OK].

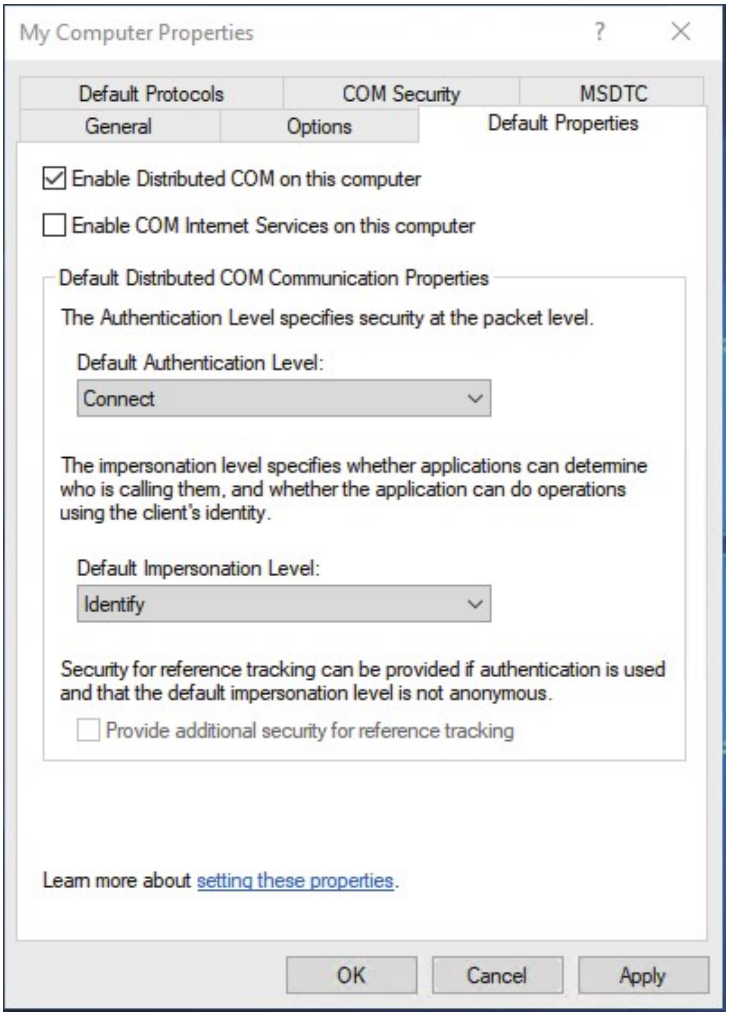


Figure C3.2-10 Default Properties tab of the My Computer Properties dialog box

6. Change the default authentication level of the SOE OPC server.
   a. In the hierarchy tree, expand [Component Services] > [Computers] > [My Computer] > [DCOM Config].

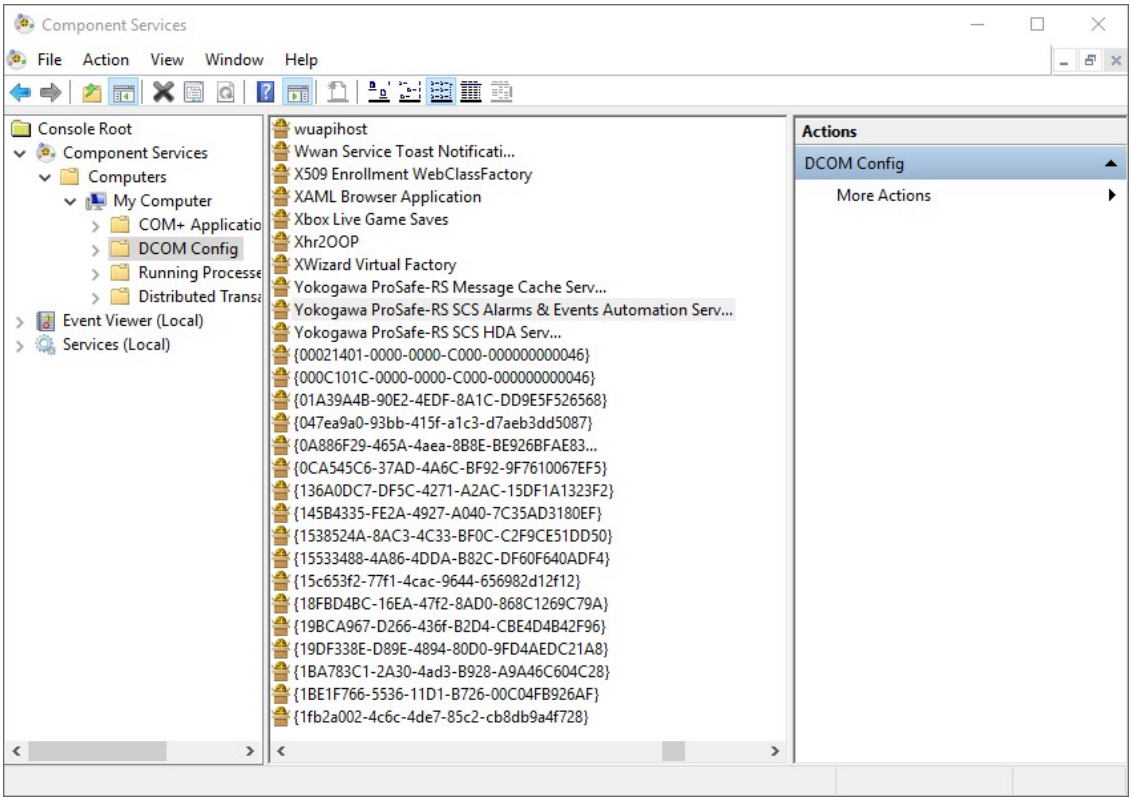


Figure C3.2-11 DCOM Config

b. Select Yokogawa ProSafe-RS SCS Alarms & Events Automation Server and select [Properties] from the right-click menu.
The Properties dialog box appears.

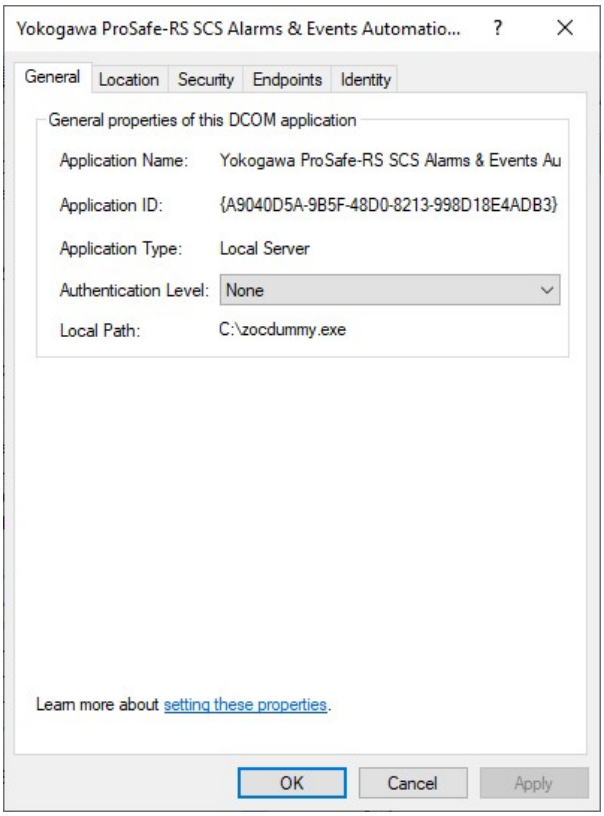


Figure C3.2-12 Yokogawa ProSafe-RS SCS Alarms & Events Automation Server Properties dialog box

c. In the Yokogawa ProSafe-RS SCS Alarms & Events Automation Server Properties dialog box, click the General tab and select [None] for the Authentication Level, and click [OK].

d. From the hierarchy tree, open the DCOM Config window, select Yokogawa ProSafe-RS SCS HDA Server, and select [Properties] from the right-click menu.
The Properties dialog box appears.

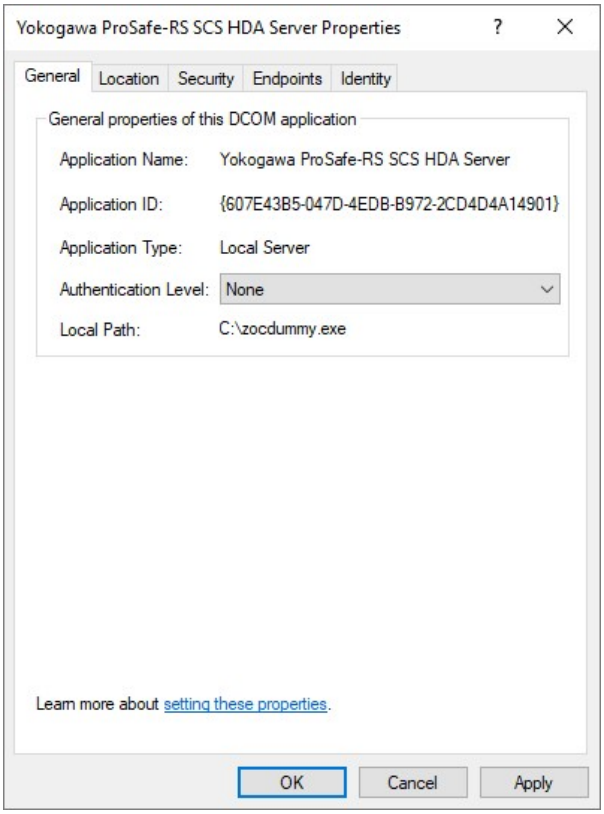


Figure C3.2-13 Yokogawa ProSafe-RS SCS HDA Server Properties dialog box

e. In the Yokogawa ProSafe-RS SCS HDA Server Properties dialog box, click the General tab and select [None] for the Authentication Level, and click [OK].

7. Restart the computer.

Settings for the legacy model

If the SOE OPC server security model is the legacy model, the following settings are required. Be sure to restart the computer after you finish the configuration.

- Firewall settings
- DCOM settings
- Local security settings

Firewall setting procedure

Disable the Windows Firewall.

1. Open the Control Panel.
2. Select [System and Security] > [Windows Defender Firewall].
Help protect your PC with Windows Defender Firewall appears.

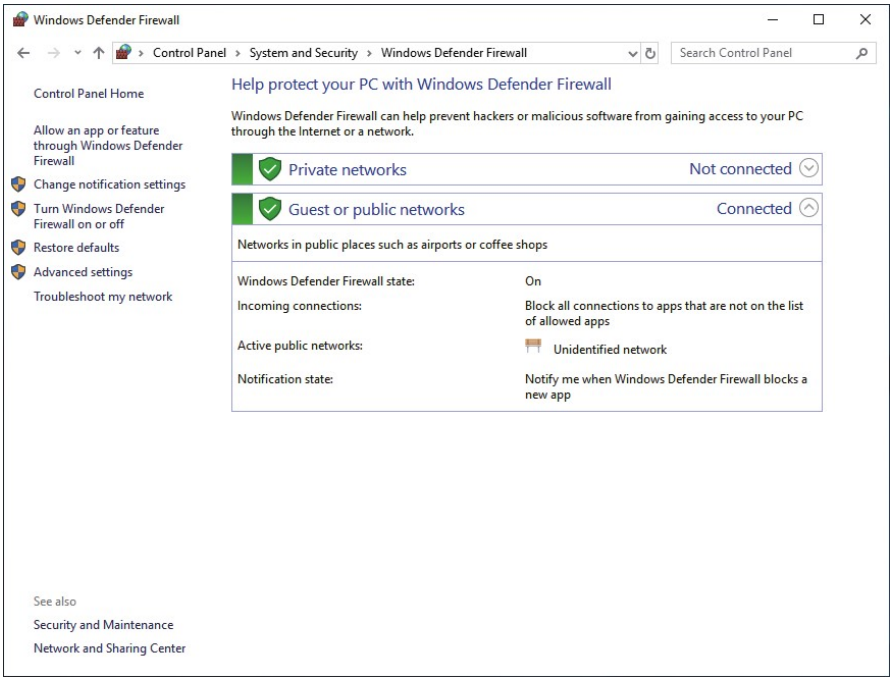


Figure C3.2-14 Help protect your PC with Windows Defender Firewall

3. Click [Turn Windows Defender Firewall on or off].
   The Customize settings for each type of network dialog box appears.

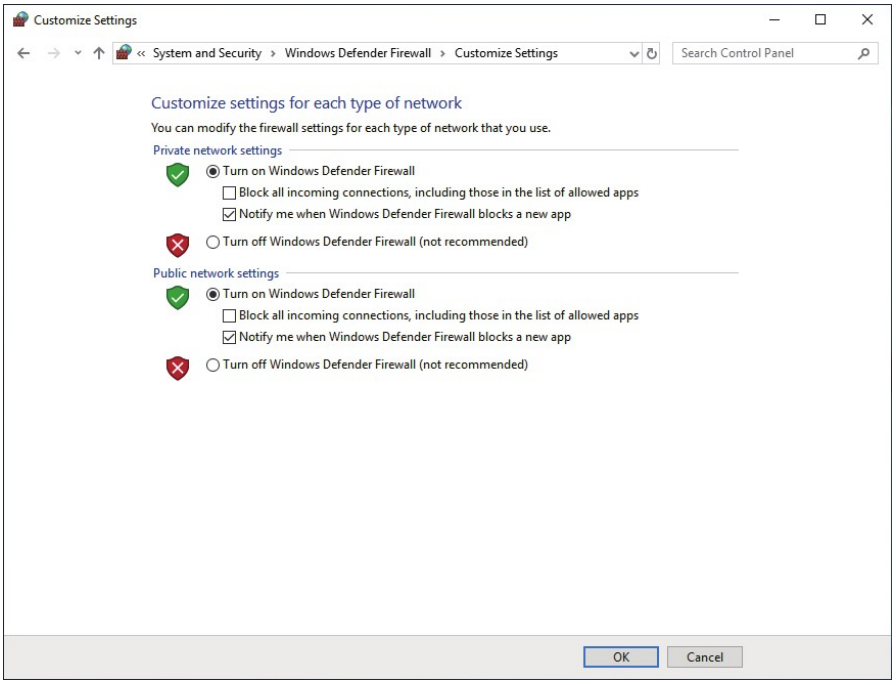


Figure C3.2-15 Turning Windows Defender Firewall on or off

4. For the location settings of each network, select [Turn off Windows Defender Firewall (not recommended)], and click [OK].

DCOM setting procedure

For DCOM, add the Everyone user and configure "Access Permissions" and "Launch and Activation Permissions" for the Everyone user and default user. After that, change the default authentication level.

1. Edit the Access Permissions settings for the Everyone user.

   a. Open the Control Panel.

   b. Select [System and Security] > [Administrative Tools] > [Component Services].
   The Component Services window appears.

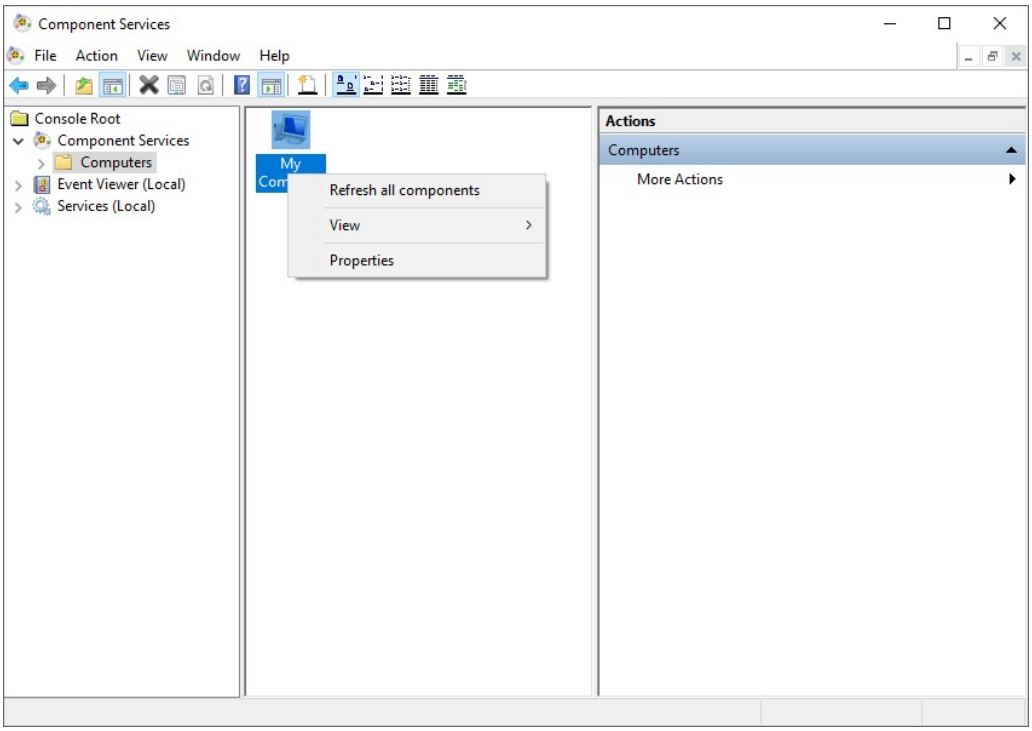


Figure C3.2-16 Component Services window

   c. Right-click [Component Services] > [Computers] > [My Computer] and select [Properties].
   The My Computer Properties dialog box appears.

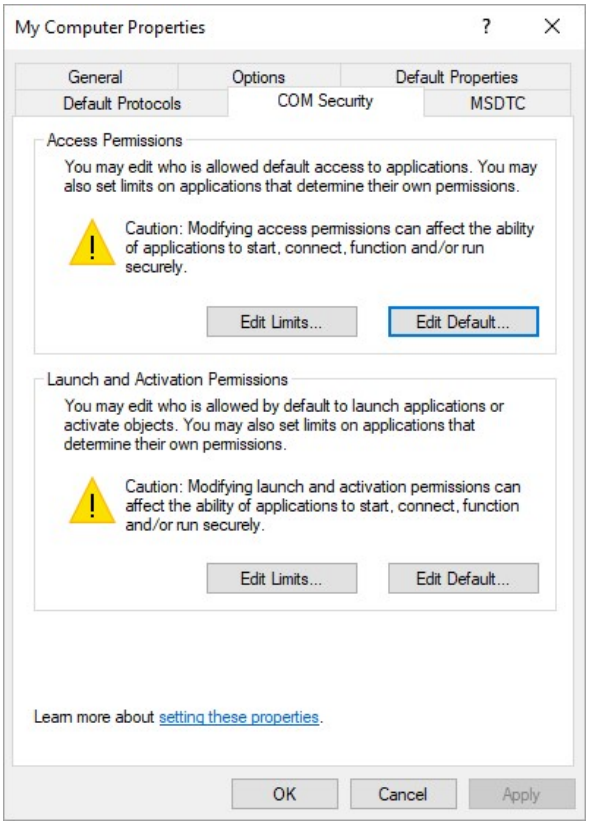


Figure C3.2-17 COM Security tab of the My Computer Properties dialog box

d. Click the COM Security tab and click [Edit Default] for Access Permissions.
The Access Permission dialog box appears.

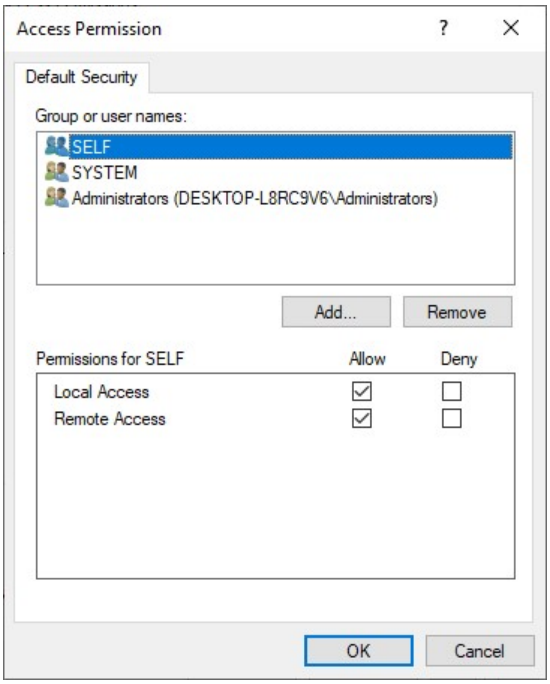


Figure C3.2-18 Default Security tab of the Access Permission dialog box

e. Click [Add].
The Select Users or Groups dialog box appears.

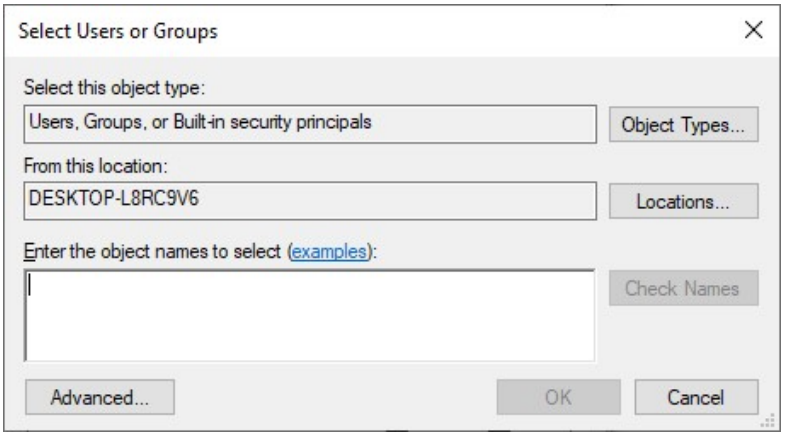


Figure C3.2-19 Select Users or Groups dialog box

f. Enter `Everyone` for the object name to select and click [OK].
The [Everyone] user is added to the Access Permission dialog box.

g. Select [Everyone], select the "Allow" check boxes for "Local Access" and "Remote Access," and click [OK].

2. Edit the default values of Launch and Activation Permissions.

a. In the My Computer Properties dialog box, click the COM Security tab and click [Edit Default] for Launch and Activation Permissions.
The Launch and Activation Permission dialog box appears.

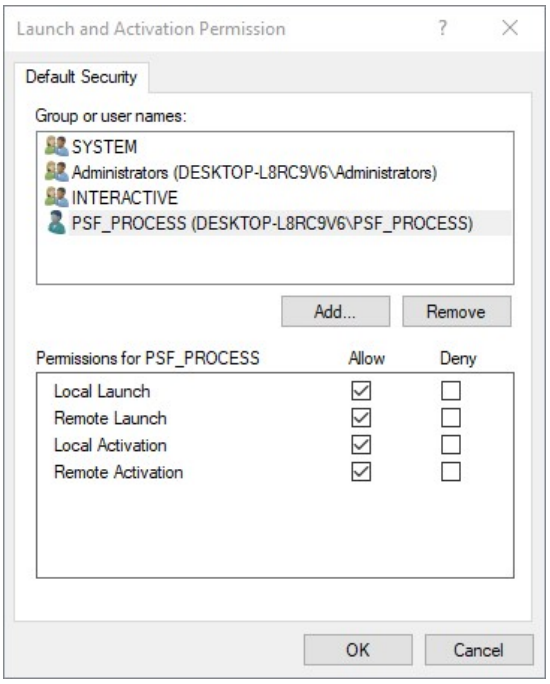


Figure C3.2-20 Default Security tab of the Launch and Activation Permission dialog box

b. Click [Add].
The Select Users or Groups dialog box appears.

c. Enter `Everyone` for the object name to select and click [OK].
The [Everyone] user is added to the Launch and Activation Permission dialog box.

d. Select [Everyone], select the "Allow" check boxes for "Local Launch," "Remote Launch," "Local Activation," and "Remote Activation," and click [OK].

3. Edit limits for Access Permissions.

   a. In the My Computer Properties dialog box, click the COM Security tab and click [Edit Limits] for Access Permissions.
   The Access Permission dialog box appears.

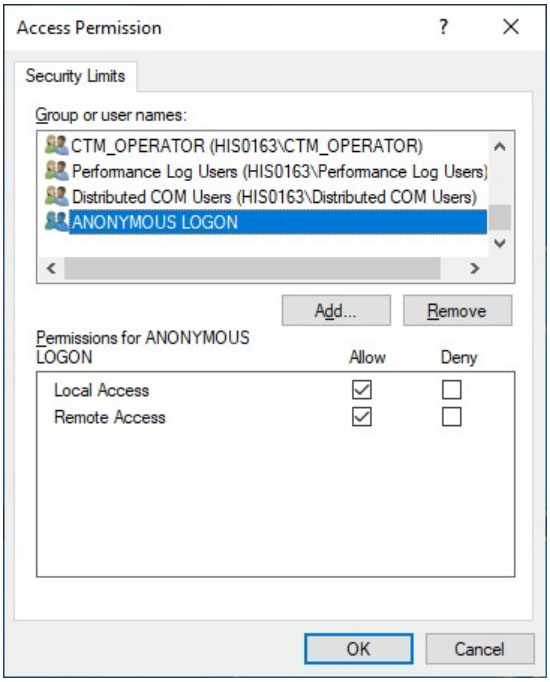


Figure C3.2-21 Security Limits tab of the Access Permission dialog box

   b. Select [ANONYMOUS LOGON] in the Group or user names list, select the "Allow" check boxes for "Local Access" and "Remote Access," and click [OK].

4. Edit limits for Launch and Activation Permissions.

   a. In the My Computer Properties dialog box, click the COM Security tab and click [Edit Limits] for Launch and Activation Permissions.
   The Launch and Activation Permission dialog box appears.

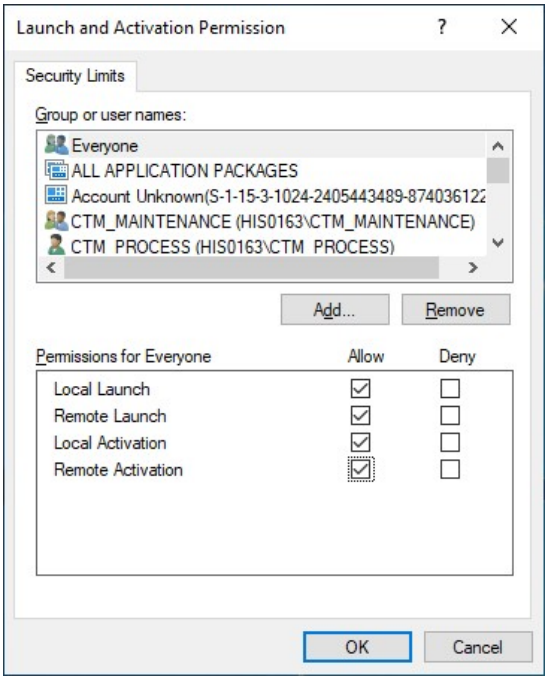


Figure C3.2-22 Security Limits tab of the Launch and Activation Permission dialog box

b. Select [Everyone] in the Group or user name list, select the "Allow" check boxes for "Local Launch," "Remote Launch," "Local Activation," and "Remote Activation," and click [OK].

5. Edit the default properties.

a. In the My Computer Properties dialog box, click the Default Properties tab and select [None] for the Authentication Level, and click [OK].

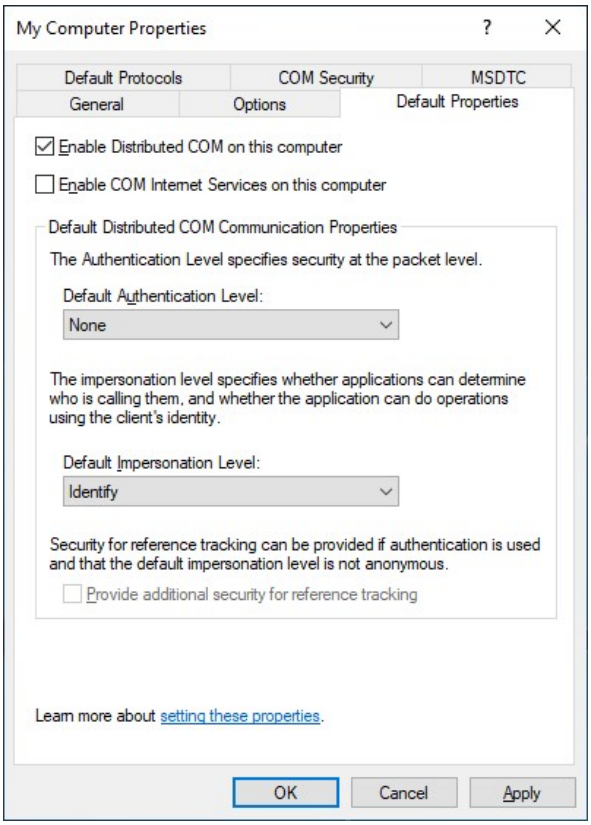


Figure C3.2-23 Default Properties tab of the My Computer Properties dialog box

Local security policy setting procedure

Set the local security policy.

1. Select [Control Panel] > [System and Security] > [Administrative Tools] > [Local Security Policy].
   The Local Security Policy window appears.

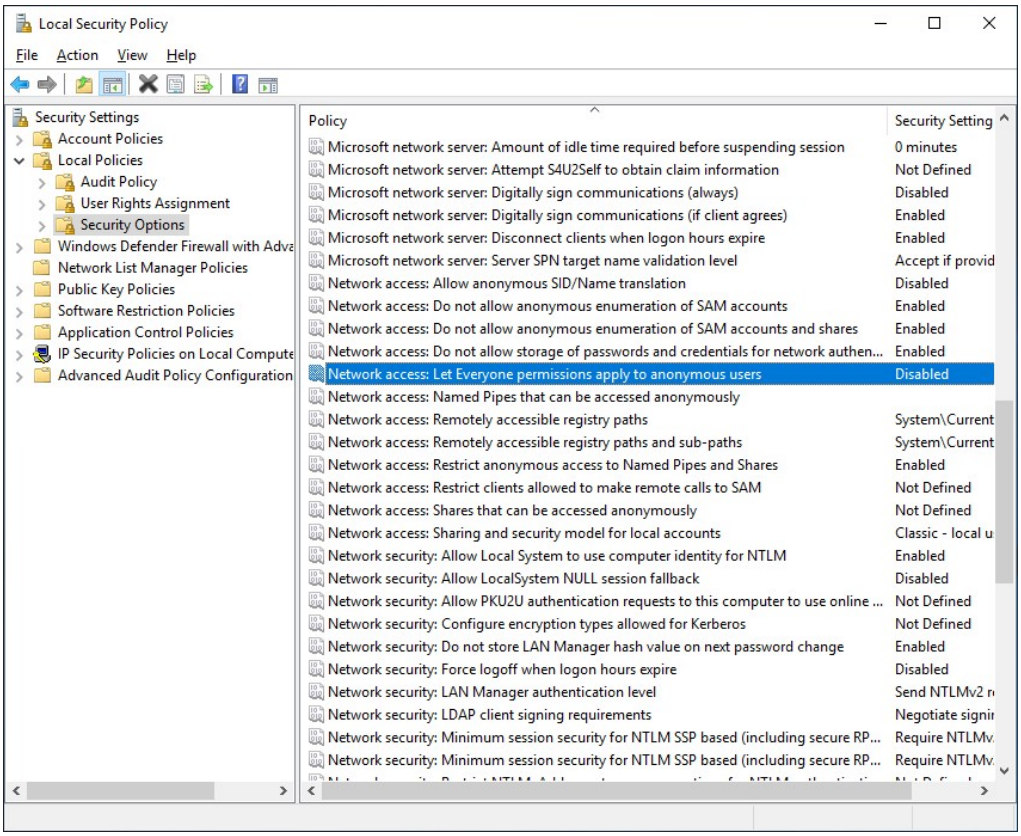


Figure C3.2-24 Local Security Policy window

2. Open [Security Settings] > [Local Policies] > [Security Options].
3. In the Policy column, double-click [Network access: Let Everyone permissions apply to anonymous users].
   The Network access dialog box appears.

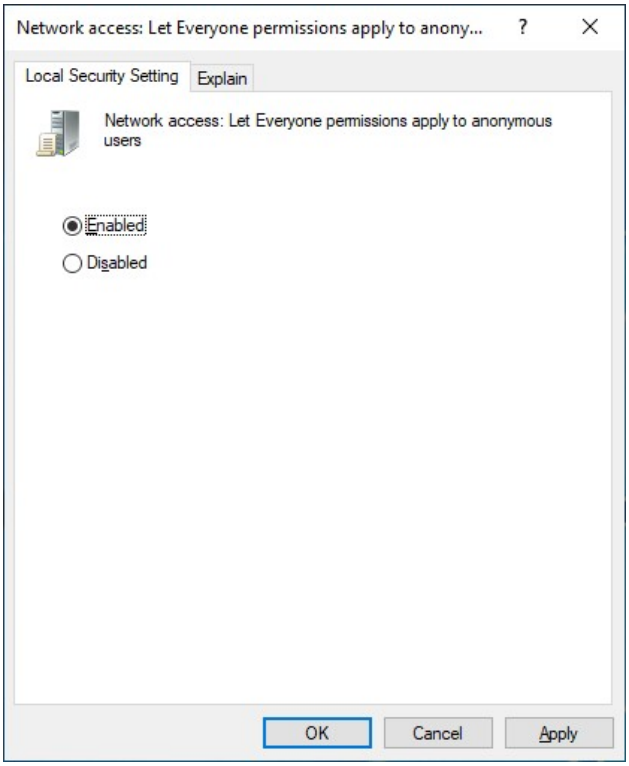


Figure C3.2-25 Network access dialog box

4. Select [Enabled] and click [OK].
   In the Security Options folder, confirm that "Enabled" is selected in the "Security Setting" field for [Network access: Let Everyone permissions apply to anonymous users].
5. Restart the computer.

D. Subsystem communication

The subsystem communication function is one of the Modbus communication functions that are provided by ProSafe-RS. This function enables a safety control station (SCS) to act as the Modbus master and communicate with subsystems.

D1. Common items regarding subsystem communication functions

The subsystem communication function enables communication, such as reading and writing subsystem data between SCSs and PLCs (Programmable Logic Controllers), or other subsystems connected to the SCS's communication module.

This section describes common subsystem communication functions that are not dependent on subsystem types.

D1.1 Overview of subsystem communication

This section describes the structure of subsystem communication functions within the SCS and gives an overview of communication between the subsystem and the SCS.

Type of subsystem communication function

The following subsystem communication function is available in an SCS: The communication module in the SCS becomes the communication master.

- MODBUS communication
- ProSafe-SLS communication

Subsystem communication modules

SCS and PLC subsystems are connected through subsystem communication modules installed in the SCS. Subsystem communication modules are classified into the following three types:

- ALR111 RS-232C serial communication module
- ALR121 RS-422/RS-485 serial communication module
- ALE111 Ethernet communication module

Structure of subsystem communication functions

The following section provides an overview of subsystem communication.

- Functional structure and data flow
- Relationship of subsystems and the application logic

Functional structure and data flow

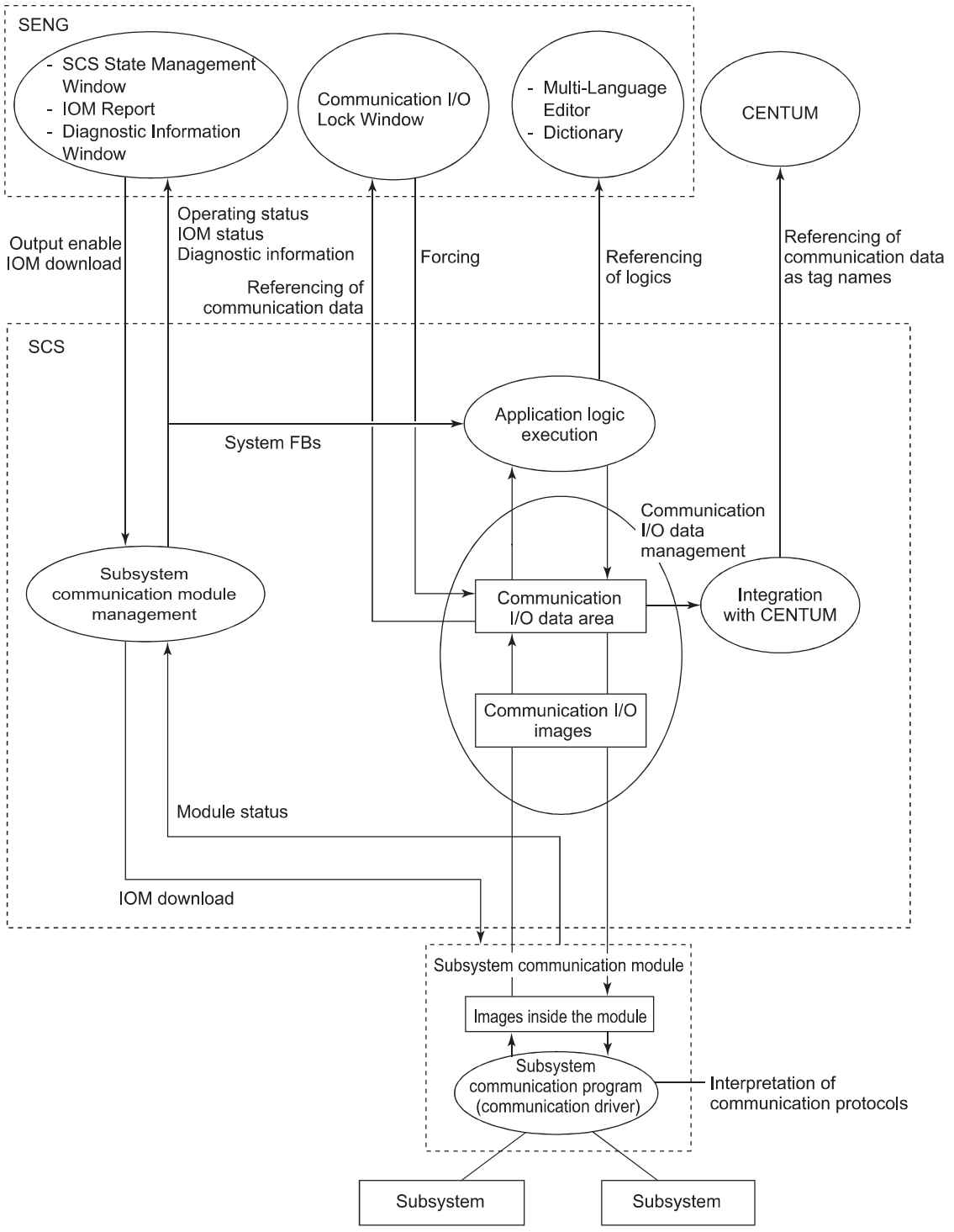


Figure D1.1-1 Functional structure and data flow

Relationship of subsystems and the application logic

- Input data from subsystems are input to the application logic via the communication I/O data management function.
- Output values calculated by the application logic are output to subsystems via the communication I/O data management function.

- The subsystem communication program interprets communication protocols (such as the Modbus protocol).
- The communication I/O data management function is a general-purpose data management function not dependent on communication protocols. The communication I/O data management function manages the communication I/O data area consisting of 1000 words in which subsystem register images are mapped.
- The subsystem communication input FBs and subsystem communication output FBs are used to access the communication I/O data management function from the application logic.

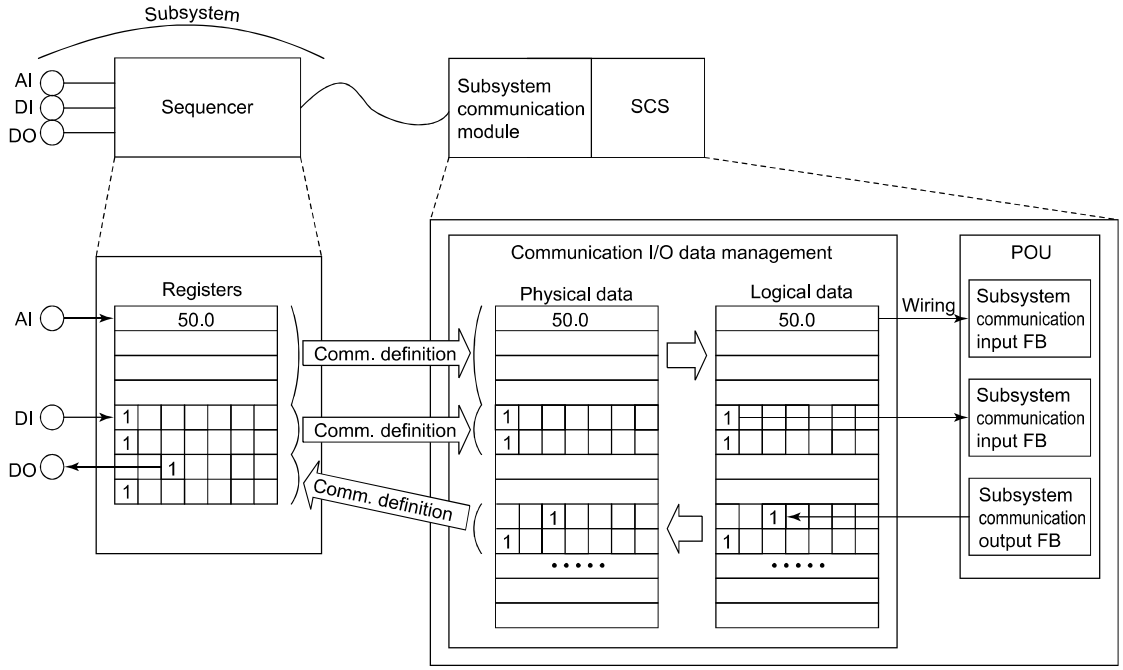


Figure D1.1-2 Relationship of communication I/Os and registers

Communication with subsystems

The subsystem communication module communicates with each subsystem in accordance with the transmission specifications and communication definitions set with subsystem communication builders to refresh the images inside the module.

The subsystem communication module interprets subsystem communication protocols and performs communication based on the protocols. Thus, the CPU only exchanges data with the subsystem communication module and does not perform any processing specific to each subsystem communication type.

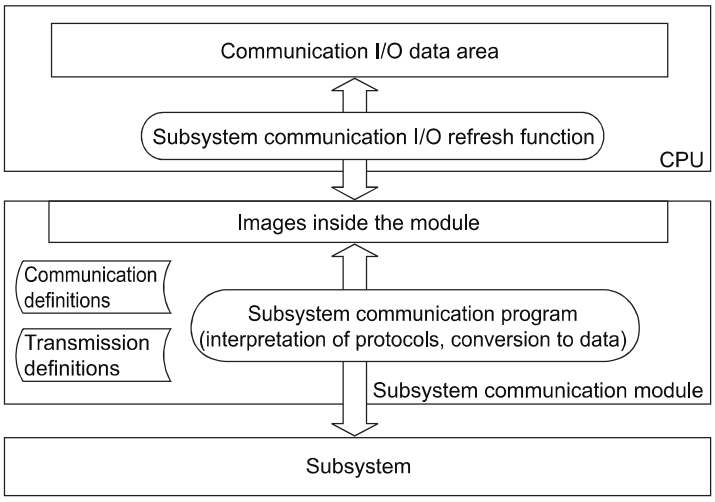


Figure D1.1-3 Communication between SCS and subsystem

Data flow and refresh time

The data refresh time varies depending on the subsystem type, amount of acquired data and transmission specifications. The following describes the flow of data not dependent on subsystem types.

Data refresh time (input through output)

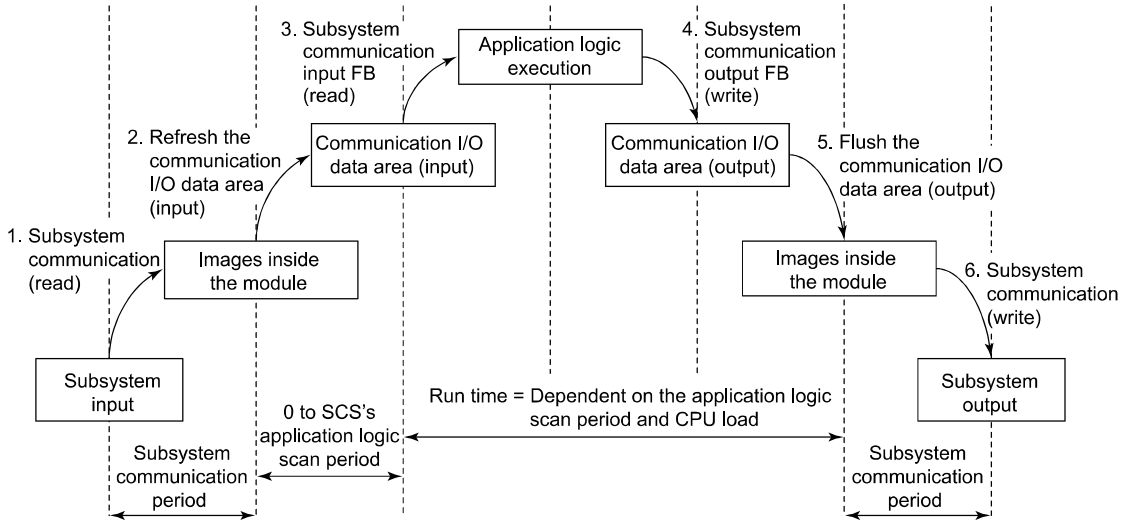


Figure D1.1-4 Data refresh time (input through output)

Data flow and timings

1. Subsystem communication (read)

   The data acquisition period varies depending on the subsystem type and transmission specifications.

2. Refresh the communication I/O data area (input)

   The data is read from the subsystem communication module to the communication I/O data area at the beginning of the SCS scan period.

3. Subsystem communication input FB (read)

   The data is read from the communication I/O data area (input) when the subsystem communication input FB is executed.

4. Subsystem communication output FB (write)

   The data is written to the communication I/O data area (output) when output from the subsystem communication output FB.

5. Flush the communication I/O data area (output)

   At the end of the SCS scan period, the communication I/O data area is flushed and the data is written to the subsystem communication module.

6. Subsystem communication (write)

   The data acquisition period of each subsystem from the subsystem communication module varies depending on the subsystem type and transmission specifications.

SEE ALSO For more information about transmission specifications, refer to:

"■ Transmission specification" on page D2-2

■ Period of subsystem communication and communication time

The following section describes the period of subsystem communication and communication time by using a serial communication module and Ethernet communication module.

● Period of serial communication

Subsystem communication is performed asynchronously with the scan period of the application logic execution function. Data is written only when written by the CPU.

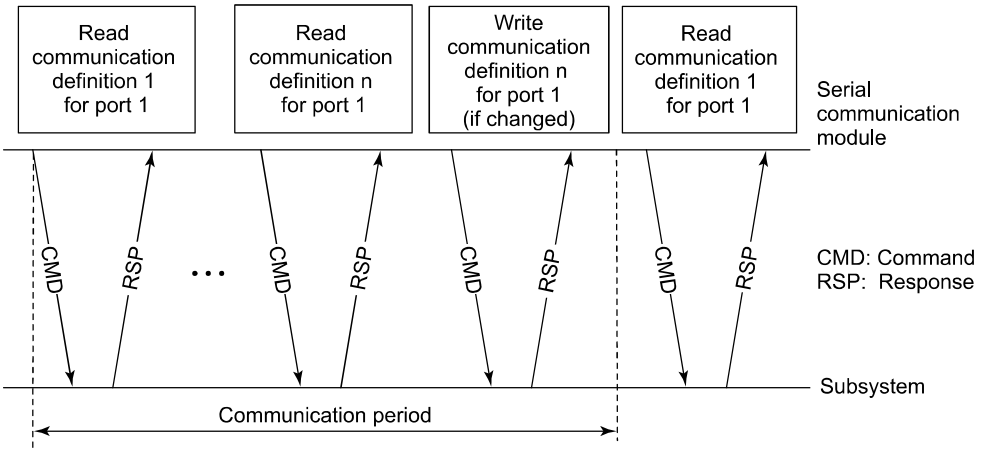


Figure D1.1-5 Subsystem communication (example numbers of communication definitions for port 1 is "n")

In serial communication, each port of the serial communication module communicates at a different period. The communication period of each port represents the sum of times required to communicate all communication definitions set for the port.

Example:

Communication definition 1: Port 1

Communication definition 2: Port 1

Communication definition 3: Port 2

Communication definition 4: Port 2

Communication period of port 1 = (Communication time for communication definition 1) + (Communication time for communication definition 2)

Communication period of port 2 = (Communication time for communication definition 3) + (Communication time for communication definition 4)

Ethernet communication period

Subsystem communication is performed asynchronously with the scan period of the SCS application logic. Data is written only when written by the CPU.

Communication between the Ethernet communication module and PLC is processed in parallel for each IP address. In other words, the request creation process is completed in the Ethernet communication module, and is performed for the PLC of a different IP address after frame transmission.

A single communication allocation definition is processed one at a time. For example, if two PLCs exist and communication allocation is set to “3” and “1” respectively, transmission is performed in the following order. However, it is assumed that communication in each PLC is performed without delay.

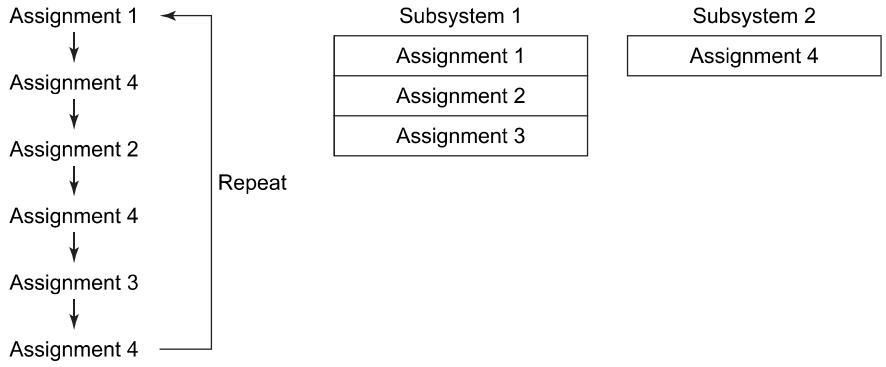


Figure D1.1-6 Communication allocation definition process

Assurance of simultaneity of communication data

In the SCS (between the subsystem communication module and the communication I/O data management function), simultaneity of data is assured in units of 32 bits.

Between the subsystem communication module and each subsystem, the unit of data in which simultaneity is assured varies, depending on the subsystem communication program and the subsystem.

SEE ALSO For more information about assurance of simultaneity of communication data for Modbus communication programs, refer to:

“■ Simultaneity of communication data” on page D2-2

Handling of subsystem data

The following table shows how subsystem data types are handled in the SCS.

Table D1.1-1 Types of subsystem data handled

Subsystem data type	Data type in SCS	Remark
Bit (DI/DO)	BOOL (bit)	With/without bit reversing
32-bit floating	REAL (32-bit floating)	With/without word reversing
16-bit signed integer	DINT (32-bit signed integer)	
16-bit unsigned integer	DINT (32-bit signed integer)	
32-bit signed integer	DINT (32-bit signed integer)	With/without word reversing
SLS event type	N/A (*1)	Without bit reversing, without word reversing

*1: SLS event type represents the ProSafe-SLS data type that is used exclusively for acquiring events. This data type is used internally by the SCS. It cannot be used in application logics.

In order to handle the subsystem communication data on SCS, the Communication I/O Builder is used for wiring the subsystem data and the SCS data according to the data types of subsystem. All the wired data are referred to as "communication data." A communication datum consists of data value and data status.

Output enable operation

- Following an initial cold start of the SCS, input communications from subsystems will start as soon as the subsystem communication module is started. Output communications to subsystems will start following the output enable operation for subsystem communication. Note, however, that output will start immediately after the subsystem communication module is started following a recovery from an error, no output enable operation is required in such a case. Readback of output will start as soon as the subsystem communication module is started.
- Output from the subsystem communication module is disabled only after an initial cold start of the SCS.
- Regardless of the status of the subsystem communication module, output enable operation for the safety output modules can be performed at any time.
- Output enable operation can be performed even when a subsystem communication error is present. In this case, output will start only for those outputs that can be communicated.

IOM download

When an IOM download is performed, the subsystem communication program is downloaded to the subsystem communication module and the communication module is restarted. No output enable operation is required.

Status monitoring from SENG or HIS

- The status of the subsystem communication module can be monitored in the status display window of the SENG or HIS.
- From a SENG, communication program names and error information can be referenced using SCS Maintenance Support Tool's IOM Report.
- The forcing status of subsystem communication data and errors in the subsystem communication module are notified as diagnostic information messages.

D1.2 Dual-redundant communication

When a serial communication module (ALR111/ALR121) or Ethernet communication module (ALE111) is used, you can have a dual-redundant configuration in the subsystem communication.

This section explains about dual-redundant communication by using ALR111, ALR121 and ALE111.

D1.2.1 Dual-redundant communication in ALR111 and ALR 121

If the ALR111 or ALR121 is used, dual-redundant communication can be implemented by connecting two serial communication modules side by side. Note, however, that dual-redundant communication cannot be implemented without readback.

ALR121 redundancy is not supported by the ProSafe-SLS communication function.

Data flow in a dual-redundant configuration of subsystem communication modules

The following figure illustrates the flow of data when the subsystem communication module has a dual-redundant configuration and readback is performed.

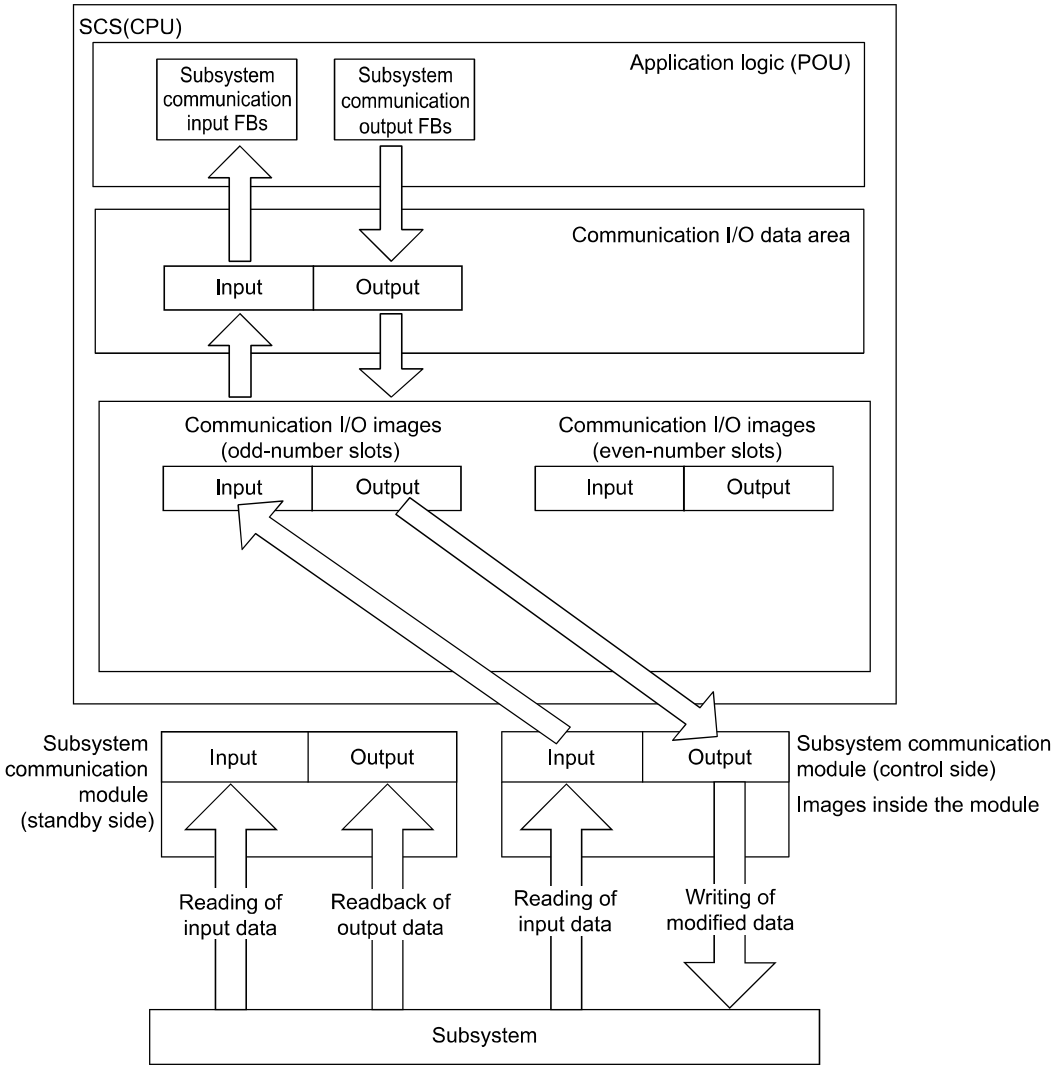


Figure D1.2.1-1 Data flow in dual-redundant configuration of subsystem communication modules

Flow of input data

The two dual-redundant subsystem communication modules both communicate with subsystems periodically and refresh the images inside the subsystem communication modules.

The SCS references the image (area for input) inside the subsystem communication module on the control side. The image (area for input) inside the module is copied to the communication I/O image in odd-number slot and set in the communication I/O data area.

Flow of output data

Data is written to subsystems only from the subsystem communication module on the control side. Details of the flow of output data are as follows:

- The CPU of the SCS refreshes only the data for the subsystem communication module on the control side.
- Both the subsystem communication modules on the control and standby sides read the data output from each subsystem (readback).
- The subsystem communication module on the control side compares the value read back from the subsystem and the write data from the CPU, and writes the output data to the subsystem only when the two values are different. If the two values are the same, the subsystem communication module on the control side reflects the value read back from the subsystem in the image (area for output) inside the module.
- The subsystem communication module on the standby side does not write data, so data is not refreshed by the CPU. The image (area for output) inside the subsystem communication module on the standby side is refreshed via readback of the output subsystem data that have been changed via writing from the subsystem communication module on the control side. This operation equalizes the output data of both the subsystem communication modules on the control and standby sides.

TIP

When you have online-change downloaded the configuration of the subsystem communication module from a single to dual-redundant configuration, the modules start the dual-redundant operation immediately after the download is complete. This does not affect the operating mode of the SCS because the output of the SCS stays enabled.

SEE ALSO

For more information about readback communication, refer to:

D2.5, “Readback communication” on page D2-20

D1.2.2 Dual-redundant communication in ALE111

In Ethernet communication module (ALE111), you can have a dual-redundant configuration in the subsystem communication by using two adjacent ALE111.

The following are two types of dual-redundant configuration in ALE111:

- Dual-redundant Ethernet communication module only
- Dual-redundant network

Dual-redundant Ethernet communication module only

The Ethernet communication module is set as dual-redundant configuration, and connected to the same network domain. Communication destination subsystem is placed on a different network domain through the same network domain or default gateway.

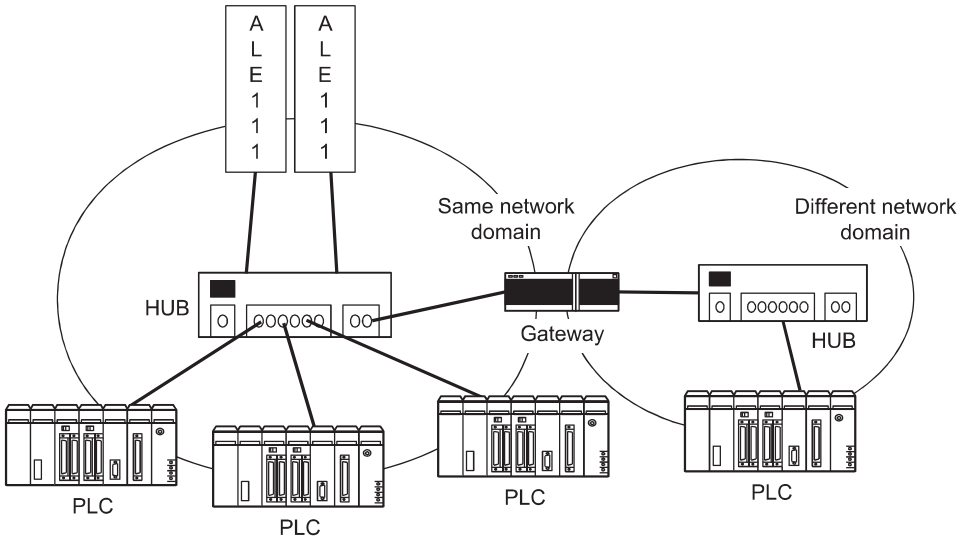


Figure D1.2.2-1 Dual-redundant Ethernet communication module-only configuration

Dual-redundant network

The subsystem communication interface as well as the Ethernet communication module are set as dual-redundant configuration. A network domain for ALE111 with odd slots is separated from another network domain for ALE111 with even slots.

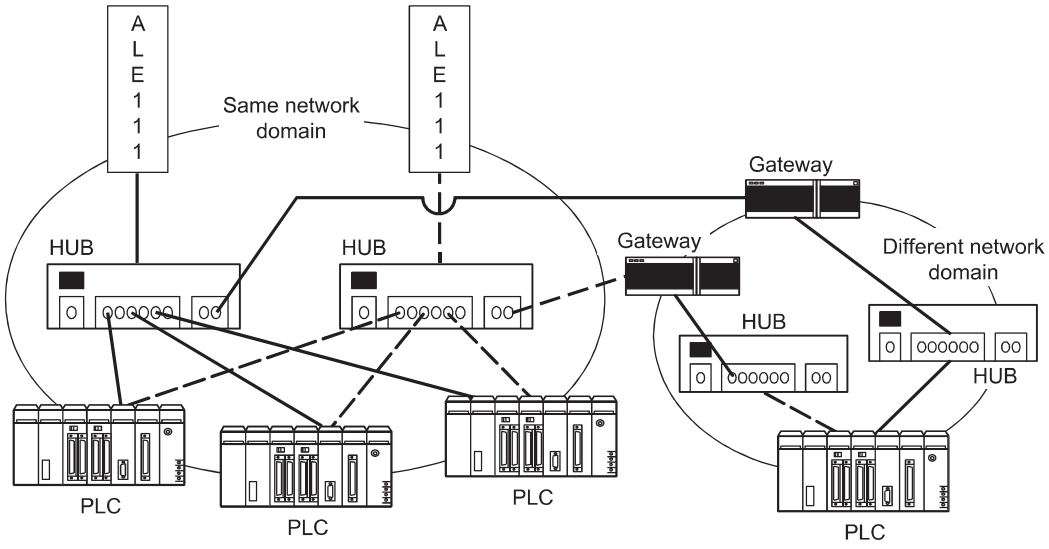


Figure D1.2.2-2 Dual-redundant network configuration

Dual-redundant switching method

Control right switch if any of the following conditions is true in dual-redundant ALE111 configuration.

- Condition 1
  Standby ALE111 is in normal state, and control ALE111 is in abnormal state
- Condition 2
  If all communication in standby ALE111 are in normal state, and any part of communication in control ALE111 is in abnormal state

In Service/Out Service system alarms will be sent if the control right in ALE111 are switched. If the switching is due to communication error, the SS-COM Error system alarm will also be sent. However, the SS-COM alarm may not be sent because the SS-COM Error alarm will not continue to be sent during a communication error in the same station number.

Limitations on dual-redundant Ethernet communication modules

This section explains the restrictions when the Ethernet communication module is set to dual-redundant configuration.

- Dual-redundant configuration during an online change is not guaranteed.
- Dual-redundancy is not supported if addresses without readback are used. To provide a dual-redundant configuration, you need to use only addresses with readback.

TIP

If an address without readback is specified in a dual-redundant configuration, the following problems will occur.

With readback, data is read from the Modbus/TCP PLC, compared with the data in the CPU of the SCS, and then the CPU data is written to the subsystem if the two data are different.

Without readback, the data in the CPU is compared with the data in the communication module, without reading data from the subsystem, and the CPU data is written to the Modbus/TCP PLC only when there is a difference between the data.

If the communication module on the control side is normal, the data in the communication module on the standby side is not updated. Therefore the data in the module may be old when the control right switches. In this case, the data in the CPU cannot be compared with the data in the communication module, and data cannot be written without readback.

In Modbus communication, whether or not readback is used is determined by an address function code that is specified in the Communication I/O Builder.

SEE ALSO

For more information about readback communication, refer to:

D2.5, “Readback communication” on page D2-20

D1.3 Error handling actions

This section describes the error handling actions after a restart of the subsystem communication module, initial cold start of the SCS, occurrence of a communication error, and so on.

Error conditions and error handling actions

The following table summarizes the conditions in which error handling actions occur, as well as the specific actions.

Table D1.3-1 Conditions in which error handling actions occur and specific actions

Condition	Impact on application logic (Subsystem communication I/O FBs)	Subsystem communication
Initial cold start of the SCS (the SCS operating mode is shifting from Waiting Mode to Running Mode)	Input data: Value from the subsystem Input status: GOOD Output status after output enable operation: GOOD	Only inputs are communicated and data is not output until the output enable operation is performed. Output starts after the completion of output enable operation (for subsystem communication) (*1)
• Communication error (subsystem communication error, communication definition error) • Faulty subsystem communication module • Restart of the subsystem communication module due to online change download • Path error between the CPU and subsystem communication module	Upon occurrence Input data: Value of "Input Processing at Fault" Input status: BAD Output status: BAD After recovery Input data: Value from the subsystem Input status: GOOD Output status: GOOD	At occurrence: communication not possible (*2) After recovery: I/O is resumed. Values are output from the application logic (*3) (*4)
Adding a new subsystem communication I/O FB (online change download) (*5)	During online change download Input data: 0 or FALSE Input status: BAD Output status: BAD After online change download Input data: Value from the subsystem Input status: GOOD Output status: GOOD	No impact. Communication continues.
Adding a subsystem communication module online (*6)	Until the module starts up Input data: 0 Input status: BAD Output status: BAD After the module started up Input data: Value from the subsystem Input/output status: Status of communication with the subsystem	Until the module starts up: Communication is not possible. After the module started up: Communication starts. In the case of outputs with readback, the output values are read back from the subsystem immediately after the recovery of subsystem communication and are output. After that, values from the application logic are output.

*1: The output enable operation using SCS Maintenance Support Tool enables both safety output and subsystem communication output. Dedicated system function blocks are provided for enabling safety output and subsystem communication output, respectively.
*2: The SCS operating mode is not affected by communication errors or subsystem communication module errors.
*3: If errors need to be latched, application logics that reference data status needs to be created.
*4: If the subsystem communication module is locked and in the case of outputs with readback, the output values are read back from the subsystem immediately after the recovery of subsystem communication and are output.
*5: Even when a subsystem communication I/O FB instance is deleted and then a new instance is recreated, it is recognized as addition of a new subsystem communication I/O FB.
*6: The operating mode of the SCS is not affected because the output of the SCS stays enabled.

Restart of the subsystem communication module when subsystem communication data is locked

If you perform the following types of operations that require a subsystem communication module restart, it is recommended that you lock the subsystem communication data first.

- Before performing an online change download requiring a restart of the subsystem communication module
- Before replacing the failed subsystem communication module. Perform an IOM download after the replacement.

The following table lists the values and statuses of locked communication I/O data before and after the recovery of the subsystem communication module to a normal state.

Table D1.3-2 Statuses of locked communication I/O data

		Before recovery	After recovery
Communication input	Logical data	Data value: Value immediately before locking Data status: Value immediately before locking	Data value: Value immediately before locking Data status: Value immediately before locking
	Physical data	Data value: Value immediately before occurrence of an error Data status: BAD	Data value: Value from the subsystem Data status: GOOD
Communication output	Logical data	Data value: Value from the application logic Data status: Value immediately before locking	Data value: Value from the application logic Data status: Value immediately before locking
	Physical data	Data value: Value immediately before locking Data status: BAD	Data value: Output value from the subsystem immediately after recovery of communication Data status: GOOD
Output to subsystem		Communication is not possible.	Input: Resumed. Output: Output value from the subsystem immediately after recovery of communication

Notification of error conditions

- Error conditions such as errors in the subsystem communication module and those relating to subsystem communication are notified to the application logic, SENG and HIS.
- To handle error conditions in the application logic, use system FBs for subsystem communication.
- With the use of system FBs for subsystem communication, an application logic that detects unlocked subsystem communication data and overflow of lock limit can be created. If any subsystem communication data remains unlocked or the number of locks exceeds the maximum value, a diagnostic information message will be notified to the SENG or HIS.

Diagnostic information messages

If the subsystem communication module status or communication status with any subsystem has changed, a diagnostic information message is generated to notify the change. Diagnostic information messages are generated in the following conditions:

- The subsystem communication module has started or shut down.
- A subsystem communication error has occurred or has been reset.

- A subsystem communication output enable operation has been performed.
- When a subsystem communication module is added or deleted online

Conversion of real-type input data

When the communication I/O data is real-type input data and the value is Not-A-Number (NaN), infinity, or subnormal, the communication I/O data I/O function of SCS converts the physical data to logical data as shown in the following figure and pass it to the application Logic.

Table D1.3-3 Data conversion for real-type input data with NaN, infinity, or subnormal values

Physical data	Logical data
Value: NaN Data status: GOOD	Value: pre-defined input value at fault Data status: BAD
Value: NaN Data status: BAD	
Value: infinity Data status: GOOD	Value: pre-defined input value at fault Data status: BAD
Value: infinity Data status: BAD	
Value: subnormal Data status: GOOD	Value: 0.0 Data status: GOOD
Value: subnormal Data status: BAD	Value: pre-defined input value at fault Data status: BAD

Display of NaN, infinity, or subnormal values

When the value of physical data of communication I/O data is NaN, infinity, or subnormal, the value is displayed in the Communication I/O Lock window as shown in the following table.

Table D1.3-4 Display format for physical data with a NaN, infinity, or subnormal value

Display format	NaN			Positive infinity	Negative infinity	Subnormal
Displayed with 5 decimal places	1.#QNAN	-1.#QNAN	-1.#IND0	1.#INF0	-1.#INF0	0.00000

D1.4 Setting items relating to subsystem communication

The following describes the setting items relating to subsystem communication. Subsystem communication builders can be used to set items relating to communication modules and those relating to communication I/O data. This section mainly describes for the case when performing RS original engineering.

- Settings relating to communication module
  To perform subsystem communication, define the serial communication module (ALR111/ ALR121) or Ethernet communication module (ALE111) and set required I/O parameters. When performing I/O list engineering, you can use the IOM Definition Editor. When performing RS original engineering, you can use the I/O Wiring View and I/O Parameter Builder.
- Settings relating to communication I/O data
  You need to allocate the communication I/O data, and assign element numbers and subsystem communication I/O FB. When performing I/O list engineering, you can use Safety Communication I/O Editor. When performing RS original engineering, you can use Communication I/O Builder.

TIP

The setting item names displayed may differ between I/O list engineering and RS original engineering, but the settings are the same.

SEE ALSO

For more information about engineering of subsystem communication modules using Safety Communication I/O Editor, refer to:

D1.5, “Engineering for subsystem communication modules” on page D1-37

For more information about I/O list engineering, refer to:

D., “Procedures to create applications using the I/O list engineering method” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about RS original engineering, refer to:

Appendix 2., “RS original engineering” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Builders for subsystem communication

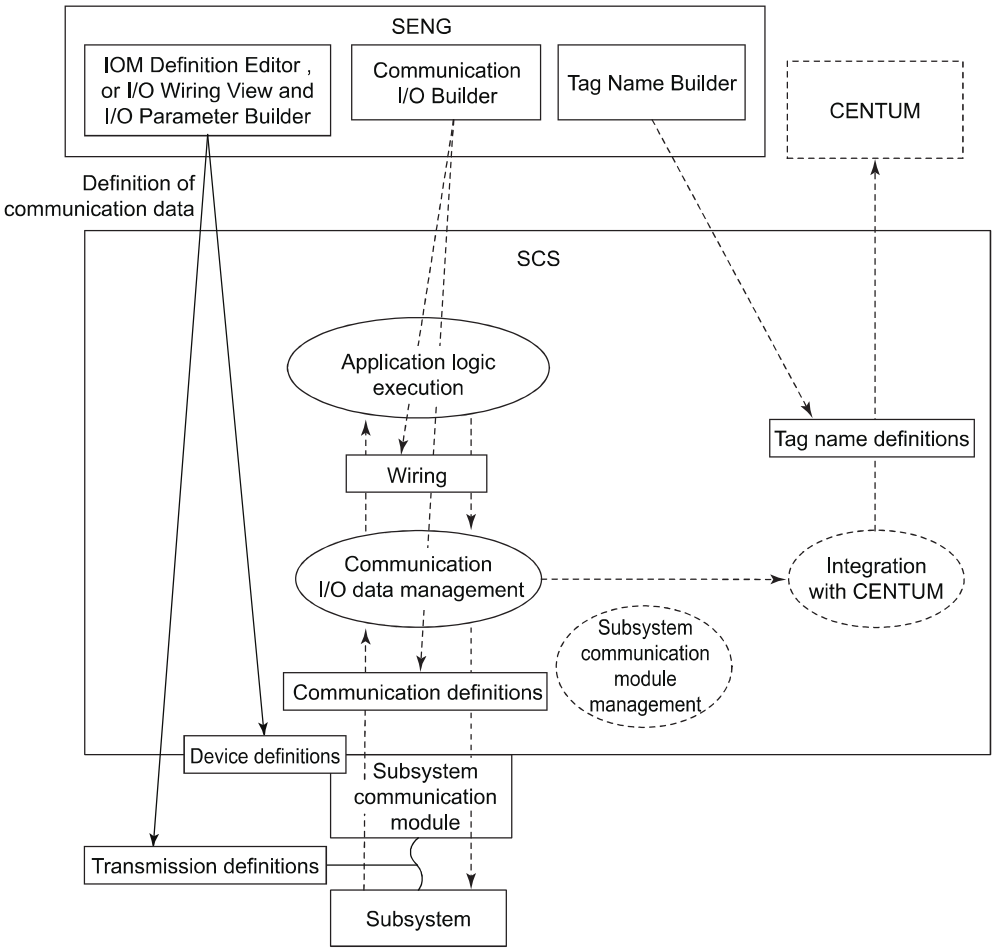


Figure D1.4-1 Subsystem communication builders

Subsystem communication settings

- Device definitions provide settings relating to the mounting position and redundancy of the subsystem communication module.
- Transmission definitions provide settings relating to the transmission specifications of the subsystem communication module. The setting items vary depending on the type of subsystem communication module.
- Communication definitions provide settings relating to data accesses to/from subsystems. The setting items vary depending on the communication protocol.
- Wirings provide settings for assigning the communication I/O data area to subsystem communication I/O FBs.

Settings related to integration with CENTUM

- Tag name definitions provide settings for assigning tag names to subsystem communication I/O FBs.

Engineering procedure using related builders

The I/O Wiring View, I/O Parameter Builder, Communication I/O Builder, and Dictionary View are used to create communication definitions. The procedure and builders used in each step are as follows:

1. Define subsystem communication I/O FBs by using the Dictionary View.
2. Define a subsystem communication module by using the I/O Wiring View.
   Add a subsystem communication module, and set its mounting position (node number, slot number) and specify whether to use a dual-redundant or single configuration.
3. Set parameters for the subsystem communication module by using the I/O Parameter Builder.
4. Define communication I/O assignments in the Comm. I/O Definition tab of the Communication I/O Builder. Assign subsystem communication data to element numbers. This assigns the subsystem communication data to the communication I/O data area.
5. Associate the element numbers and subsystem communication I/O FBs in the Comm. I/O Wiring tab of the Communication I/O Builder.
   Associate (wire) the subsystem communication I/O FBs defined in step 1 with the element numbers defined in step 4. Associate one subsystem communication I/O FB with one element number. This links the subsystem communication data assigned to the communication I/O data area with the subsystem communication I/O FBs.

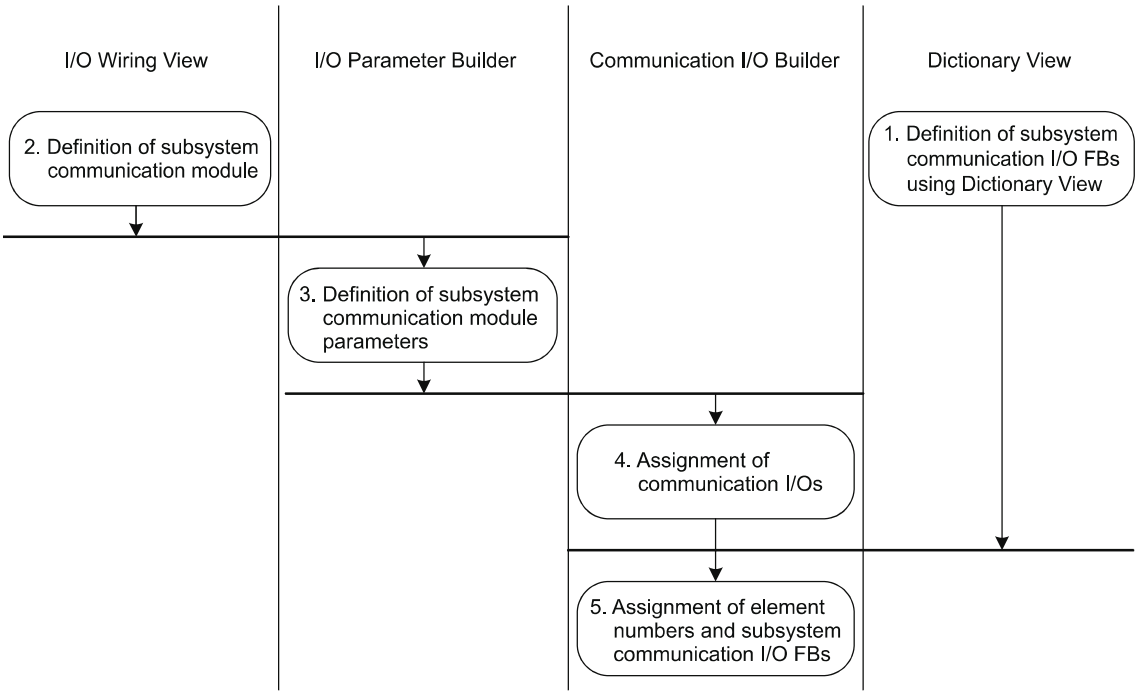


Figure D1.4-2 Engineering procedure using related builders

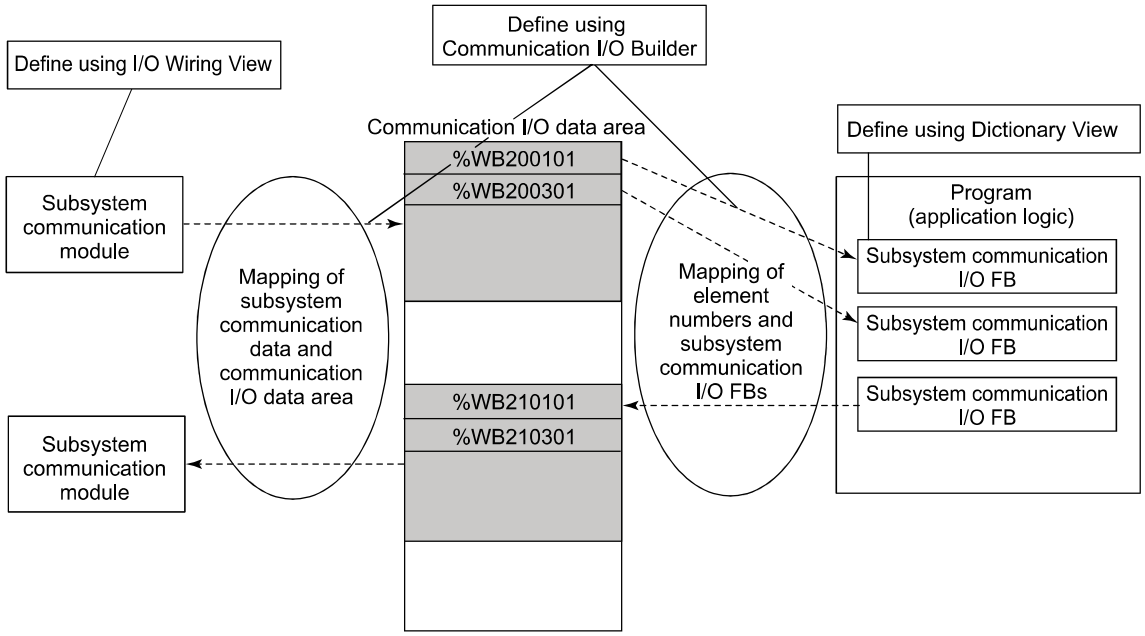


Figure D1.4-3 Wiring of subsystem communication I/O FBs and element numbers

The types of subsystem communication I/O FBs vary depending on the type of communication I/O data to be assigned.

Table D1.4-1 Types of subsystem communication I/O FBs and types of data that can be wired

Data type	Type of wirable subsystem communication I/O FBs
Analog input (16-bit signed integer)	SCI_I
Analog input (32-bit signed integer) (*1)	
Analog input (16-bit unsigned integer)	
Analog input (32-bit floating) (*1)	SCI_R
Analog output (16-bit signed integer)	SCO_I
Analog output (32-bit signed integer) (*1)	
Analog output (16-bit unsigned integer)	
Analog output (32-bit floating) (*1)	SCO_R
Discrete input	SCI_B
Discrete output	SCO_B

*1: This data type cannot be used in communication with ProSafe-SLS.

D1.4.1 Settings using the I/O Parameter Builder

When performing RS original engineering, you can use the I/O Parameter Builder to set the parameters in the subsystem communication module. The parameters to specify differ depending on the type of the communication module.

When performing I/O list engineering, the builder becomes display-only.

Serial communication module settings for subsystem communication

Serial communication module settings for subsystem communication are specified in the Module tab where common communication module parameters are set, and in the Port tabs where port parameters are set.

The Port tabs include the Port 1 and Port 2 tabs. Together with the Module tab, thus, a total of three tabs are available.

SEE ALSO

For more information about recommended settings and items for consideration when using the Modbus communication program with the serial communication module, refer to:

D2.4.2, “Items set in the I/O Parameter Builder” on page D2-16

Module tab

The following items are set in the Module tab:

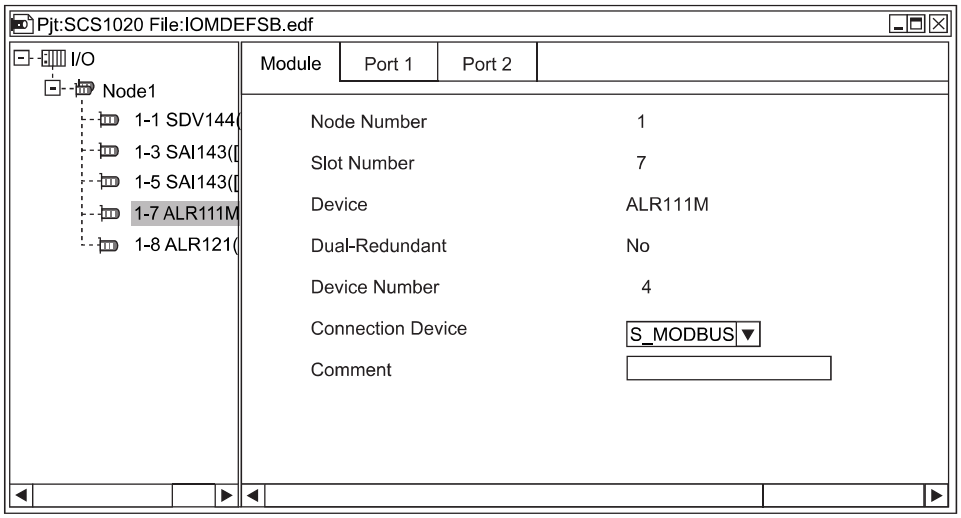


Figure D1.4.1-1 Module tab (serial communication module for subsystem communication)

Node Number

The node number corresponding to the mounting position of the module is displayed. The node number is defined in the I/O Wiring View of SCS Manager.

- The "Node Number" field is read only.

Slot Number

The slot number corresponding to the mounting position of the module is displayed. The slot number is defined in the I/O Wiring View of SCS Manager.

- The "Slot Number" field is read only.

Device

The type of module is displayed. The device (module type) is defined in the I/O Wiring View of SCS Manager.

- The "Device" field is read only.

Dual-Redundant

Whether the module is used in a single or dual-redundant configuration is displayed. The dual-redundant specification is defined in the I/O Wiring View of SCS Manager.

- The "Dual-Redundant" field is read only.

Device Number

The device number assigned to the module. The device number is defined in the I/O Wiring View of SCS Manager.

- The "Device Number" field is read only.

Connection Device

Set the type of connection device (subsystem). This field is displayed only when the module type is a subsystem communication module.
Select the subsystem communication program to be used.

Comment

A comment regarding the module. A desired comment can be entered using up to 24 single-byte characters or 12 double-byte characters.

Port 1 and Port 2 tabs

The setting items in the Port 1 and Port 2 tabs change in accordance with the module type and the "Connection Device" setting in the Module tab. The setting items are the same between the Port 1 and Port 2 tabs.

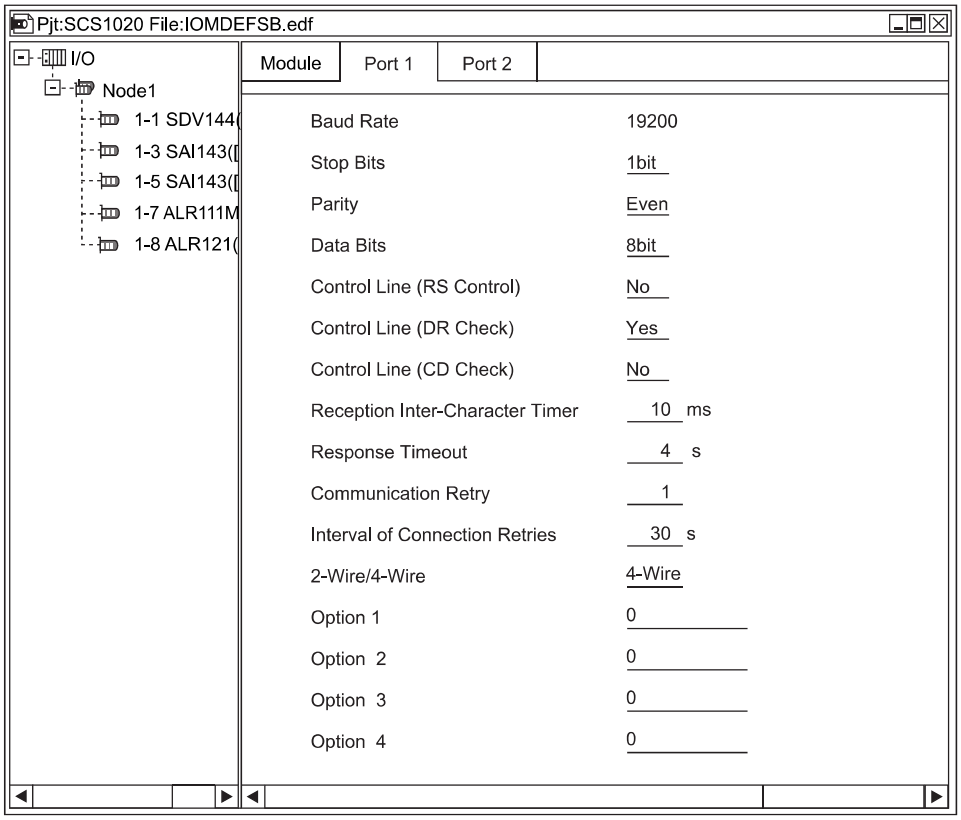


Figure D1.4.1-2 Port 1 tab (example where S_MODBUS is set as Connection Device)

Table D1.4.1-1 Setting items available in Port 1 and Port 2 tabs

Title		Description	Remark
Baud Rate		Specify the baud rate.	-
Stop Bits		Specify the stop bits.	-
Parity		Specify the type of parity.	-
Data Bits		Specify the data bit length of subsystem data to be transmitted.	-
Control Line	RS Control	Specify whether or not to use RS control when sending data from the ALR111M.	Valid only when the ALR111M is used.
	DR Check	Specify whether or not to use DR signal line check when sending data from the ALR111M.	Valid only when the ALR111M is used.
	CD Check	Specify whether or not to use CD signal line check when sending data from the ALR111M.	Valid only when the ALR111M is used.
Reception Inter-Character Timer		Specify the period to monitor inter-character time when data is received by the ALR111M/ALR121M.	-
Response Timeout		Set the timeout period to wait for subsystem response.	-
Communication Retry		Set the number of retries to be attempted after a communication error occurs.	-
Interval of Connection Retries		Set the interval of communication with a station that generated a communication error to check for recovery of communication (recovery communication).	-

Continues on the next page

Table D1.4.1-1 Setting items available in Port 1 and Port 2 tabs (Table continued)

Title	Description	Remark
2-Wire/4-Wire	Specify the 2-wire or 4-wire connection method.	Valid only when the ALR121M is used.
Options 1 to 4	Not used	-

Baud Rate

Specify the baud rate of communication. Select from 1200, 2400, 4800, 9600, 19200 and 38400 bps. The default is 19200 bps.

Stop Bits

Specify the stop bits of communication. Select 1 bit or 2 bits. The default is 1 bit.

Parity

Specify the parity. Select None, Odd or Even. The default is Even.

Data Bits

Specify the data bit length of subsystem data to be transmitted. Select 7 bits or 8 bits. The default is 8 bits.

RS Control

Specify whether or not to use RS control when sending data from the ALR111M. This setting is valid only when the ALR111M is used. The default is No (without RS control).

- No (without RS control)
  The RS signal line is always turned ON regardless of whether or not data is sent from the ALR111M.
- Yes (with RS control)
  The RS signal line is turned ON when data is sent from the ALR111M, and turned OFF after the sending is completed.

DR Check

Specify whether or not to use DR signal line check when sending data from the ALR111M. This setting is valid only when the ALR111M is used. The default is Yes (with DR check).

- No (without DR check)
  Text data is sent from the ALR111M regardless of the DR status.
- Yes (with DR check)
  Text data is sent from the ALR111M only when the DR is ON. If the DR signal line does not turn ON after elapse of the transmission enable monitoring time, a "Line Not Ready (A393)" error will occur.

The DR signal is normally connected to the ER (Data Terminal Ready) signal line of the subsystem and used to determine if the subsystem can receive data (normal operation). If the signal line of the subsystem cannot be used, set No (without DR check) in this field or change the wiring so that the DR signal line turns ON (*1) .

*1: For example, the RS signal line of the applicable module can be looped back to the DR signal line.

CD Check

Specify whether or not to use a CD signal line check when sending data from the ALR111M. The default is No (without CD check).

- No (without CD check)
  Text data is sent from the ALR111M regardless of the CD status.

- Yes (with CD check)
  Text data is sent from the ALR111M only when the CD is OFF. If the CD signal line does not turn OFF after elapse of the transmission monitoring time, a "Communication line busy (A392)" error will occur.

Reception Inter-Character Timer

The reception inter-character timer (reception inter-character timeout setting) is a function for monitoring the time between adjacent characters received (interval after one character is received until the next character is received) by the ALR111M/ALR121M. In the Modbus communication program, the receive operation is considered complete if no characters are received within the set time.

If communication is performed via a modem or other device that provides data buffering function, this value needs to be set in consideration of the communication delay (inter-character delay) caused by the buffering at the modem. Note, however, that increasing the reception inter-character time will affect the RS communication time, since completion of reception is determined based on elapse of this time.

Default: 10 ms

Setting range: 0 to 99999 ms

Response Timeout

Set the timeout period to wait for subsystem response. The unit is second.

Default: 4 sec

Setting range: 0 to 99 sec

Communication Retry

Set the number of retries to be attempted after a communication error occurs.

Default: 1 time

Setting range: 0 to 99 times

Interval of Connection Retries

Set the interval of communication with a station that generated a communication error to check for recovery of communication (recovery communication). The unit is second.

Default: 30 sec

Setting range: 1 to 999 sec

2-Wire/4-Wire

Specify the 2-wire or 4-wire connection method used by the ALR121M. This setting is valid only when the ALR121M is used.

Option 1 to 4

Specify the different communication parameter options for each subsystem communication program.

Ethernet communication module settings for subsystem communication

For an Ethernet communication module for subsystem communication, you can specify the parameters in the Module tab.

SEE ALSO For more information about recommended settings and items for consideration when using the Modbus communication program with the Ethernet communication module, refer to:

D3.3.2, “Settings in the I/O Parameter Builder” on page D3-10

D1.4.2 Settings using the Communication I/O Builder

The Communication I/O Builder is used to define communication I/O data assignments and wire communication I/O variables.

When performing I/O list engineering, the builder becomes display-only.

SEE ALSO

For more information about recommended settings and items for consideration when using the Modbus communication program with the serial communication module, refer to:

D2.4.3, “Items set in the Communication I/O Builder” on page D2-17

For more information about recommended settings and items for consideration when using the Modbus communication program with the Ethernet communication module, refer to:

D3.3.3, “Settings in the Communication I/O Builder” on page D3-13

Communication I/O settings

The Communication I/O Builder is used to perform the following tasks:

- Assign subsystem communication data to the communication I/O data area (%WW)
- Define communication details in the communication I/O data area in accordance with the subsystems
- Wire %WB elements and communication I/O variables

The structure of the Communication I/O Builder window is as follows:

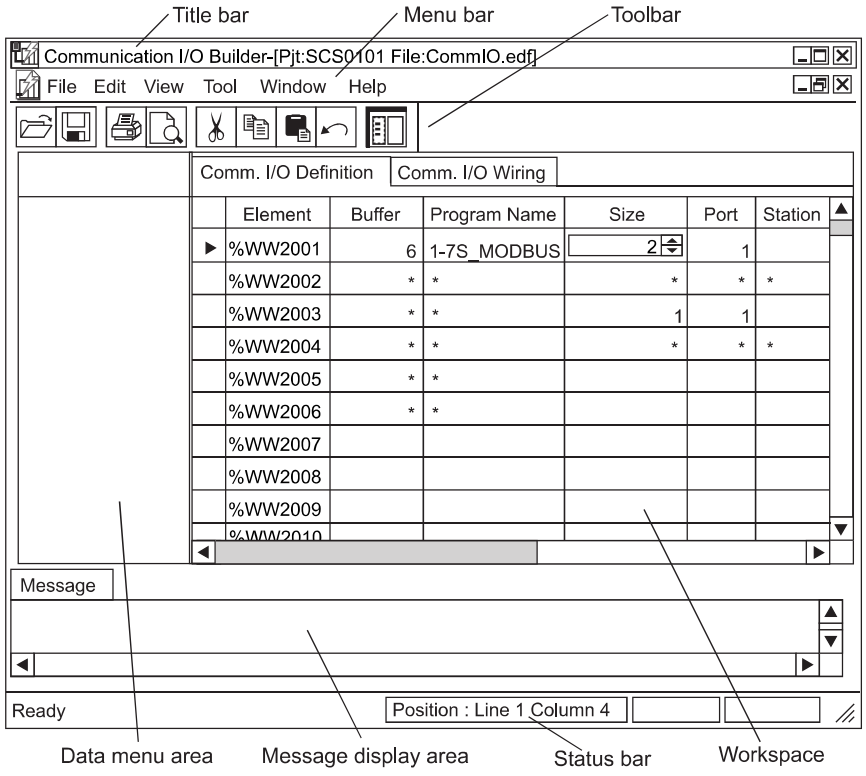


Figure D1.4.2-1 Structure of Communication I/O Builder window

Comm. I/O Definition tab

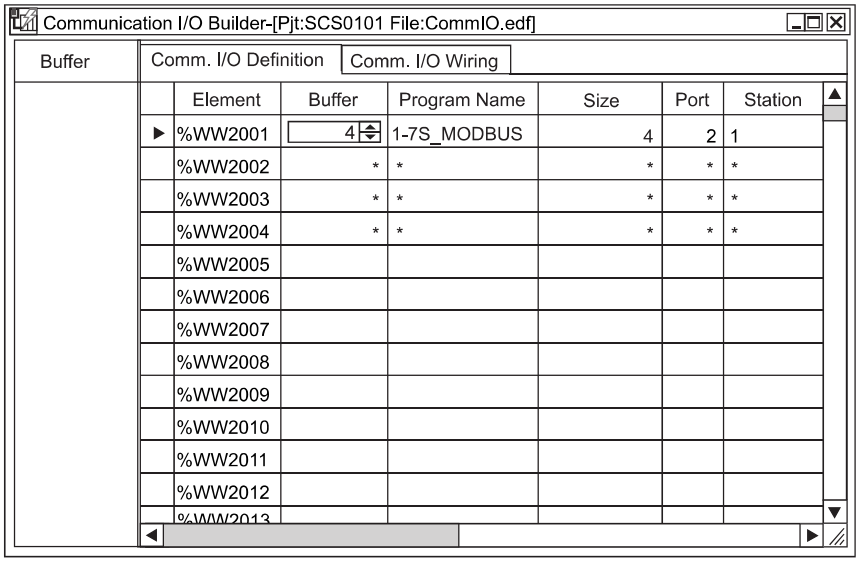


Figure D1.4.2-2 Comm. I/O Definition tab

The items set in the Comm. I/O Definition tab are as follows:

- Element: Read only
- Buffer
- Program Name
- Size
- Port
- IP Address
- 2nd IP Address
- Station
- Device Address
- Data Type
- Reverse
- Input Processing at Fault
- Input Value at Fault

Element

The buffer address within the communication I/O data area is displayed.

Display format: %WWnnnn

%WW: Fixed

nnnn: 2001 to 3000

Buffer

You need to specify the size of the communication I/O data area to be used by the subsystem communication program, in units of words (16 bits). This can only be entered when the "Element number" row is an odd number.

- Input unit: 2 (even number)
- Input range: 2 to 1000
- Size limitation: The total size shall not exceed 1000.

After a size has been specified to allocate the buffer, moving to the next setting item will display asterisks (*) in the subsequent "Buffer" and "Program Name" fields corresponding to the buffer size that has been allocated, where there is no error in the defined items. These asterisks indicate that the applicable communication I/O data area has been allocated. The "Buffer" and "Program Name" fields showing asterisks do not accept new settings. Deleting a "Program Name" for which a buffer is allocated will not delete the asterisks in the corresponding "Program Name" field.

If a "Buffer" is deleted, the items defined in the allocated buffer area (Program Name, Size, Port, IP address, 2nd IP address, Station, Device Address, Data Type, Reverse, Input Processing at Fault, Input Value at Fault) as well as asterisks will be deleted, and these fields can accept new settings.

If a "Buffer" is changed, the asterisks will also be changed. The "Buffer" field cannot be changed to a value smaller than the value in the "Size" field. Moreover, the designated value of Buffer should not conflict with the reserved area. If the error value is entered, it would be cancelled so as to revert to the previous value.

Example:

When changing the buffer for %WW2001 to "4"

Table D1.4.2-1 Example of definitions before change

Element	Buffer	Program Name	Size	• • •
%WW2001	2 (*1)	1-3S_MODBUS		
%WW2002	*	*		
%WW2003	4	1-5S_MODBUS		
%WW2004	*	*		
%WW2005	*	*		
%WW2006	*	*		

*1: An attempt to change "2" to "4" will generate an error, since specifying "4" overlaps with the area already allocated for %WW2003.

Program name

Specify the program name by using a combination of the node number and slot number for the defined subsystem communication module, and a fixed character string. The program name can be entered using up to 12 single-byte alphanumeric characters and symbols (+, -, _).
The "Program Name" field cannot be selected if the corresponding "Buffer" field is not specified or no module is defined.

In the case of a dual-redundant module configuration, specify the odd slot number.

Program Name : n-s Fixed character string

- n: Node number
- s: Slot number
- Fixed character string:
  Enter the character string determined for the subsystem ("Connection Device" specified with the I/O parameter).

If the program name is changed, a confirmation dialog box appears with a message asking if you want to delete the communication data and wirings. The following shows the content of communication data.

- Size
- Port
- Station number
- Device Address
- Data type
- Comment
- Reverse

Clicking [OK] deletes the communication data and wirings.

Clicking [Cancel] restores the original program name without deleting the communication data and wirings.

Size

You can set the size (data length) from the beginning address of the area allocated in the "Buffer are". This can only be entered when the "Element number" row is an odd number.

- Input range: 1 to 1000

If an odd number is specified as the size, the odd number will be displayed, but the actual size to be allocated will correspond to an even number being the sum of the specified odd number and 1.

If the data type is SLSEVENT, set the size to 24.

An error will occur in the following situations:

- The specified size exceeds the range allocated in the "Buffer" field.
- The total sum of sizes assigned to all discrete inputs/outputs, when the "Data Type" is discrete input or output, exceeded 256 words.
- An odd value is specified when the "Data Type" is 32-bit analog input or output.
- An attempt is made to change the assigned size to a value other than 24 when the "Data Type" is SLSEVENT.

After specifying a size and moving to the next setting item, asterisks (*) is displayed in the subsequent "Size," "Port," "IP Address," "2nd IP address," "Station," "Device Address," "Data Type" and "Reverse" fields corresponding to the specified size if there is no error in the defined items. These asterisks indicate that data of the specified size has been assigned. The fields with asterisks do not accept new settings. In this case, even if you deleted "Port," "IP Address," "2nd IP Address," "Station," "Device Address," "Data Type" or "Reverse" fields, asterisks cannot be deleted.

If a "Size" is deleted, the items defined in the data of the assigned size (Port, IP Address, 2nd IP Address, Station, Device Address, Data Type, Reverse, Input Processing at Fault, Input Value at Fault) as well as asterisks will be deleted, and these fields can accept new settings.

If a "Size" is changed, the asterisks will also be changed. If the "Size" is changed to a smaller value, the items that have been set in the data corresponding to the size decremented will be deleted.

Table D1.4.2-2 Example of completed item settings

Element	Buffer	Program Name	Size	Port	IP Address	2nd IP Address	Station	Device Address	Data Type	Reverse
%WW2001	4	1-3S_MODTCP	2	1	172.21.0.5	172.21.1.5	1	A10012	Input (Discrete)	No
%WW2002	*	*	*	*	*	*	*	*	*	*

Continues on the next page

Table D1.4.2-2 Example of completed item settings (Table continued)

Element	Buffer	Program Name	Size	Port	IP Address	2nd IP Address	Station	Device Address	Data Type	Reverse
%WW2003	*	*								
%WW2004	*	*								
%WW2005										

Port

You can specify the port for the subsystem communication module.

- When using ALR111M/ALR121M
  Select 1 or 2. The default is 1.
- When using ALE111M
  Always set to 1.

IP Address

You can set the IP address for the subsystem.

2nd IP Address

If the network is set to dual-redundant configuration, you need to set the subsystem IP address where an Ethernet communication module with even slot communicates.

Station

Specify the station number for the subsystem. Select a value between 0 and 255. The specifiable values vary depending on the subsystem. The default is 1.

Device address

Specify the content of data to be acquired from the other device, using a combination of the communication method used by the subsystem and the beginning data address.
To use the SLSEVENT data type, enter "SLSEVENT."

After the SLSEVENT data type is specified, this item is set to "SLSEVENT" automatically.

Data type

Specify the type of subsystem data. The following list shows the data types that can be selected:

- 1: Input (16-Bit Signed) (Analog input (16-bit signed integer))
- 2: Input (32-Bit Signed) (Analog input (32-bit signed integer))
- 3: Input (16-Bit Unsigned) (Analog input (16-bit unsigned integer))
- 4: Input (32-Bit Floating) (Analog input (32-bit floating))
- 5: Output (16-Bit Signed) (Analog output (16-bit signed integer))
- 6: Output (32-Bit Signed) (Analog output (32-bit signed integer))
- 7: Output (16-Bit Unsigned) (Analog output (16-bit unsigned integer))
- 8: Output (32-Bit Floating) (Analog output (32-bit floating))
- 9: Input (Discrete) (Discrete input)
- 10: Output (Discrete) (Discrete output)

- 11: SLSEVENT

If discrete input or output is selected, whether or not the total sum of "Sizes" assigned to all discrete inputs/outputs is 256 words or less is checked. If the total size exceeds 256 words, an error will occur.

If 32-bit analog input or output is selected, whether or not the corresponding "Size" field contains an even number is checked. If an odd number is entered, an error will occur.

When the ProSafe-SLS communication function is used, data types 2, 4, 6, and 8 cannot be specified. Also note that data type 11 can be specified only when the ProSafe-SLS communication function is used.

If data type 11 is selected, using any combination other than the following will lead to an error.

Table D1.4.2-3 Items to be set for acquisition of ProSafe-SLS events

	Program Name	Size	Device Address	Data type
Setting value	n-sS_SLSMOD	24	SLSEVENT	SLSEVENT

Within all the communication definitions, only one SLSEVENT can be defined to one set of station number and port combination. Defining multiple SLSEVENT for the same station number and port combination will lead to a build error.

Reverse

Specify whether or not to store subsystem data in the SCS after reversing the order of bits/words comprising the data.
The selectable items vary depending on the data type specified in the "Data Type" field. The following combinations of reverse specifications can be selected for each data type:

- 32-bit analog input/output: "2: No," "3: Words (word reversing)"
- Discrete input/output: "1: Bits (bit reversing)," "2: No"
- 16-bit analog input/output: Fixed to "2: No"
- SLSEVENT: Fixed to "2: No"

Input processing at fault

Specify the value to be input to the application logic, instead of the input value received from the subsystem, upon detection of an error. This field can be specified only when "discrete input" or "analog input" is selected in the "Data Type" field.
The errors that trigger this setting include errors occurring on both sides of the path from the CPU to the communication module, errors in the communication module, and communication errors between subsystems and the communication module. Errors in subsystems are not applicable.

Table D1.4.2-4 Input processing at fault (discrete input)

Selection		Description
0	0	Set the input value to 0 upon error detection.
1	1	Set the input value to 1 upon error detection.
2	Hold	Retain the value before detection of an error (default).

Table D1.4.2-5 Input processing at fault (analog input)

Selection		Description
2	Hold	Retain the value before detection of an error (default).
3	Fixed Value	Use the input value specified in "Input Value at Fault" upon error detection.

Input value at fault

If "Fixed Value" is specified in "Input Processing at Fault," specify the input value to be used instead of the input value received from the subsystem.

- Default: 0
- Input range: A value of up to 11 digits and containing a negative sign and/or a decimal point

Comm. I/O Wiring tab

The Comm. I/O Wiring tab shows a list of elements corresponding to the areas assigned in the Comm. I/O Definition tab.

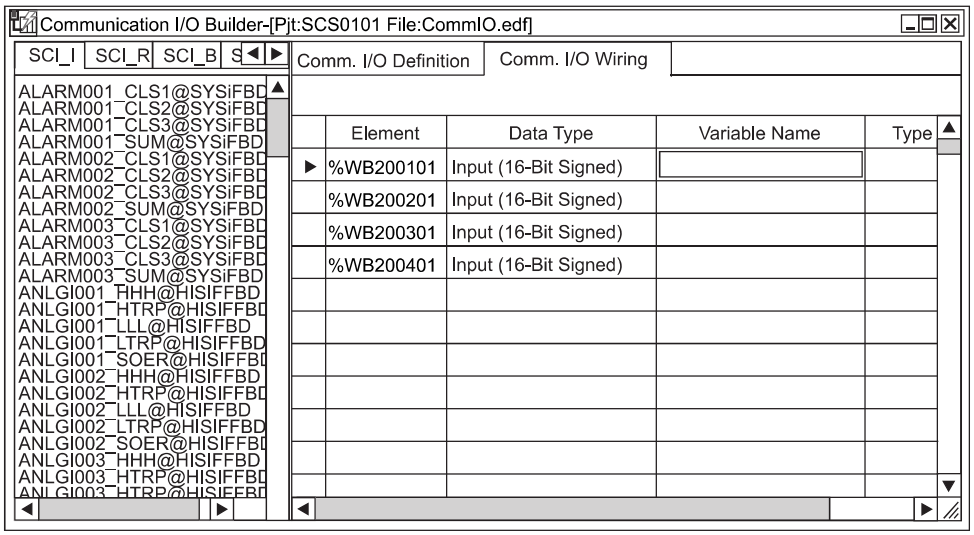


Figure D1.4.2-3 Comm. I/O Wiring tab

The items set in the Comm. I/O Wiring tab are as follows:

- Element: Read only
- Data Type: Read only
- Variable Name
- Type: Read only
- Comment: Read only

Element

An element or elements (%WB) is/are assigned automatically in accordance with the element number (%WW) for which "Buffer" and "Size" have been set in the Comm. I/O Definition tab as well as the applicable "Data Type" field.

Example:

If the selected element is %WW2001, "Size" is 4 words, and "Data Type" is "Input (16-Bit Signed)", the following elements will be assigned automatically:
%WB200101, %WB200201, %WB200301, %WB200401

Because the areas to which data type SLSEVENT is assigned on the Communication I/O Definition tab cannot be wired to variables, such areas do not appear on the Communication I/O Wiring tab.

Data type

The data type specified in the Comm. I/O Definition tab is displayed.

- The "Data Type" field is read only.

Variable name

You can use any of the following methods to set the instance name for a Subsystem Communication FB (SCI_B, SCI_I, SCI_R, SCO_B, SCO_I, SCO_R) in each variable name.

- Enter the variable name directly.
- Double-click on a variable name displayed in the "Variable Name" tab in the left pane.
- Drag a variable name from Dictionary View and drop it into the Variable Name text box.

Table D1.4.2-6 Examples of variable specification

Variable name(*1) (*2)	Scope	Description
SCIB1	Global	Global variable
SCIB2@PROG1	PROG1	Local variable of PROG1 function
FB01.SCIB3	Global	Internal variable SCIB3 of user-defined function block instance FB01
FB01.SCIB3@PROG1	PROG1	Internal variable SCIB3 of user-defined function block instance FB01 defined locally in PROG1 function
FB01.FB2.SCIB3	Global	Internal variable SCIB3 of user-defined function block instance FB2, which is used in user-defined function block instance FB01 (maximum limit of function block nesting)

*1: Also note the following:
- If an instance is a local variable, Scope name must be added after "@".
- If an instance is defined as an internal variable for a User-defined Function Block, assign an instance name to the User-defined Function Block from Dictionary View in Workbench.
- The variable name is specified in the format of "[Instance Name].[Internal Variable Name]," and up to two nests are permitted in each variable.

*2: A variable name can be up to 67 characters long.
Communication I/O Builder also checks the following items:
- The variable name consists only of alphanumeric characters and "@", "." or "_". If any other character is used, an error will occur.
- The variable name begins with an alphabetic character or "_"; otherwise, an error will occur.
- If a variable name has 3 or more nests, an error will result. In the above table, "FB01.SCIB3" and "FB01.SCIB3@PROG1" have one nest, while "FB01.FB2.SCIB3" has two nests.

The following table lists the combinations of variable types and data types specified in the Comm. I/O Definition tab. The types of the variable are the Subsystem communication FBs.

Table D1.4.2-7 Data types and specifiable variable types

Data type	Variable type
Analog input (16-bit signed integer)	SCI_I
Analog input (32-bit signed integer)	
Analog input (16-bit unsigned integer)	
Analog input (32-bit floating)	SCI_R
Analog output (16-bit signed integer)	SCO_I
Analog output (32-bit signed integer)	
Analog output (16-bit unsigned integer)	
Analog output (32-bit floating)	SCO_R
Discrete input	SCI_B
Discrete output	SCO_B

Type

The selected variable type is displayed. The type of the variable is the Subsystem communication FB.

- The "Type" field is read only.

Comment

A comment for the selected variable is displayed.

- The "Comment" field is read only.

D1.5 Engineering for subsystem communication modules

When I/O list engineering is selected, engineering for subsystem communication modules is performed using the safety communication I/O list.

Safety Communication I/O Editor is configured of a grid which defines the Signal Definition list, Program Group Definition list, and Communication Group Definition list.

Follow these steps to define communication I/O:

1. Input the basic definition of the signal definition
   With Safety Communication I/O Editor, set P&ID Tag, I/O Type, Signal Protocol, I/O Tag, Data Type, RS Project, and SCS of the signal definition.
2. Input the IOM assigned information of the signal definition
   Set Node Type, Node, IOM Category, IOM Type, and Slot of the signal definition.
3. Input the data structure of the signal definition
   Set the items for the data structure such as Program Group, Communication Group, Position, and Bit Position.

   Position is the order of %WW in Communication Group. With DI and DO, the order of the bit is set as its Bit Position. Position and Bit Position are required in order to decide the numbers for %WW and %WB in later steps.
4. Create a program group
   Set Program Protocol and Connection Device Type.
5. Create a communication group
   Set the items such as IP Address, Port, and Station.
6. Calculate %WW
   Set Size, Offset, and Element.
7. Reflect onto the SCS project
   When the Build process of RS Generation Manager is run, the safety communication I/O list and information of the IOM are reflected onto the SCS project. The subsystem FB instance specified under I/O Tag is created and wired with the subsystem communication definition.

Creating a program group

Before defining a program group, define I/O points in the Signal Definition list. You can also import the safety communication I/O list.

1. In order to define a program group, click [Program].
   The program group name defined in the Signal Definition list automatically appears.

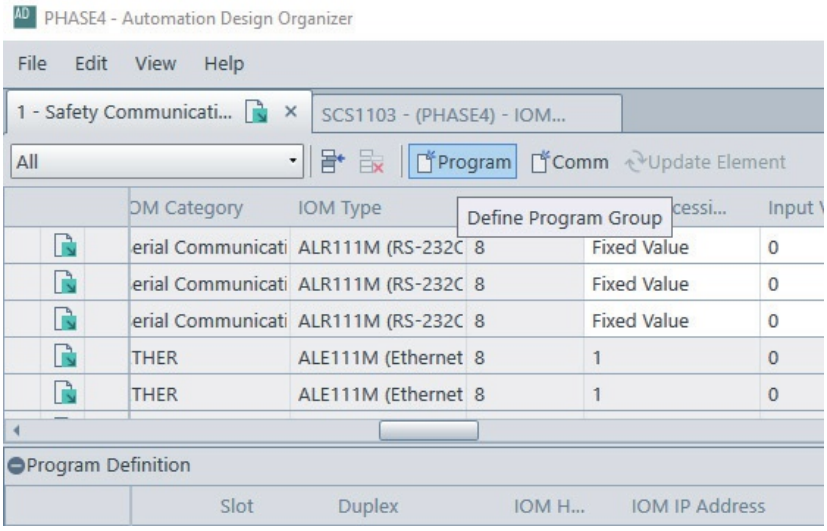


Figure D1.5-1 Defining a program group

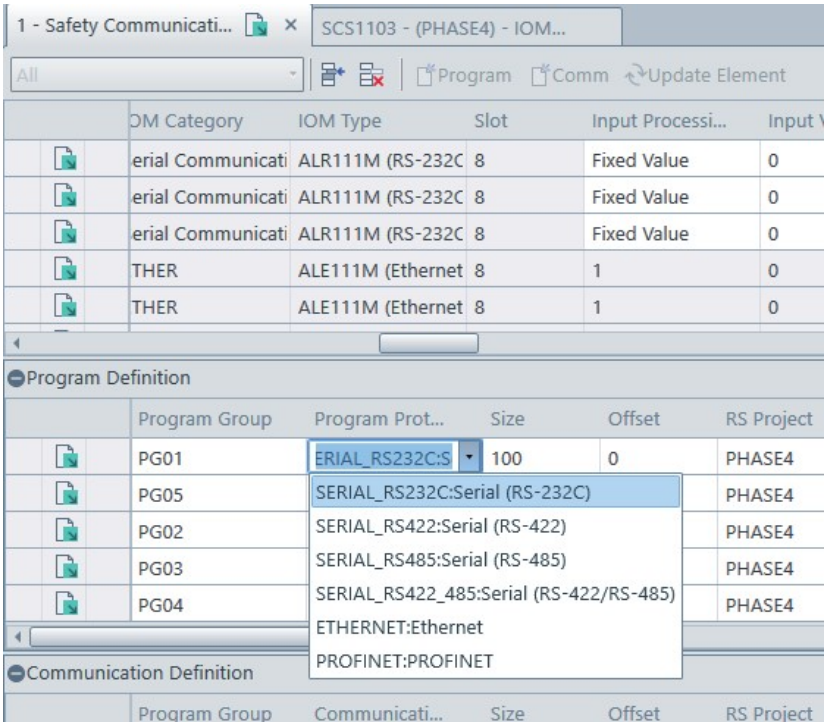


Figure D1.5-2 Example of a program group automatically appearing

2. Define Program Protocol and Connection Device Type.

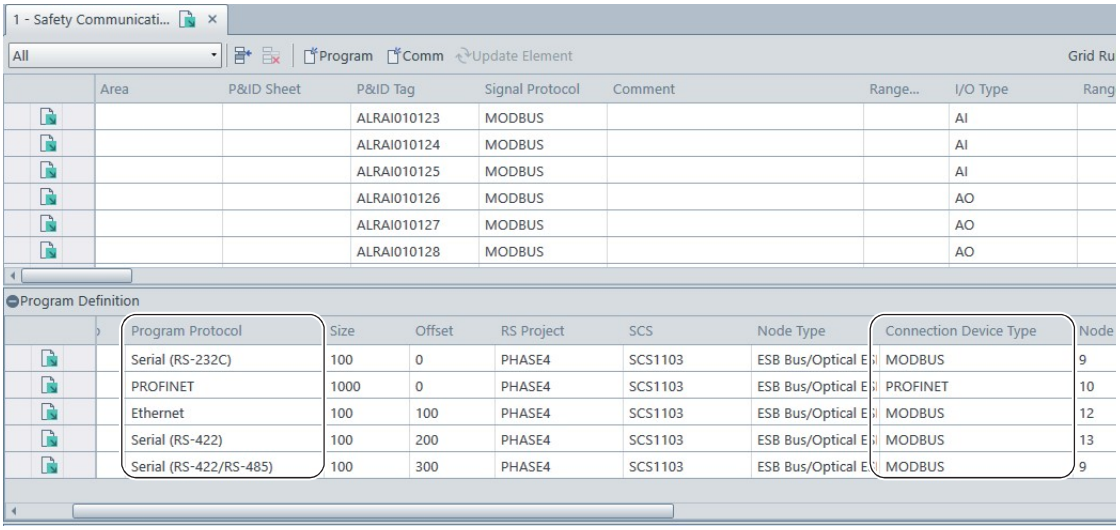


Figure D1.5-3 Example of Program Protocol and Connection Device Type definitions

Creating a communication group

1. In order to define a communication group, click [Communication].
   The program group name and communication group name defined in the Signal Definition list automatically appear.

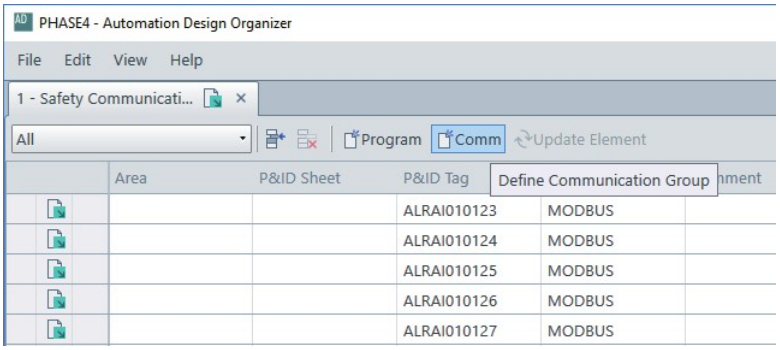


Figure D1.5-4 Communication group definitions

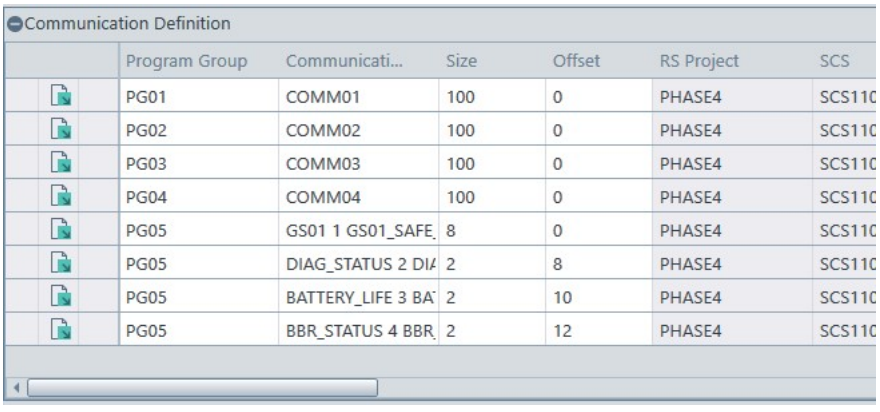


Figure D1.5-5 Display example of the program group name and communication group name

2. Define other necessary information.
3. Save the safety communication I/O list.

Calculating %WW

1. In the SCS folder, open Comm_I/O.

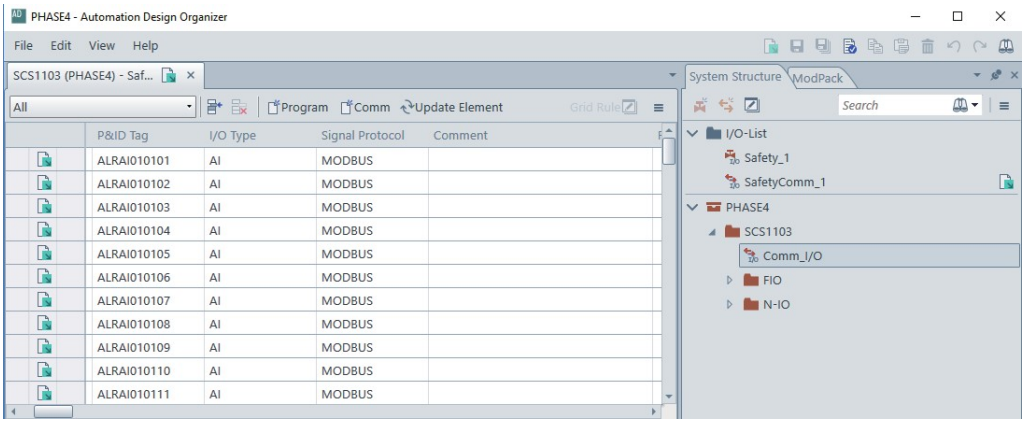


Figure D1.5-6 Display example of Comm_I/O

2. Calculate the size and define the offset of the program group and communication group. In order to automatically set the size, click [Calculate] on the Communication Definition tab.

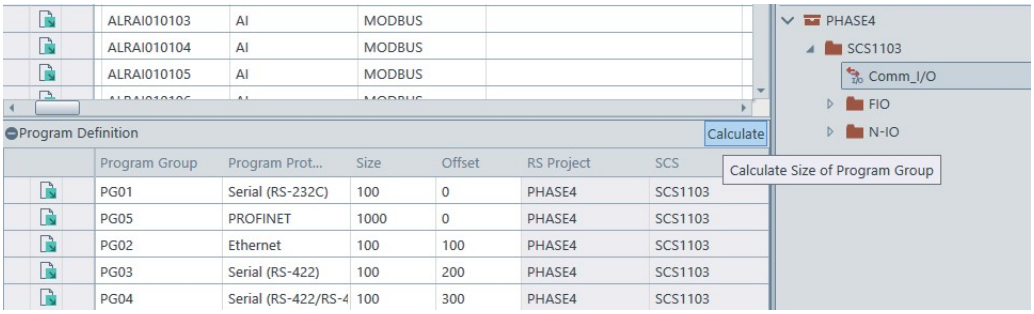


Figure D1.5-7 Resetting the size automatically

3. Define [Offset] in the communication definition.

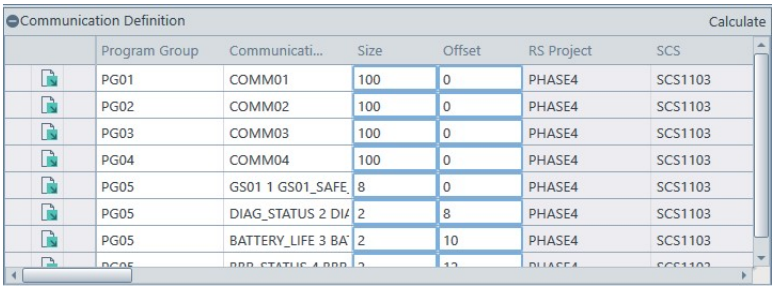


Figure D1.5-8 Defining the offset

4. In order to set Size automatically, click [Calculate] on the Program Definition tab. Then, define Offset in the program definition.

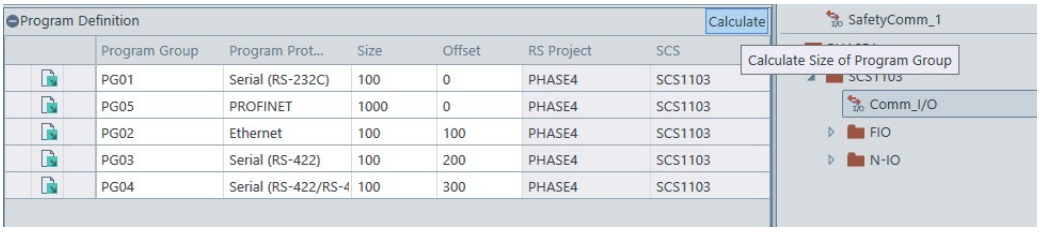


Figure D1.5-9 Defining a program definition with the offset

5. Click [Update Element].
   The element names automatically appear according to the specified position and offset.

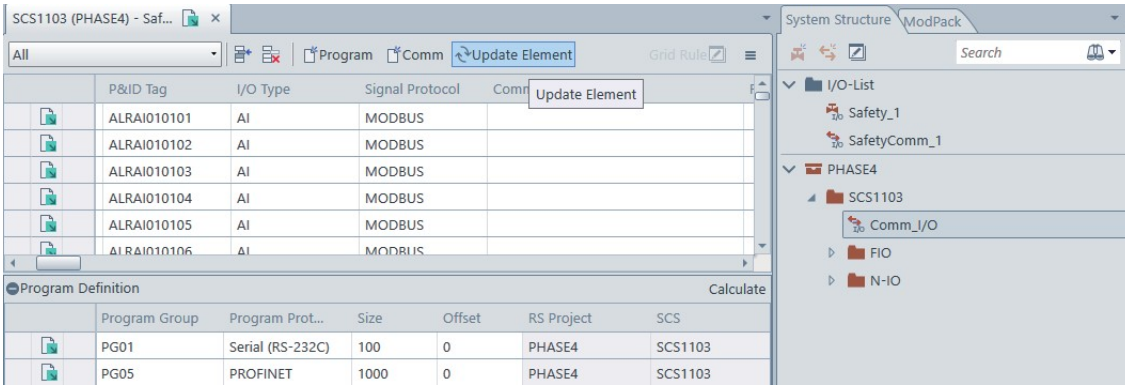


Figure D1.5-10 Automatic display of the element names

6. Change Fix Element of the signal definition to [Y]. Doing so will fix the element numbers. Save the list and check-in.

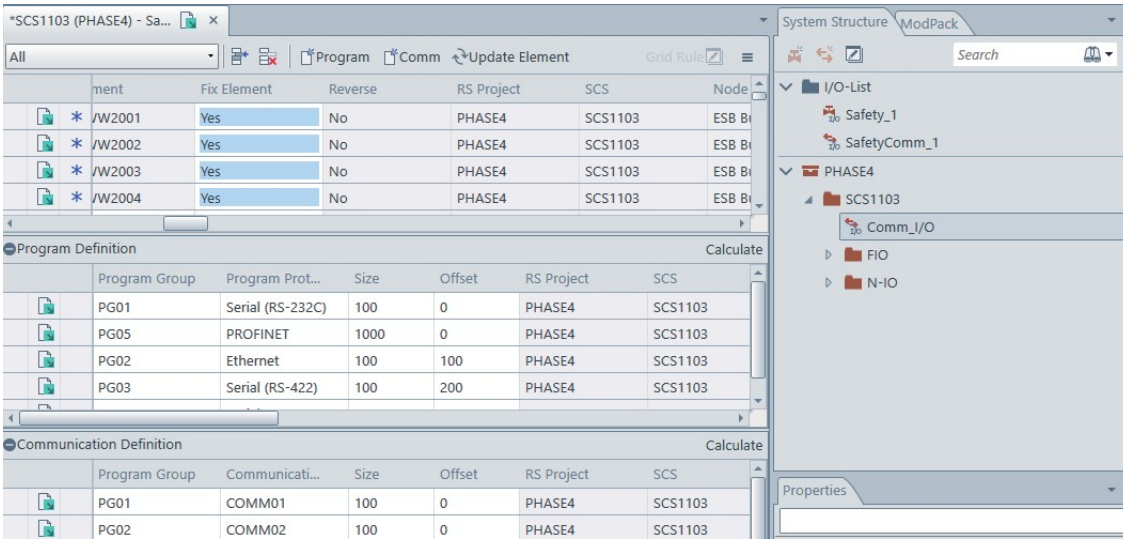


Figure D1.5-11 Fixing the element numbers

D1.6 Storage formats of subsystem data

This section describes the formats in which Modbus equipment data that has been read is stored in the SCS.

The storage formats for different Modbus equipment, such as bit devices, word devices, special coils and communication statuses, are explained.

Bit devices

When 16 x m (m = 1, 2, ...) numbers of bit devices are read from address n in the Modbus equipment, the Modbus equipment data is stored in the SCS as follows.

In the Communication I/O Builder, specify "m" in "Size". You can also reverse the order of bits in units of 16 bits.

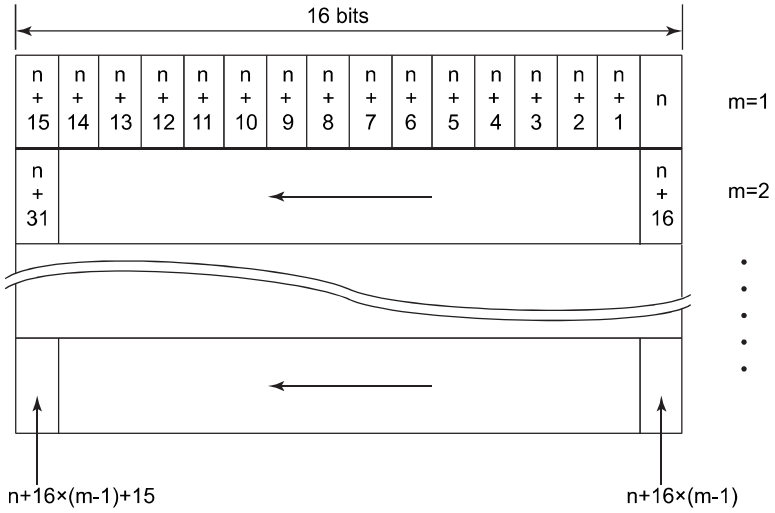


Figure D1.6-1 Storage image of bit devices

Word devices

16-bit data

If m numbers of word devices are read from address n, the applicable word registers (16 bits) in the Modbus equipment will be stored in the SCS as follows.

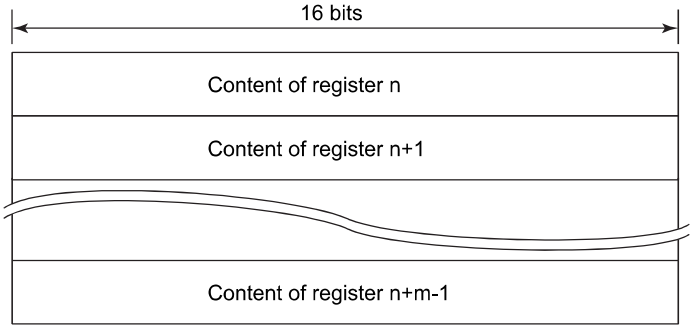


Figure D1.6-2 Storage image of word devices

32-bit data

Word registers (16 bits) in the Modbus equipment are stored in the SCS in the order of registers, as shown in the following. However, if 32-bit data is defined as the data type, two word registers are combined and treated as 32-bit data.

If word reversing is not specified in the SCS (default), the first register is recognized as the upper word, while the next register is regarded as the lower word.

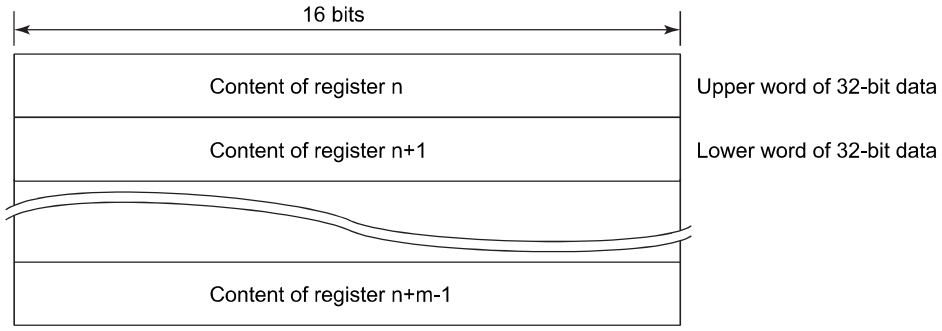


Figure D1.6-3 Order of 32-bit data in SCS (without word reversing)

If 32-bit data is stored in word registers in the Modbus equipment, some Modbus equipment models may store the data in pairs of two 16-bit word registers in the order of low-order word and high-order word, as follows. This word order (16 bits) is opposite to the order in the SCS.

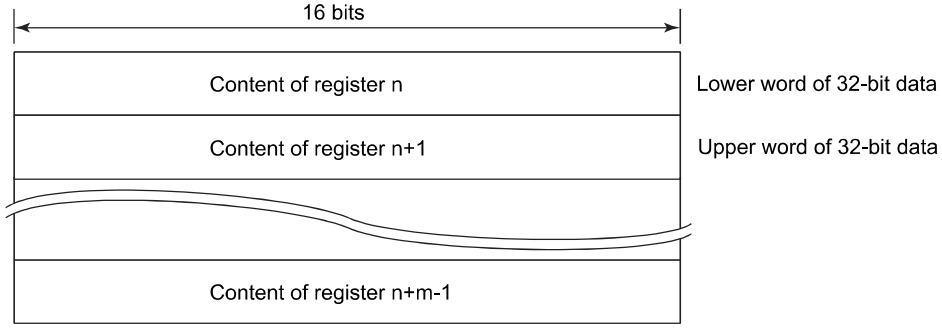


Figure D1.6-4 Order of 32-bit data in Modbus equipment (opposite order from the SCS)

If the previously mentioned Modbus equipment data is to be stored in the SCS, the data order can be switched to units of words (16 bits) by specifying "Reverse" in the Communication I/O Builder.

Special coils

Special coils in Modbus equipment have a data length of 1 word (16 bits). Special coils in Modbus equipment are stored in the SCS as follows.

By specifying "Reverse" in the Communication I/O Builder, you can reverse the order of bits.

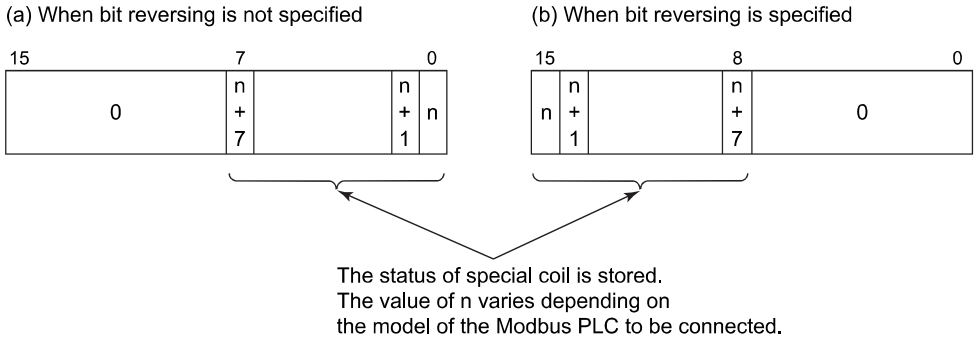


Figure D1.6-5 Storage image of special coil data

Communication status

Modbus equipment communication status STSnnn indicates the status of communication with each station corresponding to a station number of nnn to nnn+15.

The communication status is specified as follows:

- Of the stations defined in the Communication I/O Builder, those communicating normally are indicated as "0."
- Of the stations defined in the Communication I/O Builder, those experiencing an error are indicated as "1."
- Stations not physically performing communication (not defined in the Communication I/O Builder) are indicated as "0".

With communication status, the station number specification in the Communication I/O Builder has no specific meaning. It is only relevant in that the number corresponding to the youngest station among the stations physically performing communication should be set. Specify the address as follows:

Table D1.6-1 Communication status

Description	Address
Communication status of stations 1 to 16	STS001
Communication status of stations 17 to 32	STS017

The correspondence of bits and station numbers is as follows:

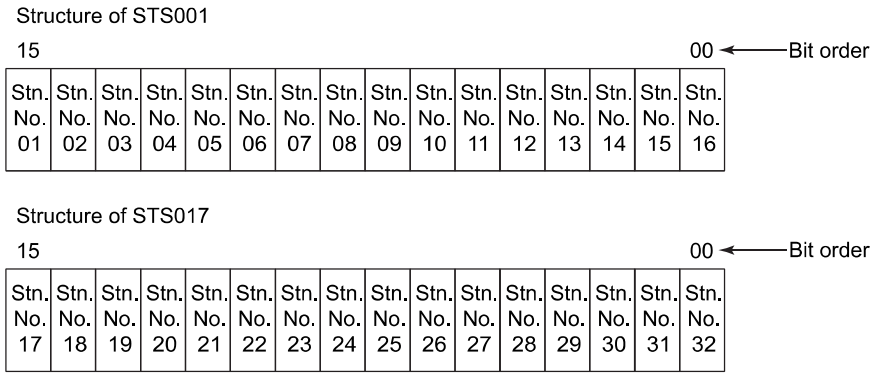


Figure D1.6-6 Correspondence of communication status bits and station numbers

D1.7 Troubleshooting

If a communication module error occurs, you can use the SCS Maintenance Support Tool to acquire information on the communication module and communication error information. This section describes typical troubleshooting cases.

The status display window shows the status of ALR111/121 or ALE111 in red

If the status of the communication module appears in red in the status display window of the SCS Maintenance Support Tool, check the error code that is related to the I/O module of the diagnostic information message.

There is no response and communication fails

- Check if the transmission specifications are consistent with those of the communication destination party.
- Check if the cable wiring complies with the specifications.
- Analyze the communication log for the cause of the communication error by using the SCS Maintenance Support Tool.

A response message under abnormal conditions is received

Analyze the cause of abnormal response from the error code included in the message

Connection cannot be established and communication fails (specific to Modbus TCP)

Check if the destination IP address and port number are correct.

D2. Modbus communication (ALR111, ALR121)

This section explains Modbus communication. The Modbus communication function enables subsystem communication between an SCS and a Modbus PLC, such as the reading and writing of subsystem data, by connecting the Modbus PLC to an ALR111 RS-232C serial communication module or an ALR121 RS-422/RS-485 serial communication module.

Overview of Modbus connection

The subsystem communication function implements communication with PLCs and other subsystems via a subsystem communication module. The Modbus communication program is downloaded to the subsystem communication modules and runs on them.

Reading of data from subsystems or writing of data to subsystems is performed by the application logic execution function via the communication I/O data area and subsystem communication I/O FBs.

The following figure illustrates the flow of data in subsystem communication.

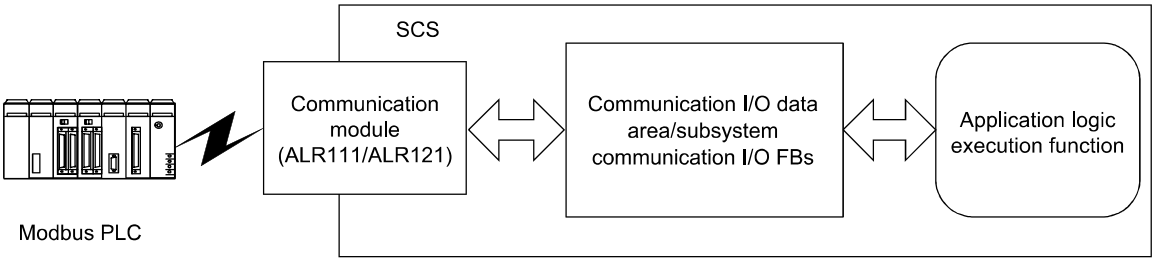


Figure D2-1 Data flow of subsystem communication function

TIP

When using the communication module for CENTUM FCS, you need to perform an IOM download to download the Modbus communication program for the SCS to the module.

D2.1 Communication specifications

This section describes the specifications for communication between an SCS and a Modbus PLC.

Communication capacity

The following table summarizes the Modbus-specific communication capacity applicable to communication between a Modbus PLC and an SCS.

Table D2.1-1 Capacity of communication between SCS and Modbus PLC

Item	Maximum capacity	Remark
Amount of data that can be communicated per serial communication module	1000 words (1 word = 16 bits)	Limitations of the SCS: Communication I/O data area: 1,000 words per SCS Number of communication data items: 500 data items per SCS
Number of subsystem stations that can be communicated with	30 stations per port	If is recommended that the number of stations be limited to a maximum of four or so, in order to minimize the impact on communications with other normal stations when an error occurs in a communication with a given station.
Size of communication data per communication definition	125 words	One communication definition corresponds to one communication. This limitation applies to one communication using the Modbus protocol.
Number of usable ports	2	Communications are performed independently (in parallel) using two ports.

Simultaneity of communication data

Modbus PLCs assure simultaneity of communication data in units of 16 bits. Accordingly, simultaneity of communication data between a serial communication module and a Modbus PLC is also assured in units of 16 bits.

TIP

Modbus PLCs process data in units of 16 bits. Simultaneity of 32-bit data depends on the application software used on the Modbus PLC side. To assure simultaneity of communication data in units of 32 bits, the application software on the Modbus PLC side needs to set 32-bit data within the same control period.

Transmission specification

The transmission specifications for subsystem communication with a Modbus PLC are as follows:

Table D2.1-2 Transmission specification

Item	Description(*1)	Remark
Interface	RS-232C (D-sub, 9-pin)	ALR111
	RS-422/RS-485 (2-wire, [4-wire])	ALR121(*2)
Transmission method	Half-duplex	
Synchronization method	Start-stop synchronization	
Baud rate	1200, 2400, 4800, 9600, [19200], 38400 bps	
Transmission protocol	Modbus protocol (RTU mode)	
Transmission code	Binary	

Continues on the next page

Table D2.1-2 Transmission specification (Table continued)

Item		Description(*1)	Remark
Data type	Start bit	Fixed to 1	
	Data bit	8	
	Parity bit	None, [Even], Odd	
	Stop bit	1	
Control line	RS control	Yes, [No]	Valid only for ALR111
	DR check	[Yes], No	Valid only for ALR111
	CD check	Yes, [No]	Valid only for ALR111
Time monitoring	Transmission enable monitoring time	1000 ms	
	Reception inter-character timer	0 to 99999 ms [10 ms]	(*2)
	Inter-character monitor timeout	Not handled as errors.	(*2)
Text frame	Reception start character	None	
	EOT character	None	
XON/XOFF control		None	
Response timeout		0 to 99 sec [4 sec]	
Communication retry		0 to 99 [1]	
Interval of connection retries		0 to 999 sec [30 sec]	
Transmission wait time		1 sec	
Option 1		0 to 5	Specification of recovery communication method
Option 2		0 to 1	(*3)
Option 3		0	
Option 4		0	

*1: The recommended settings are shown in [ ].
*2: With Modbus, the reception inter-character timer is used to detect completion of reception. Thus, setting a longer time for the reception inter-character timer will delay the time to reception completion. This timer should be set to around 10 ms (corresponding to the time required for sending 10 characters) at 9600 bps.
*3: Wind-up specification without readback.
0: Valid
1: Invalid

IMPORTANT

When performing subsystem communication with a Modbus PLC, always specify 8 for the data bit length. In addition, always specify 1 for the stop bit length. If any other value is specified, a communication error will occur.

Communication error code

Modbus PLC-specific error codes resulting from address and communication errors are as follows:

Table D2.1-3 Communication error code - Modbus

Error code (hexa-decimal)	Description	Remarks
A3B0	No response	
A3B1	Inappropriate station number (When the station number is other than the range between 1 and 255)	(*1)
A3B2	Station number 0 cannot be set	(*1)
A3B3	Inappropriate address name	(*1)
A3B4	Inappropriate address number	(*1)
A3B5	Too many communication processing points	(*1)
A3B6	Write to a read-only device occurred	(*1)
A3B8	Odd number is used for the size of 4-byte register	(*1)
A3B9	Option 1 setting is out of range	(*1)
A3BA	Cannot create communication frame	(*1)
A3C0	CRC-16 error	(*2)
A3C1	Response message error (Station error)	(*2)
A3C2	Response message error (Address error)	(*2)
A3C3	Response message error (Function code error)	(*2)
A3C4	Response message error (Data error)	(*2)
A3C5	Response message error (Received data size error)	(*2)
A3C6	Response message error (Received data length error)	(*2)
A3D1	Error code $01 received	(*2)
A3D2	Error code $02 received	(*2)
A3D3	Error code $03 received	(*2)
A3D4	Error code $04 received	(*2)
A3D5	Error code $05 received	(*2)
A3D6	Error code $06 received	(*2)
A3D7	Error code $07 received	(*2)
A3D8	Error code $08 received	(*2)
A3D9	Error code $09 received	(*2)
A3DA	Error code $0A received	(*2)
A3DB	Error code $0B received	(*2)
A3DC	Error code $0C received	(*2)
A3DD	Error code $0D received	(*2)
A3DE	Error code $0E received	(*2)
A3DF	Error code $0F received	(*2)
A3E0	Error code $10 received	(*2)
A3E1	Error code $11 received	(*2)
A3E2	Error code $12 received	(*2)
A3E3	Error code $13 received	(*2)
A3E4	Error code $14 received	(*2)
A3E5	Error code $15 received	(*2)
A3E6	Error code $16 received	(*2)

Continues on the next page

Table D2.1-3 Communication error code - Modbus (Table continued)

Error code (hexa-decimal)	Description	Remarks
A3E7	Error code $17 received	(*2)
A3E8	Error code $18 received	(*2)

*1: Definition error for ALR111/ALR121. If this error occurs, no communication can be performed to the Modbus PLC.
*2: This is an error when an error message was received from the Modbus PLC.

ALR111 RS-232C serial communication module

This section describes the LED indications, connector pin layout and cable connection of the ALR111 RS-232C serial communication module.

LED indications in the ALR111 RS-232C serial communication module

Table D2.1-4 ALR111 LED indications

LED	Description
STATUS	Hardware ready
ACT	Operating normally
DX	Dual-redundant configuration
SND1, SND2	Sending data from RS port 1 or 2
RCV1, RCV2	Receiving data by RS port 1 or 2

Terminal assignments for the ALR111 RS-232C serial communication module

Table D2.1-5 RS-232C D-sub 9-pin connector specification

Pin No.	Signal	Name	Processing on ALR111 side
1	CD	Carrier Detect	Send data if the CD is OFF (only when CD check is performed). Receive data if the CD is ON.
2	RD	Receive Data	
3	SD	Send Data	
4	ER	Data Terminal Ready	Output "ON" if normal.
5	SG	Signal Ground	
6	DR	Data Set Ready	Send data if the DR is ON (only when DR check is performed).
7	RS	Request to Send	This signal is always ON if RS control is not performed. If RS control is performed, the ALR111 outputs "ON" when sending data.
8	CS	Clear to Send	Send data if the CS is ON.
9	-	Not used	

ALR121 RS-422/RS-485 serial communication module

The following describes the LED indications, connector pin layout and cable connection for the ALR121 RS-422/RS-485 serial communication module.

LED indications in the ALR121 RS-422/RS-485 serial communication module

Table D2.1-6 ALR121 LED indications

LED	Description
STATUS	Hardware ready
ACT	Operating normally
DX	Dual-redundant configuration
SND1, SND2	Sending data from RS port 1 or 2
RCV1, RCV2	Receiving data by RS port 1 or 2

Terminal assignments of the ALR121 RS-422/RS-485 serial communication module

Table D2.1-7 ALR121 connector specifications

Terminal	Name
TX+	Send Data (Positive phase signal)
TX-	Send Data (Negative phase signal)
RX+	Receive Data (Positive phase signal)
RX-	Receive Data (Negative phase signal)
SG	Signal Ground

Cables provided by Yokogawa Electric Corporation

Yokogawa Electric Corporation provides the following four types of cables for connecting a serial communication module to a subsystem.

RS-232C modem cables

These cables are used to connect an ALR111 with a modem.

- AKB131: RS-232C modem cable (9-25 pins) for RS circuit isolated device (for ALR111 to modem connection)
- AKB135: RS-232C modem cable (9-25 pins) (for ALR111 to modem connection)

RS-232C null modem cables

These cables are used to connect an ALR111 with a subsystem.

- AKB132: RS-232C null modem cable (9-25 pins) for RS circuit isolated device (for ALR111 to RS-232C device connection)
- AKB133: RS-232C null modem cable (9-9 pins, male) (for ALR111 to FA-M3 connection)
- AKB134: RS-232C null modem cable (9-9 pins, female) (for ALR111 to RS-232C device connection)
- AKB136: RS-232C null modem cable (9-25 pins) (for ALR111 to RS-232C device connection)

RS-232C cable

This cable is used to connect an ALR111 with a subsystem.

- AKB163: RS-232C cable (for ALR111 to FA500 connection)

RS-422/RS-485 cable

This cable is used to connect an ALR121 with a subsystem.

- AKB164: RS-422/RS-485 cable (for ALR121 to FA-M3 connection)

D2.2 Connection of serial communication module and Modbus PLC

This section describes how to connect a serial communication module with a Modbus PLC using a cable.

Connecting an ALR111 RS-232C serial communication module with a Modbus PLC

The ALR111 uses a RS-232C D-sub, 9-pin connector, but the computer link unit of the connected Modbus PLC may be equipped with a RS-232C D-sub, 25-pin connector or a 9-pin connector. Select a connection cable appropriate for the subsystem to be connected.

A modem is required for connecting an ALR111 with a Modbus PLC. As long as the ALR111 and Modbus PLC are sharing the same grounding system, the two can be connected directly using a RS-232C cable of a length not exceeding 15 m.

IMPORTANT

The length of the RC-232C cable connecting the ALR111 to the modem, and one connecting the modem to the Modbus PLC, shall not exceed 15 m.

Modem connection

The following figure shows a cable connection when an ALR111 and a Modbus PLC are connected via a modem.

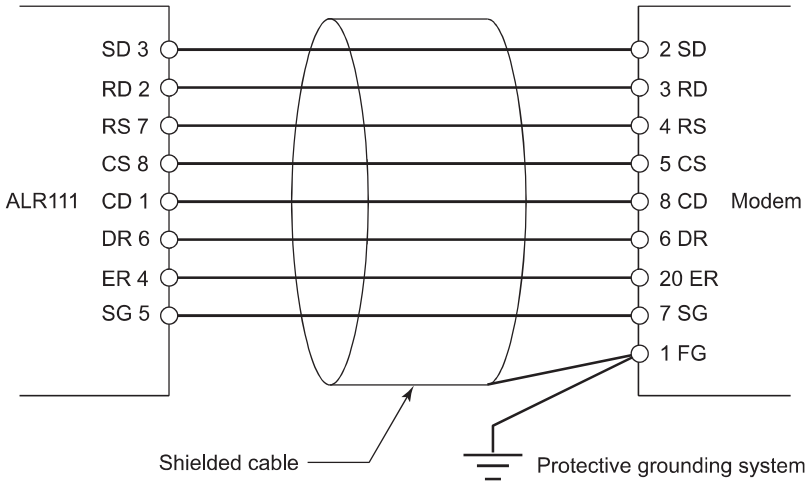


Figure D2.2-1 Cable connection of ALR111 and Modbus PLC via modem (RS-232C D-sub, 25-pin)

Connecting a RS-232C D-sub, 25-pin connector to a Modbus PLC (direct connection)

The following example shows a cable connection where an ALR111 is connected directly to a Modbus PLC equipped with an RS-232C D-sub 25-pin connector. In this connection, a cable with an RS-232C D-sub, 25-pin connector needs to be used.

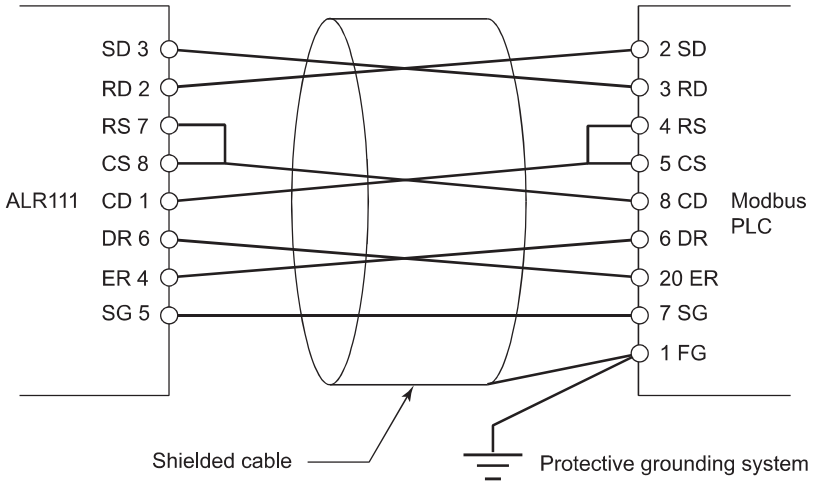


Figure D2.2-2 Direct cable connection of ALR111 and Modbus PLC (RS-232C D-sub, 25-pin)

Connecting a RS-232C D-sub, 9-pin connector to a Modbus PLC (direct connection)

The following example shows a cable connection where an ALR111 is connected directly to a Modbus PLC equipped with an RS-232C D-sub 9-pin connector. In this connection, a cable with an RS-232C D-sub, 9-pin connector needs to be used.

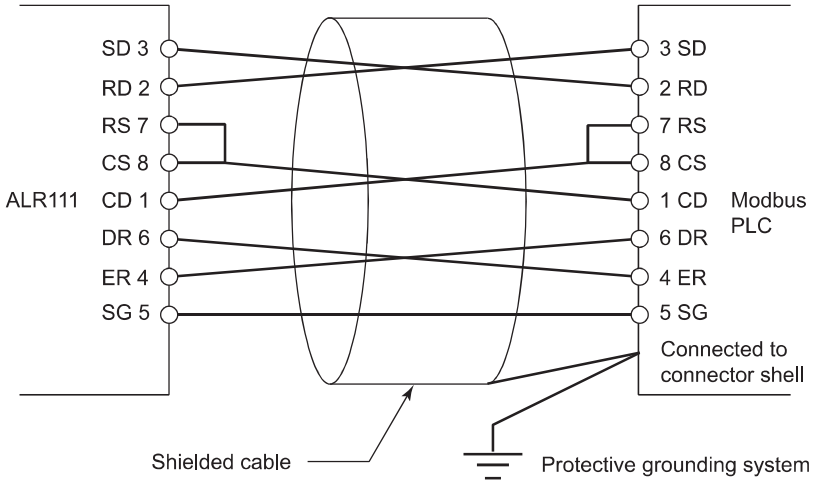


Figure D2.2-3 Direct cable connection of ALR111 and Modbus PLC (RS-232C D-sub, 9-pin)

SEE ALSO For more information about connecting the ALR111 (RS-232C) to each Modbus PLC model, refer to:

Modbus PLC user manuals

Connecting an ALR121 RS-422/RS-485 serial communication module with a Modbus PLC

The specific connection varies depending on the Modbus PLC model.

SEE ALSO For more information about connecting the ALR121 (RS-422/RS-485) to each Modbus PLC model, refer to:

Modbus PLC user manuals

D2.3 Modbus PLC devices accessible from SCSs

This section describes the Modbus PLC devices that can be accessed from SCSs.

Internal data of a Modbus PLC are called devices. Devices can be bit devices or word devices, as described in the following explanation.

- Bit devices
  Data in which each bit has a meaning. An input relay is a bit device.
- Word devices
  Data in which each word (1 word = 16 bits) has a meaning. A holding register is a word device.

Modbus PLCs also have devices called "special coil" and "communication status."

Accessible devices

To access Modbus PLC devices, you must set [Comm Device & Address] of Signal Definition and [Size] of Communication Definition in the Safety Communication I/O Editor, or set [Device Address] and [Size] in the Communication I/O Builder.

With Modbus PLCs, "Device Address" is set using the following format:

<Function code> + <Device type> + <Address within device>

To specify input relays 100012 to 100015, for example, set A100012 for "Device Address" and 1 for "Size." "A" of A100012 indicates a function code, "1" indicates a device type, and "00012" indicates an address within device.

The table below lists the Modbus PLC devices accessible from SCSs, as well as the corresponding addresses and Modbus protocol function codes.

Table D2.3-1 Bit devices

Device	Address			Modbus protocol function code (hexadecimal)	
	Function code	Modbus PLC device type	Address in the Modbus PLC device	Read	Write
Coil	A	0	XXXX	01	0F
	B				05
	X			-	0F
	Y				05
Input relay	A	1	XXXX	02	-
Link relay:(*1)	A	D	XXXX	12	1D
	B				19
	X			-	1D
	Y				19
Step status:(*1)	A	S	XXXX	17	-

*1: These are Memocon-SC GL60S devices and not available on other models.

Table D2.3-2 Word devices

Device	Address			Modbus protocol function code (hexadecimal)	
	Function code	Modbus PLC device type	Address in the Modbus PLC device	Read	Write
Input register	A	3	XXXX	04	-
Holding register	A	4	XXXX	03	10
	B				06
	C				10
	X			-	10
	Y				06
	Z				10
Constant register: (*1)	A	C	XXXX	13	1E
	B				1A
	C				1E
	X			-	1E
	Y				1A
	Z				1E
Elapsed step time:(*1)	A	5	XXXX	14	-
Link register:(*1)	A	R	XXXX	15	1F
	B				1B
	C				1F
	X			-	1F
	Y				1B
	Z				1F
Extended register: (*1)	A	A	XXXX	16	20
	B				1C
	C				20
	X			-	20
	Y				1C
	Z				20
4-byte register	A	W	XXXX	04	-

*1: These are Memocon-SC GL60S devices and not available on other models.

Table D2.3-3 Other devices

Device	Address			Modbus protocol function code (hexadecimal)	
	Function code	Modbus PLC device type	Address in the Modbus PLC device	Read	Write
Special coil	SP001			07	-
Communication status	STSXXX			-	-

The meaning of each function code is as follows. The size is specified in the Safety Communication I/O Editor or Communication I/O Builder.

- A
  Read data for the specified size.

  Write data for the specified size specified. Readback is supported.
- B
  Read data for the specified size.

  Write data individually to each modified device in units of 1 bit for a bit device, or in units of 16 bits for a word device. With readback.
- C
  Read data for the specified size.

  Write data individually to each modified device in units of 32 bits. With readback.
- X
  Write data for the specified size when a change occurs. Readback is not supported.
- Y
  Write data individually only to each modified device for the size of each device when a change occurs. Without readback.
- Z
  Write data individually only to each modified device in units of 32 bits when a change occurs. Without readback.

Table D2.3-4 List of function codes

Function code	Device	Read	Write	Readback
A	Bit device	All data for one communication definition	All data for one communication definition	Yes
	Word device	All data for one communication definition	All data for one communication definition	Yes
B	Bit device	All data for one communication definition	In units of 1 bit	Yes
	Word device	All data for one communication definition	In units of 16 bits	Yes
C	Word device	All data for one communication definition	In units of 32 bits	Yes
X	Bit device	-	All data for one communication definition	No
	Word device	-	All data for one communication definition	No
Y	Bit device	-	In units of 1 bit	No
	Word device	-	In units of 16 bits	No
Z	Word device	-	In units of 32 bits	No

IMPORTANT

With a dual-redundant configuration based on ALR111/ALR121s, it is always necessary to perform readback when data is written to the Modbus PLC. Writing of data without readback is not supported in a dual-redundant configuration.

Supported function codes, accessible devices, and sizes vary depending on the Modbus PLC model.

SEE ALSO

For more information about readback communication, refer to:

D2.5, “Readback communication” on page D2-20

For more information about supported function codes, accessible devices, sizes, and so on, refer to:

The user manual for your Modbus PLC

D2.4 Builder setting items specific to Modbus PLCs

This section describes the builder setting items specific to Modbus PLCs.

When performing RS original engineering, you can define the serial communication module and set I/O parameters by using I/O Wiring View and I/O Parameter Builder. In addition, you need to use Communication I/O Builder to allocate the communication I/O data, and assign element numbers and subsystem communication I/O FB.

When performing I/O list engineering, you can define the serial communication module and set I/O parameters by using IOM Definition Editor. In addition, you need to use Safety Communication I/O Editor to allocate the communication I/O data, and assign element numbers and subsystem communication I/O FB.

TIP

This section mainly describes for the case when performing RS original engineering. The setting item names displayed may differ between I/O list engineering and RS original engineering, but the settings are the same.

SEE ALSO

For more information about engineering of subsystem communication modules using Safety Communication I/O Editor, refer to:

D1.5, “Engineering for subsystem communication modules” on page D1-37

For more information about I/O list engineering, refer to:

D., “Procedures to create applications using the I/O list engineering method” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

D2.4.1 Settings in the I/O Wiring View

When performing RS original engineering, you need to set the following items by using the I/O Wiring View.

Subsystem communication module definition

If an ALR111/ALR121 is used for subsystem communication, you need to select ALR111M or ALR121M as the module type. You need to specify the mounting position (node, slot number) of the module, as well as whether or not to use a dual-redundant configuration.

Dual-redundancy of serial communication modules

To use serial communication modules in a dual-redundant configuration, you need to set Is-Redundant to TRUE.

D2.4.2 Items set in the I/O Parameter Builder

When performing RS original engineering, you need to set the following items in ALR111M/ ALR121M by using the I/O Parameter Builder.

■ Connection device

For the name of the connected device, select [S_MODBUS].

■ Transmission specifications

Set the transmission specifications for each port.

SEE ALSO For more information about settings information, refer to:

"■ Transmission specification" on page D2-2

■ Options 1 and 2

In Option 1, specify the method of recovery communication. In Option 2, specify the wind-up action for communication without readback.

SEE ALSO For more information about procedure for specifying recovery communication operations in Option 1, refer to:

D2.6, "Recovery communication" on page D2-25

For more information about procedure for specifying wind-up operations in Option 2, refer to:

"■ Operation in communication without readback" on page D2-21

D2.4.3 Items set in the Communication I/O Builder

This section describes the items set in the Communication I/O Builder.

This section describes the following items when a Modbus PLC is used.

- Element
- Buffer
- Program Name
- Size
- Port
- Station
- Device Address
- Data Type
- Reverse
- Input Processing at Fault
- Input Value at Fault

Element

Element numbers are displayed to specify the buffer addresses in the communication I/O data area. The "Element" field is read only and cannot be set.

Buffer

Specify the size of the storage area to be used by the Modbus communication program.
The "Buffer" is a required setting item in the Communication I/O Builder and always needs to be set.

Program name

Set the program name using the node number, slot number and S_MODBUS, as follows:
Program Name : n-s Fixed character string

- n: Node number
- s: Slot number
- Fixed character string: S_MODBUS

Size

Set the assigned size (data length) from the beginning address set in "Device Address."
The "Size" is a required setting item in the Communication I/O Builder and always needs to be set.

Specify the size in units of words (16 bits). The setting range is 1 to 125 words.

Port

Set the port of the ALR111/ALR121 to be used.
Port 1 or 2 can be set.

Station

Set the station number for the Modbus PLC.
The setting range is 1 to 255.

Device address

Set the content of data to be acquired from the other device as a combination of the communication method used by the Modbus PLC and the beginning address of the data.
The address can be set using 3 to 7 alphanumeric characters as follows:

- Coil: A0xxxx, B0xxxx, X0xxxx, Y0xxxx
- Input relay: A1xxxx
- Link relay: ADxxxx, BDxxxx, XDxxxx, YDxxxx
- Step status: ASxxxx
- Input register: A3xxxx
- Holding register: A4xxxx, B4xxxx, C4xxxx, X4xxxx, Y4xxxx, Z4xxxx
- Constant register: ACxxxx, BCxxxx, CCxxxx, XCxxxx, YCxxxx, ZCxxxx
- Elapsed step time: A5xxxx
- Link register: ARxxxx, BRxxxx, CRxxxx, XRxxxx, YRxxxx, ZRxxxx
- Extended register: AAxxxx, BAxxxx, CAxxxx, XAxxxx, YAxxxx, ZAxxxx
- 4-byte register: AWxxxx
- Special coil: SP001
- Communication status: STSxxx

The "Device Address" field is blank by default.

"xxxx" indicates an address within Modbus PLC device, and is set as a decimal or hexadecimal value between 1 and 65535 (1H and FFFFH). If a hexadecimal value is used, add "H" at the end.

The 0 or 0s at the beginning of "xxxx" can be omitted. For example, coil addresses of A023, A0023 and A00023 all represent the same address.

SEE ALSO For more information about specifying addresses , refer to:

D2.3, “Modbus PLC devices accessible from SCSs” on page D2-10

Limitations on dual-redundant serial communication modules

If even one function code without readback (X, Y or Z) is specified in the "Device Address" fields of the Communication I/O Builder, that serial communication module cannot be used in a dual-redundant configuration. Dual redundancy is not supported if readback is not used. To provide a dual-redundant configuration using two serial communication modules, specify only function codes with readback (A, B and C) for the modules.

TIP

If a function code without readback is specified in a dual-redundant configuration, the following problems will occur:

- Outputs that occurred while switching the dual-redundant modules may not be output, or the same outputs may be output again after switching.
  With readback, data is read from the subsystem, compared with the data in the CPU, and then the CPU data is written to the subsystem if the two data are different.

  Without readback, the data in the CPU is compared with the data in the serial communication module on the control side, without reading data from the subsystem, after which the CPU data is written to the subsystem and the data in the module is refreshed only when there is a difference between the data. If the serial communication module on the control side is normal, the data in the serial communication module on the standby side is not refreshed. This means that the serial communication module on the standby side will still contain old data when the control switches from the module on the control side to the module on the standby side. Since the module in this condition cannot accurately compare the data in the CPU with the data in the module, data cannot be written in this mode without readback.

  In Modbus communication, whether or not readback is used is determined by an address function code specified in the Communication I/O Builder.

- If an address without readback is specified, the control will not be switched to the applicable serial communication module in the dual-redundant configuration for 70 seconds after recovery of the module from an error.
  If the serial communication module on the standby side is reset following a restart, the serial communication status will not be considered normal for 70 seconds. If a serial communication error occurs during this period in the serial communication module on the control side, the control will not switch to the module on the control side.

SEE ALSO

For more information about readback, refer to:

D2.5, “Readback communication” on page D2-20

Data type

Set the type of subsystem data.
If 32-bit data is used, simultaneity of communication data needs to be considered.

Reverse

Set whether or not to reverse the order of bits/words in the SCS from the order of bits/words in the subsystem.

SEE ALSO

For more information about storing subsystem data on an SCS, refer to:

D1.6, “Storage formats of subsystem data” on page D1-42

Input processing at fault

Specify the value to be input to the application logic, instead of the input from the subsystem, upon detection of a communication error.

Input value at fault

Specify the input value to be used, instead of the process value, when "Fixed Value" is specified in "Input Processing at Fault."

D2.5 Readback communication

In subsystem communication, output data from subsystems are always read (read back) even when their data type is output, and each read-back data is compared with the data to be written. If a difference is found as a result of comparison, the data will be written. This method is indicated by the phrase "with readback." Readback forms the basis of subsystem communication.

On the other hand, there is another method of subsystem communication in which subsystem outputs are not read back and data is written only when the previously written data is different from the data to be written. This method is indicated by the phrase "without readback." This method is used to support one-shot outputs from Modbus PLCs.

Operation in communication with readback

Values output from subsystems are read at the subsystem communication period. The read-back data is compared with the data to be written. If there are no differences, write communication is not sent ((1) and (3) in the following figure).

If an output value is changed in the CPU and a difference occurs between the read-back data and the data to be written, communication is established with the applicable subsystem to write the new data ((2) in the following figure).

If an output value in a subsystem is changed while communication is normal, a difference occurs between the read-back data and the data to be written, in which case communication is established with the subsystem to write the new data ((4) in the following figure).

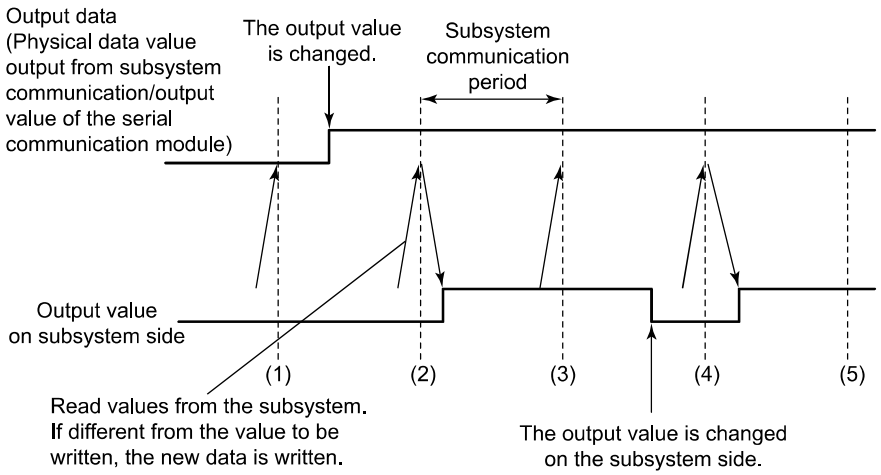


Figure D2.5-1 Output communication with readback

In a dual-redundant configuration, the serial communication module on the standby side reads back output values to confirm integrity of communication paths and prevent omission of outputs when the control right is switched.

In the following conditions, if read-back is enabled, values from subsystems are output from the serial communication module.

- While output from the communication module is disabled following an initial cold start of the SCS
- While the subsystem communication output data is locked.
  By locking the communication outputs before an online change, the outputs statuses on the subsystem side can be retained even after restarting the communication module.

Recovery from a serial communication module error

If the serial communication module has recovered from an error in a communication with readback, the output values on the subsystem side are tracked. The following figure illustrates the operations when communication output is locked.

If the serial communication module has generated an error, data from subsystems cannot be read back. Thus, the SCS retains the previous output values and does not output data ((1) and (2) in the following figure).

Once the serial communication module recovers and communication is enabled for the first time, data from subsystems are read back and subsystem output values are tracked ((3) in the following figure).

Following this, if an output value on the SCS side is changed, a difference occurs between the readback data and the data to be written. In this case, communication is established with the applicable subsystem to write the new data ((5) in the following figure).

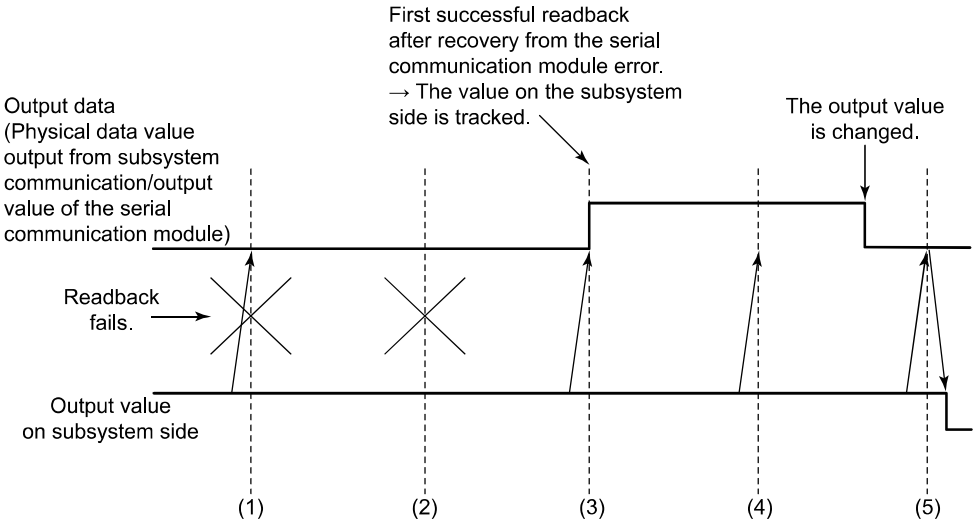


Figure D2.5-2 Operation in communication with readback after recovery from serial communication module error

Operation in communication without readback

Communication without readback is used to perform one-shot write to the Modbus PLC.

If the Modbus PLC is to accept outputs to the coils (discrete outputs) on the master side as commands to subsystems, it is necessary to perform one-shot write.

If the output to a coil is changed from OFF to ON on the master side, the Modbus PLC accepts the command and resets the corresponding output value (OFF → ON → OFF). At this time if readback is enabled, the output value will be read back from the Modbus PLC, in which case the Modbus PLC's value will be compared with the value to be written. If a difference is detected, communication will be established to write the new data again. If it is necessary to perform one-shot write, disable readback.

Without readback, output values are not read back.

The serial communication module checks the output values on the CPU side at the subsystem communication period, and does not perform communication to write data if the previous output values have not changed ((1), (3), (4) and (5) in the following figure).

Data is written only when a change is detected in any output value on the CPU side ((2) in the following figure).

Since readback communication is not performed, communication to write data is not performed, even after an output value has been changed on the Modbus PLC side ((4) in the following figure).

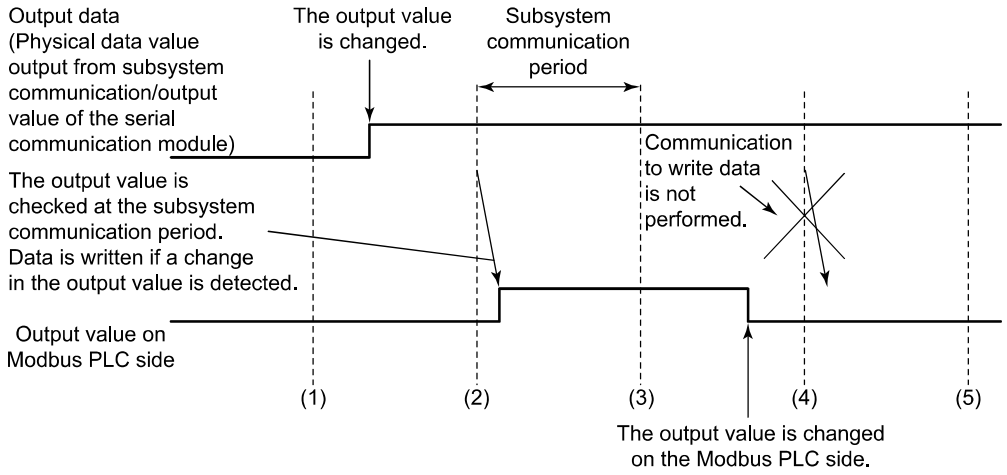


Figure D2.5-3 Output communication without readback

Settings of Option 2 (wind-up function)

The wind-up function is enabled only when a function code without readback is specified in "Device Address" in the Communication I/O Builder. Without readback, output starts when an output value has been changed on the master side. Thus, the wind-up function disables all changes to output values for 70 seconds following a reset of the serial communication module, in order to prevent unnecessary write accesses after the reset. Enable/disable this function by setting Option 2, which is an I/O parameter for Port 1 or Port 2.

- When Option 2 is set to 0
  The wind-up function is enabled.

  If the serial communication module is reset, changes to output values will not be written to the Modbus PLC for 70 seconds following the reset. Changes to output values will be written to the Modbus PLC only after elapse of 70 seconds following the reset.

- When Option 2 is set to 1
  The wind-up function is disabled. (Wind-up disable)

SEE ALSO For more information about function codes specified in [Device Address], refer to:

D2.3, “Modbus PLC devices accessible from SCSs” on page D2-10

Recovery from a serial communication module error (wind-up function enabled)

After the serial communication module recovers from an error, output values will be initialized at 0 ((1) in the following figure).

If I/O parameter "Option 2" is set to 0, changes in output values will not be written to the Modbus PLC for 70 seconds after the recovery ((3) in the following figure). Thus, discrepancies will occur between the output values on the SCS side and those on the subsystem side immediately after the reset of the serial communication module, until the output values are changed on the subsystem side.

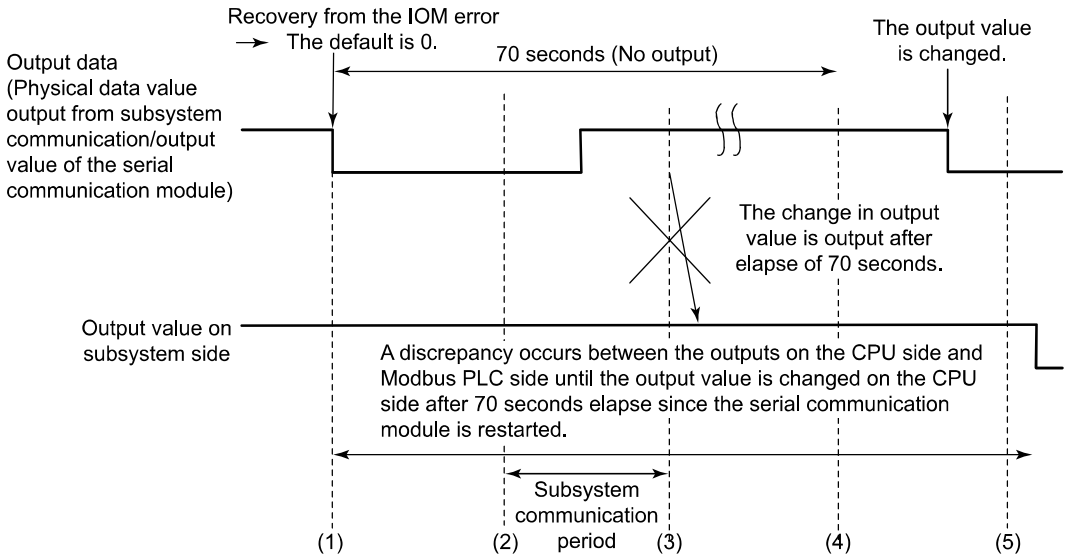


Figure D2.5-4 Operation in communication without readback after recovery from serial communication module error

With readback, output values are read back, so the differences between read-back values and values to be written are detected and the new data are written even when the output values have not been written to subsystems. Without readback, however, data will not be written unless output values on the SCS side are changed. For this reason, the statuses of output values on the SCS side may remain different from those on the Modbus PLC side after output values have been changed on the Modbus PLC or the serial communication module has been reset.

Error handling actions in communication without readback

The error handling actions in communication without readback are as follows:

- Initial cold start of the CPU (Output disabled)
  When output is disabled, the defaults of physical communication output data are 0. Output is not performed until any output value is changed on the CPU side. Once output is enabled, output will be performed when any output value is changed to a value other than 0 on the CPU side. The output timing varies depending on the setting of the wind-up function.
- Occurrence of a serial communication module error while subsystem communication data is locked
  When an error of serial communication module occurs or online change that may reset the serial communication module is performed, if any output value is changed to a value other than 0, output acts just like after an initial cold start of the CPU. The output timing varies depending on the setting of the wind-up function.

Status in communication without readback

Without readback, whether the status of communication data becomes BAD upon a serial communication error is determined by the following conditions:

- Whether there is any data to read from the station to communicate with
- The recovery communication specification that is set as I/O parameter "Option 1"

Table D2.5-1 When communication data that defined without readback becomes BAD upon serial communication error

Option 1 setting(*1)		If there is no readback for all the communication definitions for one station	If at least one communication definition for the station has readback
0	Perform recovery communication using a 08 command (loopback check command)	The status will change to BAD if a communication error occurs during a communication to write data. (If "Option 1" is set to 2, the status will automatically return to normal when recovery communication is performed.)	The status will change to BAD if a communication error occurs during a communication to write data. The status will also change to BAD if a communication error occurs in which abnormal line communication is recognized (no response, line NRDY, etc.) during a communication based on a definition with readback (input definition, or output definition with readback).
1	Perform recovery communication using a READ command		
2	Reset the error condition when recovery communication is performed		
3	Perform recovery communication using a WRITE command of 0 write size		
4	Perform recovery communication using a WRITE command based on the data written immediately before the error		
5	Do not recognize an error nor perform recovery communication	Always normal	

*1: Applicable only to the recovery communication methods without readback. With readback, recovery communication is performed using a READ command.

TIP

In addition to the previously listed conditions, the status will also change to BAD in the following cases:

- Occurrence of a serial communication module error or error in the path from the CPU to the serial communication module
- Occurrence of a range error of station number setting, range error of address setting or other definition error
- With readback, if a serial communication error occurs, the status of communication data becomes BAD at readback that is performed at every subsystem communication period.

D2.6 Recovery communication

If no response is received or a CRC-16 code error occurs during communication with a Modbus PLC, communication with the applicable station is temporarily suspended. Thereafter, communication is performed at the interval of connection retries that is set in an I/O parameter to check if the Modbus PLC that generated an error has recovered to normal state. This communication is called "recovery communication."

This section explains recovery communication.

Types and details of recovery communication

The recovery communication method is determined by the setting of I/O parameter "Option."

Option 1 (Recovery communication specification)

Recovery communication can be performed using the following five methods:

- When Option 1 is set to 0
  With readback, recovery communication is performed using a READ command.

  Without readback, recovery communication is performed using a 08 command. The 08 command is a loopback check command used to check presence of the subsystem.
- When Option 1 is set to 1
  Recovery communication is performed using a READ command regardless of the readback setting.
- When Option 1 is set to 2
  With readback, recovery communication is performed using a READ command.

  Without readback, the error condition will be reset when recovery communication is performed. If the same station generates an error again during recovery communication, a system alarm will generate every time recovery communication is performed.
- When Option 1 is set to 3
  With readback, recovery communication is performed using a READ command.

  Without readback, recovery communication is performed using a WRITE command of 0 write size.
- When Option 1 is set to 4
  With readback, recovery communication is performed using a READ command.

  Without readback, recovery communication is performed using a WRITE command based on the data written immediately before the error.
- When Option 1 is set to 5
  With readback, recovery communication is performed using a READ command.

  Without readback, any station that generated an error is not recognized as an error station. When Option 1 is set to 5, communication with the non-responding Modbus PLC will stop for the period corresponding to "No response time x (1 + Number of retries)" after each interval of connection retries set in the communication module definition.

IMPORTANT

- When Option 1 is set to 4, recovery communication is performed using the data written immediately before the error. Exercise caution since duplicate operation commands may occur if the data written immediately before the error contained an operation command to the Modbus PLC.
- On some Modbus PLC models, reading with a READ command may reset the flag. If you don't want to cause the discrepancy, specify a function code without readback in "Device Address" of the communication definitions on Communication I/O Builder.

The 08 command cannot be used for some types of Modbus PLC models.

SEE ALSO For more information about Modbus PLC, refer to:

Modbus PLC user manuals

D2.7 Communication text

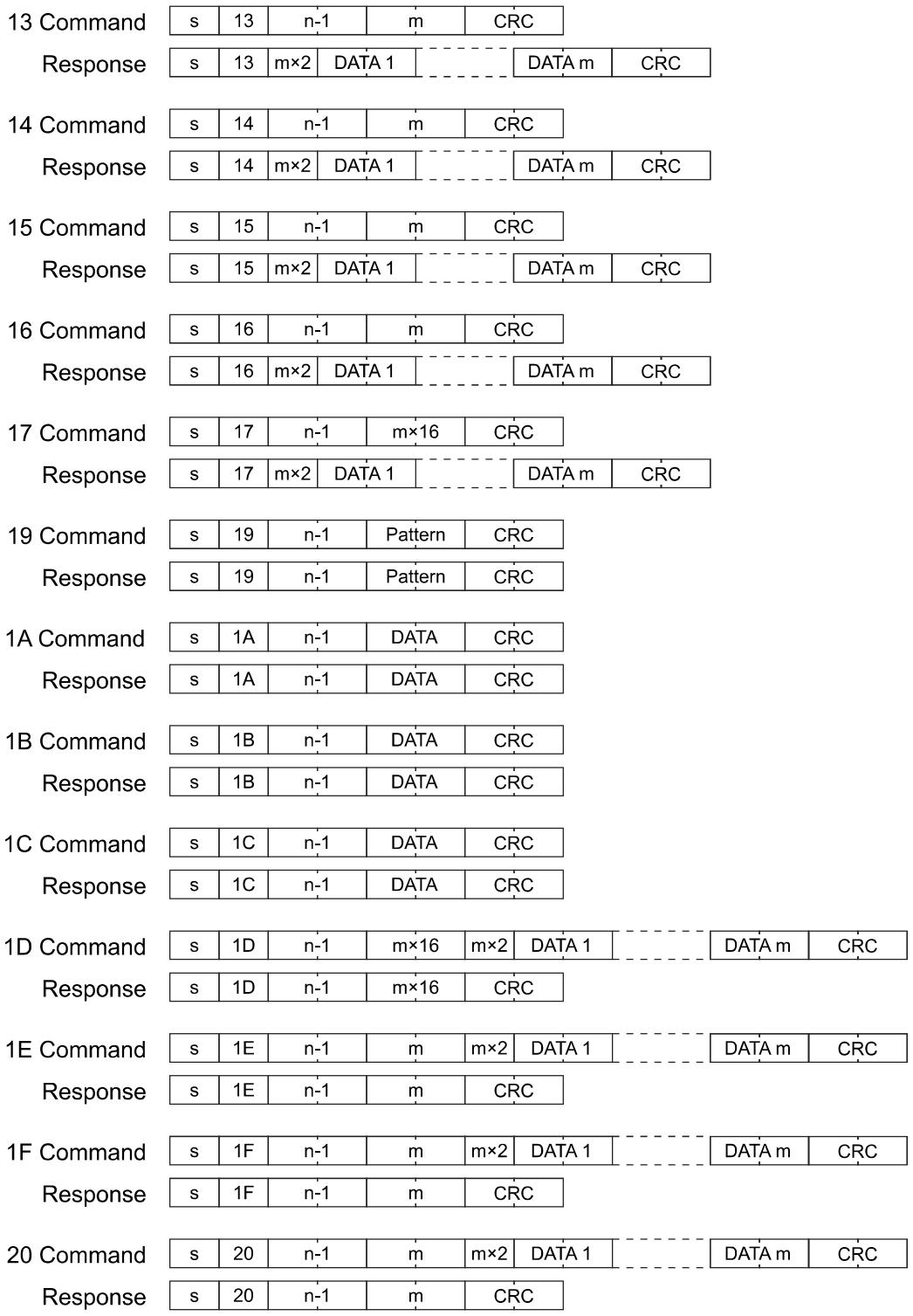
This section describes the communication text used in the Modbus protocol.

The communication text contains frames for each command in the Modbus protocol and a response to the command. The structures of communication text frames are as follows:

01 Command	s	01	n-1	m×16	CRC				
Response	s	01	m×2	DATA 1				DATA m	CRC
02 Command	s	02	n-1	m×16	CRC				
Response	s	02	m×2	DATA 1				DATA m	CRC
03 Command	s	03	n-1	m	CRC				
Response	s	03	m×2	DATA 1				DATA m	CRC
04 Command	s	04	n-1	m	CRC				
Response	s	04	m×2	DATA 1				DATA m	CRC
05 Command	s	05	n-1	Pattern	CRC				
Response	s	05	n-1	Pattern	CRC				
06 Command	s	06	n-1	DATA	CRC				
Response	s	06	n-1	DATA	CRC				
07 Command	s	07	CRC						
Response	s	07	DT	CRC					
08 Command	s	08	code	DATA	CRC				
Response	s	08	code	DATA	CRC				
0F Command	s	0F	n-1	m×16	m×2	DATA 1		DATA m	CRC
Response	s	0F	n-1	m×16	CRC				
10 Command	s	10	n-1	m	m×2	DATA 1		DATA m	CRC
Response	s	10	n-1	m	CRC				
11 Command	s	11	n-1	m	CRC				
Response	s	11	CRC						
12 Command	s	12	n-1	m×16	CRC				
Response	s	12	m×2	DATA 1				DATA m	CRC

s: Station number
n: Relative value from the beginning of the address within device
With holding register 40050, for example, n becomes 49 (40050 - 40001 = 49).
m: Assigned size set in the Communication I/O Builder (in words)
Pattern: “0xFF00” if ON, or “0x0000” if OFF

Figure D2.7-1 Communication text frame structures (1/2)

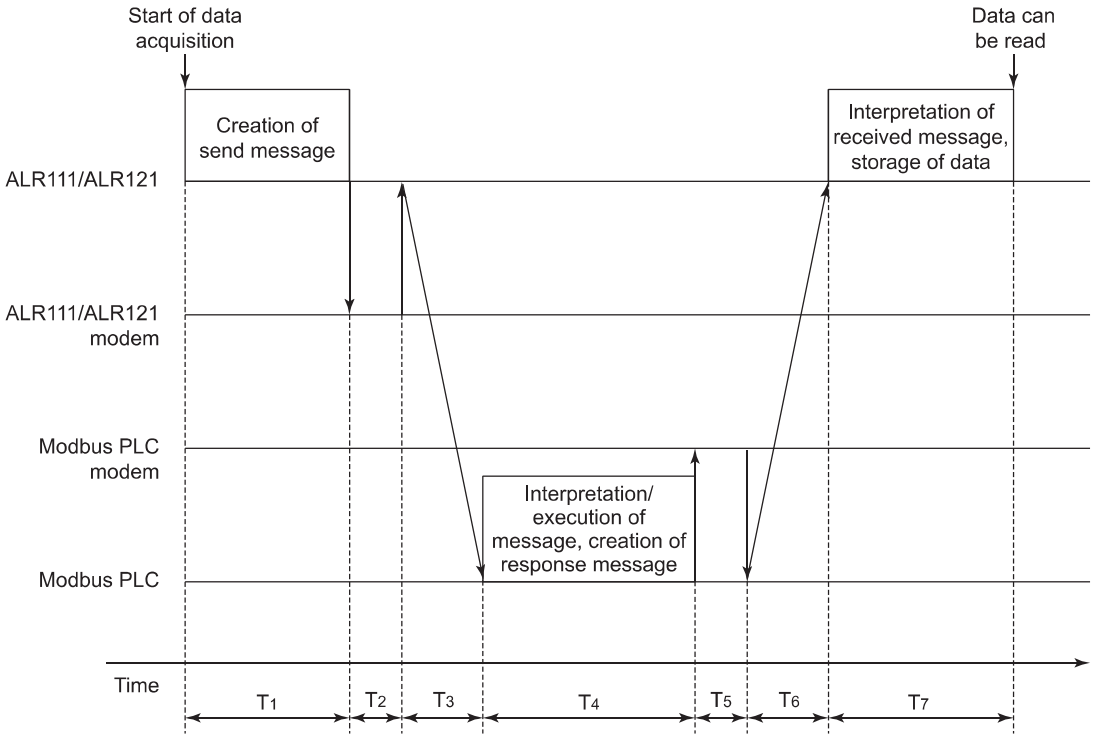


s: Station number
n: Relative value from the beginning of the address within device
With holding register 40050, for example, n becomes 49 (40050 - 40001 = 49).
m: Assigned size set in the Communication I/O Builder (in words)
Pattern: “0xFF00” if ON, or “0x0000” if OFF

Figure D2.7-2 Communication text frame structures (2/2)

D2.8 Communication time between serial communication module and Modbus PLC

The communication time between a serial communication module and a Modbus PLC is calculated as the total sum of T1 through T7 as follows.



T1: Time for creating a send message: Approx. 10 ms
T2: Delay time of the ALR111/ALR121 modem: Approx. 5 ms
T3: Time for transmitting the send message.
T4: Processing time in the Modbus PLC. Time for interpreting/executing the received message and creating a response message. Determined by the number of communication data items and number of scans performed by the Modbus PLC.
T5: Delay time of the Modbus PLC modem: Approx. 5 ms
T6: Time for transmitting the response message.
T7: Time for interpreting the response message: Approx. 15 ms

Figure D2.8-1 Timing chart for communication between a serial communication module and a Modbus PLC

TIP

Since each port performs communication independently, the sum of times required for all communication definitions set for each port becomes the data update time of the port. For example, if definitions 1 and 2 are set for port 1,
the communication period of port 1 is calculated as "(communication time for definition 1) + (communication time for definition 2)".

The following shows how to calculate the communication time.

The transmission time for sending (T3) and receiving (T6) can be calculated by using the following formulas:

$$T3 \text{ or } T6 = \frac{1000 \times \text{Number of characters} \times \text{Number of bits per one character}}{\text{Baud rate}} \text{ (ms)}$$

Number of bits per one character = Number of start bits (1) + Number of data bits (8)
+ Number of parity bits (1)
+ Number of stop bits (1)

Start bit: Fixed at 1 bit
Data bits: Fixed at 8 bits (7 bits cannot be specified)
Parity bit: Set 1 if parity is even or odd, set 0 if parity is none
Stop bit: Fixed at 1 bit
Baud rate: 1200, 2400, 4800, 9600, 19200, 38400 bps

The following table shows the character length of each device that can be transmitted by Modbus communication.

Table D2.8-1 Number of characters transmitted

Device	Read		Write	
	Send	Response	Send	Response
Coil	Fixed to 8	5 + Number of coils/8 (*1)	9 + Number of coils/4 (*1)	Fixed to 8
Holding register	Fixed to 8	5 + 2 x Number of registers	9 + 2 x Number of registers	Fixed to 8
Input relay	Fixed to 8	5 + Number of relays / 8 (*1)	-	-
Input register	Fixed to 8	5 + 2 x Number of registers	-	-

*1: Fractions after the decimal point are rounded up.

D2.9 Precautions for engineering

The subsystem communication function is used to read and set input/output data in subsystems from an SCS. SCS supports the Modbus communication protocol.

Mount a serial communication module on the SCS to connect to other systems. By accessing data of other systems via the subsystem communication from the SCS, connection with PLCS, outputs to LED and so forth can be established. Communication data from subsystems is handled by using subsystem communication input/output FBs in the application logic. The subsystem communication function does not affect the safety functions executed in the SCS.

Application capacities

The application capacity regarding subsystem communication is shown as follows:

Table D2.9-1 Application capacities

Item	Maximum number	Remarks
Number of communication modules that can be mounted	4 modules (2 pairs)/SCS	(*1) (*2)
Dual-redundancy	Possible	
Number of communication data units	2000 or 500 data units/SCS	(*3) (*4)
Communication I/O size	1000 words/SCS	(*5) (*6)
Size of data that can be communicated per communication module	1000 words	
Number of ports used per communication module	2 ports	Same protocol for the 2 ports
Number of subsystem stations that SCS can communicate with per port	30 stations	
Number of communication definitions per module	128 definitions	

*1: Total number of ALR111/ALR121/ALE111 for the subsystem communication that is mounted to the same SCS
*2: Communication modules for the Modbus slave communication and DNP3 communication are not included in the count.
*3: This specifies the number of data items that can be wired to subsystem communication input/output FB instances.
*4: 2000 data units for SCSP3, SCSL2, SCSP2, SCSP1, SCSU1, and 500 data units for SCSV1.
*5: The maximum total size of data that can be assigned to discrete inputs/outputs is 256 words (4096 bits).
*6: It is not allowed to wire the subsystem communication I/O FB instances and the allocated areas beyond the limitation on total number of communication data.

SEE ALSO For more information about details on requirements of the entire SCS for installing ALR111/ALR121, refer to:

A5.3, “Restrictions on installation of hardware” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Dual-redundancy of communication

Communication can be made dual-redundant by using two adjacent serial communication modules (an odd numbered slot and the slot with the same number +1). This redundancy method makes the communication module and communication paths to the subsystem dual-redundant. When a communication module or subsystem error occurs (including the communication errors caused by a communication routing error, subsystem interface error and so on), the dual-redundancy scheme automatically chooses the normal module as the controlling module.

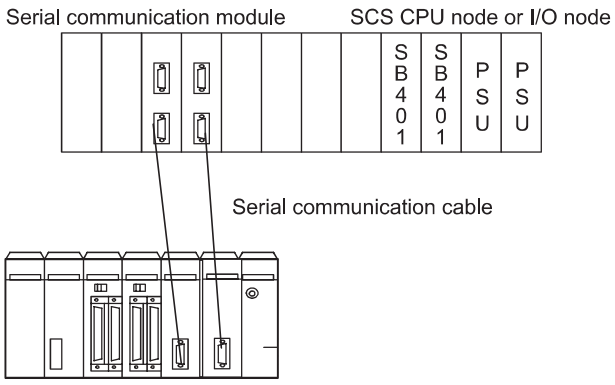


Figure D2.9-1 Example of dual-redundant communication

Two dual-redundant serial communication modules are controlled by the basic software in the CPU on the control side in order to determine which is the control side and which is the standby side. A communication module that operates normally and communicates normally with the subsystems is selected to be the control side.

The module on the control side performs read and write communication.

The module on the standby side performs read communication to diagnose the communication path.

The control right is switched from the serial communication module on the control side to the serial communication module on the standby side if either one of the following conditions is met.

- An error has been detected in the communication module on the control side and the communication module on the standby side is normal.
- An error has occurred on the control side and all communication on the standby side (2 ports) is normal.

Conditions for dual-redundancy

Modules on both sides (paths on both sides) must be able to read and write devices of subsystems. If the subsystem side is dual-redundant and reading and writing are restricted due to control rights of subsystems, communication modules cannot be made dual-redundant.

Only packages performing readback communication can make an output dual-redundant. In Modbus communication, if readback communication is disabled using the Communication I/O Builder, dual-redundancy cannot be applied.

Precautions for dual-redundant modules

The control right is determined by checking each module. This means that even if a communication error occurs on the control side, the control right is not switched unless all communication (all communication via both ports if two ports are used by one communication module) on the standby side is normal.

Data update is stopped from the time a communication error occurs and is detected on the control side until the time the control right is switched. For example, when the control right is switched due to no response from serial communication module, a communication error occurs after the following "Elapsed Time" passes.

- Elapsed Time = Response time x (number of retries + 1)

Definition of dual-redundancy

- Definition of Communication Modules

A communication module should be defined using an odd number slot. If redundancy is specified, the even number slot immediately to the right is automatically defined as a communication module as well.

- Communication Definition
  The same communication definition is used for both communication modules.

  The communication definition should be assigned to the communication module placed in the odd number slot. The same communication definition as the odd number slot is automatically assigned to the communication module in the even number slot as well.

SEE ALSO For more information about subsystem communication function, refer to:

D1., “Common items regarding subsystem communication functions” on page D1-1

About impact of online change download

The following table shows the impact of online change download of items related to the subsystem communication that can be changed online on communication modules or subsystems communication input/output FB.

Table D2.9-2 Impact of online change download

Items that can be changed online	Impact on communication modules	Impact on logic (communication input/output FBs)
Modification of transmission definition Addition of communication definition Deletion of communication definition Change of communication definition	Communication modules whose definitions are changed are restarted. No impact on other communication modules.	Communication input/output FBs wired to changed communication modules become faulty during restarting of the communication modules. They return to normal after completion of communication module restarting. No impact on other communication input/output FBs.
Addition of subsystem communication input/output FB (*1)	No impact.	Added communication input/output FBs take fixed values during online change. They return to normal operation after completion of online change.
Change of wiring for subsystem communication input/output FB	No impact.	The change is reflected. No impact on other communication input/output FBs.
Deletion of subsystem communication input/output FB Change of input operation at errors	No impact.	No impact on other communication input/output FBs.

*1: Recreating communication input/output FBs after deleting existing communication input/output FB instances is also regarded as addition of communication input/output FB.

SEE ALSO For more information about impact of online change download, refer to:

E1.7, “Online change of subsystem communication modules” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

About readback communication operations

If readback communication is enabled, outputs on the subsystem side are read and write communication is not performed unless the readback value is different from the value to be written. If the output value is changed in the CPU, and this causes the readback value to be different from the value to be written, write communication to the subsystem side is performed. If the output value is changed on the subsystem side while normal communication, and this causes the readback value to be different from the value to be written, write communication to the subsystem side is performed.

If readback communication is disabled, write communication is only performed at the timing of communication periods where the previous output value and the current output value are different. This means that even if the output value is changed on the subsystem side, a communication module does not perform write communication again.

Note that the function code of the address specified by Communication I/O Builder determines whether or not to perform readback in the Modbus communication.

Table D2.9-3 Readback communication operation

Item	With readback	Without readback
CPU initialization start (Output disabled status)	If outputs are disabled, the physical data of the communication input/output data is set to the value read back from the subsystem. The value read back from the subsystem is output until the output enable operation is performed.	If outputs are disabled, the initial value of the physical communication input/output data is set to 0. No output is made until the output value is changed. The value is output when it changes to a non-zero value after the output enable operation. (*1)
Error in locked communication module (at communication module error, online change causing a communication module to reset)	If errors occur in the ALR111/ALR121 modules or in the communication, or online changes are made while communication modules are locked, the physical data of the communication input/output data is set to the value read back from a subsystem. The value on the subsystem side is set to the output value by locking the output when performing maintenance and online change.	In the same way as in the case of initialization start, the output value is set to 0 and the value is output when it changes to a non-zero value. (*1)
Communication error	The status becomes BAD if a communication error occurs.	Even if a communication error occurs, the BAD status may not be notified. When a communication error occurs, no output is made and the output of the CPU and the output of a subsystem become different.
Dual-redundant	Dual-redundancy is supported.	Dual-redundancy is not supported if addresses without readback are used.

*1: This is handled by a function that suppresses writing for 70 seconds after restart if ALR111/ALR121 modules are restarted. This function can be disabled by changing the Option 2 setting.

SEE ALSO For more information about option settings, refer to:

D2.1, “Communication specifications” on page D2-2

D3. Modbus communication (for ALE111)

Modbus communication (for ALE111) is a function that mounts ALE111 (Ethernet communication module) in the SCS, and performs communication between the Ethernet interface in Modbus PLC and ALE111.

The Modbus/TCP master is the SCS, and the Modbus/TCP slave is Modbus PLC.

You can use Modbus communication (for ALE111) in the SCS of ProSafe-RS R4.01 or later.

Target models

The following are the supported models in Modbus communication (for ALE111):

- STARDOM autonomous controller: FCN, FCJ
- FA-M3 range-free controller: F3SP71-4S, F3SP76-7S
- Gas chromatograph: GC8000

The target model of Modbus communication (for ALE111) is referred to as Modbus/TCP PLC.

D3.1 Communication specifications

This section describes the specifications for communication between an SCS and a Modbus/TCP PLC.

Communication capacity

The following table shows the Modbus communication (for ALE111) capacity applicable to subsystem communication between the SCS and a Modbus/TCP PLC.

Table D3.1-1 Modbus communication (for ALE111) communication capacity

Item	Maximum capacity	Remarks
Number of communication modules that can be mounted	4 modules (2 pairs)/SCS	(*1) (*2)
Amount of data that can be transmitted by a single ALE111	1,000 words (1 word = 16 bits)	Limitations of the SCS Communication I/O data area: 1,000 words per SCS Number of communication data units: 2000 data units per SCS
Number of subsystem stations that can be communicated with	30 stations per port	
Size of communication data per communication definition	Word device read: 125 words Word device write: 100 words Bit device read: 2,000 bits Bit device write: 800 bits	One communication definition corresponds to one communication. This limitation corresponds to one communication in the Modbus/TCP protocol.
Number of communication definitions per module	128 definitions	
Number of usable ports	1	Ethernet port number in ALE111 is 1.

*1: Total number of ALR111/ALR121/ALE111 for the subsystem communication that is mounted to the same SCS
*2: Communication modules for the Modbus slave communication and DNP3 communication are not included in the count.

Simultaneity of communication data

Modbus/TCP PLCs assure simultaneity of communication data in units of 16 bits. Accordingly, simultaneity of communication data between an Ethernet communication module and a Modbus/TCP PLC is also assured in units of 16 bits.

TIP

Modbus/TCP PLCs process data in units of 16 bits. Simultaneity of 32-bit data depends on the application software used on the Modbus/TCP PLC side. To assure simultaneity of communication data in units of 32 bits, the application software on the Modbus/TCP PLC side needs to set 32-bit data within the same control period.

Transmission specifications

The transmission specifications for subsystem communication with a Modbus/TCP PLC are as follows.

Table D3.1-2 Transmission specifications

Item	Description (*1)	Remarks
Interface	Ethernet	IEEE802.3 compliant
Physical layer	10BASE-T	
Baud rate	10 Mbps	
Transmission method	Half-duplex	

Continues on the next page

Table D3.1-2 Transmission specifications (Table continued)

Item	Description (*1)	Remarks
Communication protocol	ARP, ICMP, UDP/IP, and TCP/IP	
Data type	Binary	
Response timeout	0 to 99 sec [4 sec]	When specified as 0, the default value (4 sec) will be reset in ALE111.
Communication retry	0 to 99 [1]	When specified as 0, the default value (once) will be reset in ALE111.
Interval of connection retries	0 to 999 sec [30 sec]	When specified as 0, the default value (30 sec) will be reset in ALE111.
Error control (CRC-16, etc.)	None	
Option 1	0 to 65535 [502]	Port number (set to 502, if 0)
Option 2	0 to 512 [0]	Setting range: 0 to 512 When connecting with a dual-redundant CPU in STARDOM, specify as 512. For other cases, specify as 0 (default value).
Option 3	0	Not used
Option 4	0	Not used

*1: The recommended settings are shown in [].

It is compliant with the protocols that are described in the following:

OPEN Modbus/TCP SPECIFICATION Release 1.0, 29 March 1999 Andy Swales Schneider Electric

Communication error code

Modbus/TCP PLC-specific error codes resulting from address and communication errors are shown in the following table.

Table D3.1-3 Communication error code list

Error code	Description
A3B0	No response
A3B1 (*1)	Subsystem station number out of range
A3B2 (*1)	Subsystem station number specified as 0
A3B3 (*1)	Address definition is abnormal (abnormality in specified element type)
A3B4 (*1)	Address definition is abnormal (abnormality in specified element number)
A3B5 (*1)	Too many communication points
A3B6 (*1)	Writing to a read-only command occurred
A3B8 (*1)	Odd number is used for the size of 4-byte register
A3B9 (*1)	Option value is out of range
A3BA (*1)	Cannot create communication frame
A3BC (*1)	IP address is not specified
A3BD	Maximum number of connection in subsystem exceeded
A3C1	The station number in received text is abnormal
A3C2	The element number in received text is abnormal
A3C3	The function code in received text is abnormal

Continues on the next page

Table D3.1-3 Communication error code list (Table continued)

Error code	Description
A3C4	Data in received text is abnormal
A3C5	Data size in received text is abnormal
A3C6	The length of the received text is abnormal
A3D1 (*2)	Error code $01 received
A3D2 (*2)	Error code $02 received
A3D3 (*2)	Error code $03 received
A3D4 (*2)	Error code $04 received
A3D5 (*2)	Error code $05 received
A3D6 (*2)	Error code $06 received
A3D7 (*2)	Error code $07 received
A3D8 (*2)	Error code $08 received
A3D9 (*2)	Error code $09 received
A3DA (*2)	Error code $0A received
A3DB (*2)	Error code $0B received
A3DC (*2)	Error code $0C received
A3DD (*2)	Error code $0D received
A3DE (*2)	Error code $0E received
A3DF (*2)	Error code $0F received
A3E0 (*2)	Error code $10 received
A3E1 (*2)	Error code $11 received
A3E2 (*2)	Error code $12 received
A3E3 (*2)	Error code $13 received
A3E4 (*2)	Error code $14 received
A3E5 (*2)	Error code $15 received
A3E6 (*2)	Error code $16 received
A3E7 (*2)	Error code $17 received
A3E8 (*2)	Error code $18 received

*1: This error is a definition error of ALE111. If this error occurs, no communication can be performed to the Modbus/TCP PLC.
*2: This is an error when an error message and an error code are received from the Modbus/TCP PLC.

D3.2 Modbus/TCP PLC devices accessible from the SCS

This section describes the Modbus/TCP PLC devices that can be accessed from the SCS.

Internal data of a Modbus/TCP PLC are called "devices". Devices can be bit devices or word devices, as described in the following explanation:

- Bit devices
  Data in which each bit has a meaning. An input relay is a bit device.
- Word devices
  Data in which each word (1 word = 16 bits) has a meaning. A holding register is a word device.

Modbus/TCP PLCs also have devices called "special coil" and "communication status".

Accessible devices

To access Modbus/TCP PLC devices, you must set [Comm Device & Address] of Signal Definition and [Size] of Communication Definition in the Safety Communication I/O Editor, or set [Device Address] and [Size] in the Communication I/O Builder.

With Modbus/TCP PLCs, "Device Address" is set by using the following format:

<Function code> + <Device type> + <Address within device>

To specify input relays 100012 to 100015, for example, set A100012 for "Device Address" and 1 for "Size." "A" of A100012 indicates a function code, "1" indicates a device type, and "00012" indicates an address within device.

The following table lists the Modbus/TCP PLC devices accessible from the SCS, as well as the corresponding addresses and Modbus protocol function codes.

Table D3.2-1 Bit devices list

Device	Address			Modbus/TCP protocol function code (hexadecimal)	
	Function code	Modbus/TCP PLC device type	Address in the Modbus/TCP PLC device	Read	Write
Coil	A	0	XXXX (*1)	01	0F
	B				05
	X			-	0F
	Y				05
Input relay	A	1	XXXX (*1)	02	-

*1: In Modicon Premium, XXXX is the reference number.

Table D3.2-2 Word devices list

Device	Address			Modbus/TCP protocol function code (hexadecimal)	
	Function code	Modbus/TCP PLC device type	Address in the Modbus/TCP PLC device	Read	Write
Input register	A	3	XXXX (*1)	04	-
	C				

Continues on the next page

Table D3.2-2 Word devices list (Table continued)

Device	Address			Modbus/TCP protocol function code (hexadecimal)	
	Function code	Modbus/TCP PLC device type	Address in the Modbus/TCP PLC device	Read	Write
Holding register	A	4	XXXX (*1)	03	10
	B				06
	C				10
	D				16 (*2)
	X			-	10
	Y				06
	Z				10
	W				16 (*2)

*1: In Modicon Premium, XXXX is the reference number.
*2: 16 command is not supported in Modicon Quantum/Premium.

Table D3.2-3 Other devices

Device	Address			Modbus/TCP protocol function code (hexadecimal)	
	Function code	Modbus/TCP PLC device type	Address in the Modbus/TCP PLC device	Read	Write
Special coil	SP000			07 (*1)	-
Communication status	STSXXX (*2)			-	-

*1: 07 command is not supported in Modicon Premium.
*2: XXX is the station number of PLC.

The meaning of each function code is as follows. The size is specified in the Safety Communication I/O Editor or Communication I/O Builder.

- A
  Read data for the specified size.

  Write data for the specified size. Readback is supported.
- B
  Read data for the specified size.

  Writes data individually to each modified device in units of 1 bit for a bit device, or in units of 16 bits for a word device. Readback is supported.
- C
  Read data for the specified size.

  Writes data individually to each modified device in units of 32 bits. Readback is supported.
- D
  Read data for the specified size.

  Writes data individually to each modified word device in units of 1 bit. Readback is supported.
- X
  Write data for the specified size when a change occurs. Readback is not supported.
- Y
  Writes data individually only to each modified device for the size of each device when a change occurs. Readback is not supported.

- Z
  Writes data individually only to each modified device in units of 32 bits when a change occurs. Readback is not supported.
- W
  Writes data individually only to each modified word device in units of 1 bit when a change occurs. Readback is not supported.

Table D3.2-4 List of function codes

Function code	Device	Read	Write	Readback
A	Bit	Read collectively	Write collectively	Yes
	Word	Read collectively	Write collectively	Yes
B	Bit	Read collectively	1-bit	Yes
	Word	Read collectively	16-bit	Yes
C	Word	Read collectively	32-bit	Yes
D	Word	16-bit	1-bit	Yes
X	Bit	-	Write collectively	None
	Word	-	Write collectively	None
Y	Bit	-	1-bit	None
	Word	-	16-bit	None
Z	Word	-	32-bit	None
W	Word	-	1-bit	None

IMPORTANT

In a dual-redundant configuration based on ALE111, only writing of data to the Modbus/TCP PLC with readback is supported. Writing of data without readback is not supported in a dual-redundant configuration.

Supported function codes, accessible devices, and sizes vary depending on the Modbus/TCP PLC model.

SEE ALSO

For more information about readback communication, refer to:

D2.5, “Readback communication” on page D2-20

For more information about supported function codes, accessible devices, sizes, and so on, refer to:

the user manual for the Modbus/TCP PLC being used

D3.3 Builder setting items in the Modbus communication

This section explains the builder settings in the Modbus communication when the Ethernet communication module is used.

When performing RS original engineering, you can define the Ethernet communication module and set I/O parameters by using I/O Wiring View and I/O Parameter Builder. After defining the Ethernet communication module and setting I/O parameters, you need to allocate the communication I/O data, and assign element numbers and subsystem communication I/O FBs by using Communication I/O Builder.

When performing I/O list engineering, you can define the Ethernet communication module, set I/O parameters, allocate communication I/O data, and allocate element numbers to subsystem communication I/O FB by using IOM Definition Editor and Safety Communication I/O Editor.

TIP

This section mainly describes for the case when performing RS original engineering. The setting item names displayed may differ between I/O list engineering and RS original engineering, but the settings are the same.

SEE ALSO

For more information about engineering of subsystem communication modules using Safety Communication I/O Editor, refer to:

D1.5, “Engineering for subsystem communication modules” on page D1-37

For more information about I/O list engineering, refer to:

D., “Procedures to create applications using the I/O list engineering method” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

D3.3.1 Settings in the I/O Wiring View

When performing RS original engineering, you need to set the following items by using the I/O Wiring View.

- Subsystem communication module definition
- Dual-redundant Ethernet communication module

Subsystem communication module definition

If an ALE111 is used for subsystem communication, you need to select ALE111M as the module type. You need to specify the mounting position (node, slot number) of the module, as well as whether or not to use a dual-redundant configuration.

Dual-redundant Ethernet communication module

To use Ethernet communication modules in a dual-redundant configuration, you need to set IsRedundant to TRUE.

D3.3.2 Settings in the I/O Parameter Builder

When performing RS original engineering, you need to set the following items in ALE111M by using the I/O Parameter Builder.

Connection Device

You need to set the type of connection device.

You should select S_MODTCP when you use the subsystem communication function in Modbus/TCP.

Default value: S_MODTCP

S_MODTCP: Modbus/TCP slave

Comment

You can enter a comment regarding the Ethernet communication module. This comment can be entered by using up to 24 single-byte characters or 12 double-byte characters.

IP Address

You need to set the IP address of the Ethernet communication module. You can enter any IP address that you want.

Default: This field is empty by default; be sure to enter an IP address. If no value is entered, an error occurs when you try to save the settings in the builder.

Format: nnn.nnn.nnn.nnn

Setting range: 0.0.0.1 to 255.255.255.254
However, do not set the following IP addresses:

- Host address digits are all zeros or all ones in binary form.
(Example: When subnet mask is 255.255.255.0, 192.168.1.0, 192.168.1.255, etc.)
- Any of the numbers delimited with a period has leading zeros.
(Example: 192.168.08.09, 192.168.008.009, etc.)

Subnet Mask

You need to set the subnet mask of the Ethernet communication module. You can enter a subnet mask that you want.

Default: This field is empty by default; be sure to enter a subnet mask. If no value is entered, an error occurs when you try to save the settings in the builder.

Format: nnn.nnn.nnn.nnn

Setting range: 0.0.0.1 to 255.255.255.254
However, do not set the following subnet masks:

- Values less than 255.0.0.0 for a class A IP address
(Example: 128.0.0.0)
- Values less than 255.255.0.0 for a class B IP address
(Example: 255.128.0.0)
- Values less than 255.255.255.0 for a class C IP address
(Example: 255.255.128.0)

Default Gateway

You need to set the gateway address of the Ethernet communication module. You can enter a desired gateway address.

Default: Blank

Format: nnn.nnn.nnn.nnn

Setting range: 0.0.0.1 to 255.255.255.254
However, do not set the following gateway addresses:

- Host address digits are all zeros or all ones in binary form.
(Example: When subnet mask is 255.255.255.0, 192.168.1.0, 192.168.1.255, etc.)
- Network address digits do not match the IP address.
(IP address is 192.168.1.1 and default gateway address is 192.168.2.2 when the subnet mask is 255.255.255.0.)
- Any of the numbers delimited with a period has leading zeros.
(Example: 192.168.08.09, 192.168.008.009, etc.)

Paired IP Address

When an Ethernet communication module is set to dual-redundant configuration, you need to set the IP address of the Ethernet communication module in even slot. You can enter any IP address that you want.

Default: The default value is empty by default; be sure to enter a paired IP address. If the paired IP address is not set with the dual-redundant configuration enabled, there will be an error when saving in the builder. If the paired IP address is set with the dual-redundant configuration disabled, there will be an error when saving in the builder.

Format: nnn.nnn.nnn.nnn

Setting range: 0.0.0.1 to 255.255.255.254
However, do not set the following IP addresses:

- Host address digits are all zeros or all ones in binary form.
(Example: When subnet mask is 255.255.255.0, 192.168.1.0, 192.168.1.255, etc.)
- Any of the numbers delimited with a period has leading zeros.
(Example: 192.168.08.09, 192.168.008.009, etc.)

Paired Default Gateway

When an Ethernet communication module is set to dual-redundant configuration, you need to set the IP address of the default gateway that is used by an Ethernet communication module in even slot. You can enter any IP address that you want.

Default: The default value is empty by default; be sure to enter an IP address of a dual-redundant default gateway. If the IP address of paired default gateway is not set with the dual-redundant configuration enabled, there will be an error when saving in the builder. If the IP address of paired default gateway is set with the dual-redundant configuration disabled, there will be an error when saving in the builder.

Format: nnn.nnn.nnn.nnn

Setting range: 0.0.0.1 to 255.255.255.254
However, do not set the following IP addresses:

- Host address digits are all zeros or all ones in binary form.
  (Example: When subnet mask is 255.255.255.0, 192.168.1.0, 192.168.1.255, etc.)
- Network address digits do not match the IP address.
  (IP address is 192.168.1.1 and default gateway address is 192.168.2.2 when the subnet mask is 255.255.255.0.)
- Any of the numbers delimited with a period has leading zeros.
  (Example: 192.168.08.09, 192.168.008.009, etc.)

Response Timeout

You need to set the timeout period to wait for subsystem response. The unit is in seconds.

Default: 4 sec

Setting range: 0 to 99 sec

Communication Retry

You need to set the number of retries to be attempted after a communication error occurs.

Default: 1 time

Setting range: 0 to 99 times

Interval of Connection Retries

You need to set the interval of communication with a station that generated a communication error to check for recovery of communication (recovery communication). The unit is in seconds.

Default: 30 sec

Setting range: 0 to 999 sec

Port number

You need to set the port number of the Modbus/TCP.

Default: 502

Setting range: 0 to 65535

Option (1 to 4)

You need to set option 1 or 2 for Modbus/TCP.

Option 1

You need to set the TCP/IP port number in option 1.

When set as 0, it will operate in the same manner when 502 is set.

Option 2

You need to set the recovery communication method in option 2.

When connecting with a dual-redundant CPU of STARDOM, you need to set 512 as specified in recovery communication. For other cases, you need to set to 0 (default value).

D3.3.3 Settings in the Communication I/O Builder

This section describes the ALE111-specific setting items in the Communication I/O Builder.

It mentions about the following items when using Modbus/TCP PLC.

- Program Name
- Port
- IP Address
- 2nd IP Address

Program Name

You need to set the program name by using the node number, slot number and S_MODTCP, as follows:

Program Name : n-s fixed character string

- n: Node number
- s: Slot number
- Fixed character string: S_MODTCP

Port

You need to set the port that is used in the subsystem communication module.

Always set to 1.

IP Address

You need to set the IP address of the equipment in the subsystem to be used.

Set the IP address of the Modbus/TCP PLC.

2nd IP Address

When the Ethernet communication module and Modbus/TCP PLC communication interface are set to dual-redundant configuration, you need to set the IP address (2nd IP address) of the subsystem side where the Ethernet communication module on the odd slot communicates.

Do not set 2nd IP address if the Modbus/TCP PLC communication interface is not set to dual-redundant configuration.

Device Address

You need to set the start address of the data in Modbus/TCP PLC.

The following table shows the addresses that can be set.

Nothing is specified by default.

Coil:	A0xxxx, B0xxxx, X0xxxx, Y0xxxx
Input relay:	A1xxxx
Input register:	A3xxxx, C3xxxx
Holding register:	A4xxxx, B4xxxx, C4xxxx, D4xxxx, X4xxxx, Y4xxxx, Z4xxxx, W4xxxx
Special coil:	SP000

Communication status: STSxxx

"xxxx" indicates an address within Modbus/TCP PLC device, and is set as a decimal or hexadecimal value between 0 and 65535 (0H and FFFFH). If a hexadecimal value is used, add "H" at the end.

The 0 or 0s at the beginning of "xxxx" can be omitted. For example, coil addresses of A023, A0023 and A00023 all represent the same address.

SEE ALSO For more information about specifying addresses, refer to:

D3.2, “Modbus/TCP PLC devices accessible from the SCS” on page D3-5

D3.4 Actions during unsteady state

This section describes the precautions relating to actions in the ALE111 when recovering from an unsteady state during a system abnormality, online change, and other occurrences. I/O operation, data status, and other operations during an unsteady state are in the same manner as the operation in serial communication module.

Actions for ALE111 during unsteady state

The following table shows an unsteady state in the Ethernet communication module, and operations between Ethernet communication module and the subsystem.

Table D3.4-1 Actions for ALE111 during unsteady state

Causes of unsteady state	Handling actions for ALE111 after recovery
Stopping both CPU	Resume communication (*1)
Power outage in the system	Reconnection standby (*2)
Offline download	Reconnection standby (*2)
Switching control right	Continuation (*3)
Power outage in the node	Reconnection standby (*2)
Communication error on both nodes	Resume communication (*1)
ALE111 maintenance (connection and disconnection)	Reconnection standby (*2)
Switching control right in ALE111	Continuation (*3)
IOM Loading for ALE111	Resume communication (*1)
Online change in ALE111 transmission definition	Resume communication (*1)
Online change of communication I/O definition	Resume communication (*1)

*1: Communication will immediately resume after recovery from an abnormality.
*2: The connection for ALE111 communication will not be established until connection in the other communicating party is closed. It takes a few minutes from the system error occurrence to the closing of the connection in the other communicating party. Communication function in ALE111 will be determined as abnormal after connection is retried, and an SSCOM error message is sent.
*3: It does not affect the state in ALE111. It will continue to operate.

Reconnection standby

When ALE111 suddenly stops due to system abnormalities such as node power outage, module connection and disconnection, the connection that operates communication in the ALE111 will be lost. After starting communication program in the ALE111, it will attempt to reconnect with the other communicating party. However, while the connection state is maintained by the subsystem, connection request from ALE111 fails and communication will not be recovered. The time when the connection state is maintained in the subsystem depends on the configuration of the TCP/IP KeepAlive function (connection existence confirmation monitor).

If the connection is terminated with an error, the communication program in ALE111 will run based on the specified number of communication error retries. If it is possible to use multiple lines in the same TCP/IP port number, and if there is a line in non-connected state in the subsystem of the communication destination party, ALE111 will establish a connection using a different pathway in the reconnection. In this case, communication will be immediately recovered after starting ALE111.

If ALE111 communication program cannot establish connection with the communication destination party even after a specified number of retries, it will be determined as a connection error, and an SS-COM error message will be output. Then, ALE111 will retry connection at a specified interval of connection retries.

SEE ALSO For more information about how to configure the KeepAlive function and the behavior thereof, refer to:

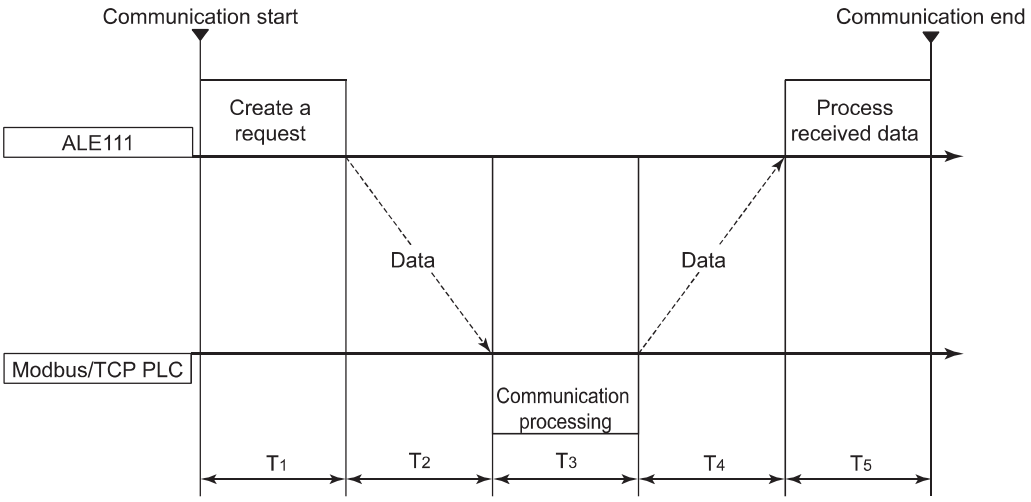
manual for each subsystem

Resuming communication

Connection in the ALE111 will be turned off during online change of ALE 111 transmission definition and communication I/O definition, IOM download for ALE111, and recovery from a system error in the route positioned above the ALE111. This will delete the subsystem connection in the communication destination party, and will immediately recover communication upon starting the ALE111.

D3.5 Communication time between Ethernet communication module and Modbus/TCP PLC

The communication time between an Ethernet communication module and a Modbus/TCP PLC is calculated as the total sum of T1 through T5 as follows.



T1: Request creation time on the ALE111 side Approx. 10 ms
T2: Request (command) transmission time
T3: Reply creation time on the Modbus/TCP PLC side
(CPU processing time on the Modbus/TCP PLC side)
T4: Reply (response) transmission time
T5: Received data processing time on the ALE111 side Approx. 10 ms

Figure D3.5-1 Timing chart for communication between a communication module and a Modbus/TCP PLC

The following shows how to calculate the communication time.

In the following example, calculation of time is provided where 50 holding register values are read.

Communication time is calculated based on the following criteria:

Compared to other processes, command transmission time (T_2) and response transmission time (T_4) take up smaller time. With T_2 and T_4 combined, it takes up 1 to 5 ms. In this example, the whole time will be calculated as $T_2 + T_4 = 5$ ms.

- Modbus/TCP PLC scan period: 50 ms

Command transmission time (T_2) + Response transmission time (T_4) = 5 ms

Modbus/TCP PLC CPU processing time (T_3) = 50 ms

$$\text{Total time} = \sum_{i=1}^{5} Ti = 10 + 5 + 50 + 10 = 75 \text{ ms}$$

TIP

Communication time is just for reference as it is greatly affected by the network traffic.

D4. ProSafe-SLS communication (for ALR121)

ProSafe-RS can acquire events of ProSafe-SLS and data using subsystem communication. Acquired events and data can be handled on SCS in the same way existing events and data are handled. If ProSafe-RS is integrated with a CENTUM system, the events and data of ProSafe-SLS can be comprehensively managed by using HIS.

SCS communicates with the communication module of ProSafe-SLS through a communication module (model: ALR121). This communication enables the following operations:

- Data access
  ProSafe-RS can access the input/output data of ProSafe-SLS using the subsystem communication function.
- Event acquisition
  ProSafe-RS can acquire the events generated by ProSafe-SLS.

  To integrate events of ProSafe-SLS with ProSafe-RS, synchronize the time of ProSafe-SLS with that of SCS to align the time stamps of these events to events of ProSafe-RS.
- Alarm notification
  To notify CENTUM HIS of error conditions as alarms when the error conditions are detected based on the diagnostic information of ProSafe-SLS, it is necessary to perform engineering and configure an application on both the ProSafe-SLS side and ProSafe-RS side.

SEE ALSO For more information about event notified in the case of a ProSafe-SLS error, refer to:

TI of ProSafe-SLS

D4.1 Operating environment

ProSafe-SLS is the only subsystem that the ProSafe-SLS communication function supports. If ProSafe-SLS and other subsystem are connected to the same communication path, proper operation of the ProSafe-SLS communication function cannot be guaranteed. To use the ProSafe-SLS communication function, check the conditions that are applicable to connection devices, subsystem communication program, and other aspects of operating environment explained here, and then make the necessary preparations.

Available input/output modules

The following table shows the input/output modules that can be used for the ProSafe-SLS communication function.

Table D4.1-1 Input/output modules that can be used for the ProSafe-SLS communication function

Model	Type	Purpose
ALR121	Serial communication module (RS-422/RS-485 interface)	For Modbus protocol (RTU mode)
SDV531	Digital output module (8 channels, 24 V DC, module isolation)	For time synchronization
SDV531-L/ L1DV531-L	Digital output module (8 channels, 24 V DC, module isolation, for long distance)	
SDV541/ L1DV541	Digital output module (16 channels, 24 V DC, module isolation)	

Available subsystem communication program

Use S_SLSMOD as the subsystem communication program for the ProSafe-SLS communication function.

S_SLSMOD is applicable only to ALR121. The S_SLSMOD-compatible hardware revisions of ALR121 conform to the conditions under which S_MODBUS can be applied.

Configuration of communication modules

When the subsystem communication program, S_SLSMOD, is applied for the communication module (model: ALR121), ALR121 can be used only in a non-redundant configuration.

D4.2 System configuration

The following figure shows an overall system configuration where ProSafe-SLS is connected to ProSafe-RS.

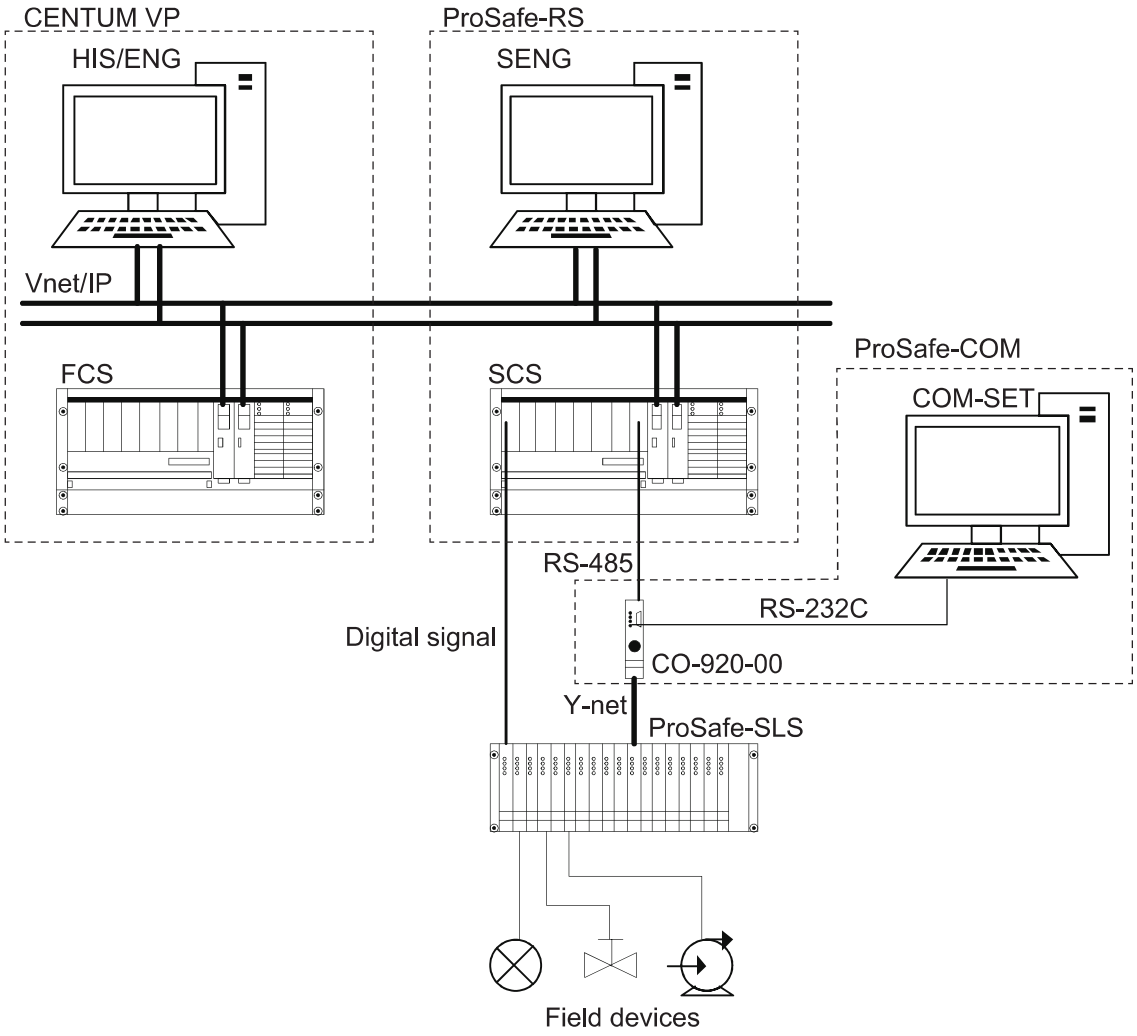


Figure D4.2-1 Example of an overall system configuration

The following table explains the terms that are used in the figure.

Table D4.2-1 Description of terms

Term	Description
ProSafe-SLS	A SIL4-certified safety instrumented system. It can be connected to other system through ProSafe-COM.
ProSafe-COM	One component of a safety instrumented system. It provides the communication function to connect ProSafe-SLS and other systems.
CO-920-00	A communication module that is one of the ProSafe-COM products. This module is hereinafter referred to as "CO-920."
COM-SET	Software package. This package is used for engineering and maintenance of CO-920. It also provides the function to display SOE events of CO-920. SET stands for "System Engineering Tool."
Y-net	A local network that connects each ProSafe-SLS module and ProSafe-COM. RS-485 serial communication is used.

D4.2.1 Connection configuration of SCS and ProSafe-SLS

The following figure shows the connection configuration of ProSafe-RS SCS and ProSafe-SLS.

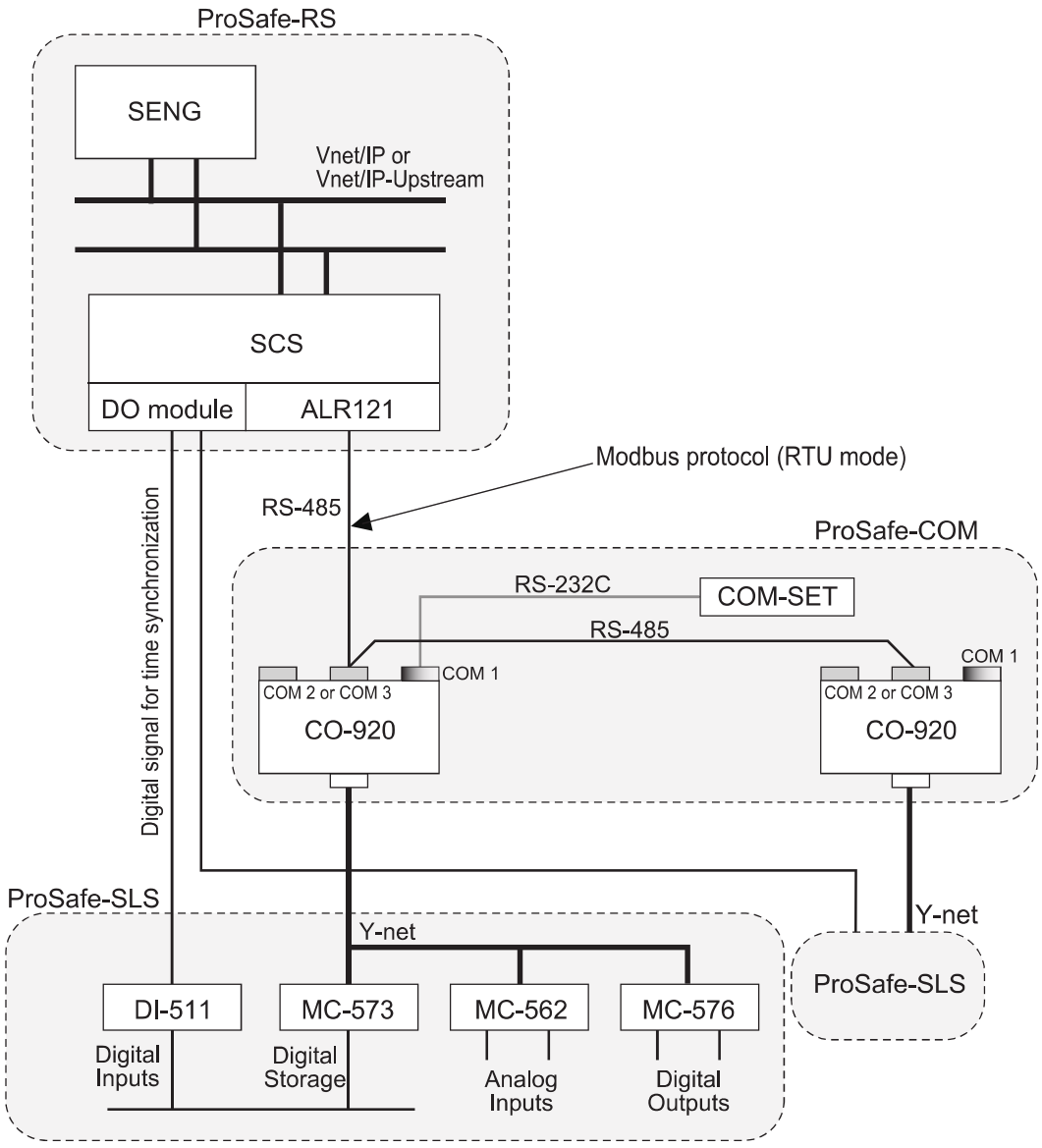


Figure D4.2.1-1 Connection configuration of ProSafe-RS SCS and ProSafe-SLS

"Vnet/IP or Vnet/IP-Upstream" in the figure is hereinafter abbreviated as "Vnet/IP."

To display the events of ProSafe-SLS in the SOE viewer as with the event data of SENG, the time of ProSafe-SLS must be synchronized with that of ProSafe-RS. The event time stamps given by ProSafe-SLS are used directly by ProSafe-RS. Connect the DO module of SCS and the DI module of ProSafe-SLS to synchronize the time.

D4.2.2 System overview of ProSafe-SLS

ProSafe-SLS is a safety system that can be applied to installations requiring the SIL4 safety level.

ProSafe-COM is one component of a safety system.

CO-920 is a communication module and one of ProSafe-COM products, which can be directly installed on a standard 19-inch cassette connector for ProSafe-SLS. To connect ProSafe-SLS to ProSafe-RS, connect CO-920 to ProSafe-RS as a communication interface with ProSafe-SLS.

For more information about the ProSafe-SLS system, refer to IMs of ProSafe-SLS.

Communication interface of ProSafe-SLS

Use Y-net as the communication interface between the ProSafe-SLS and external devices. Y-net is a local ProSafe-SLS network. Use CO-920 as an interface between the Modbus and Y-net networks. The external interface of CO-920 consists of one RS-232C port (port name: COM1) and two RS-485 ports (port names: COM2 and COM3).

The CO-920 acquires the events of ProSafe-SLS modules, time-stamps the acquired events based on its internal clock, sorts them chronologically, and then stores the sorted events in the event buffer. The resolution of time stamp is 1 ms. Events are stored in the event buffer according to the FIFO method.

Various engineering tasks on CO-920 are performed from the application software COM-SET by using RS-232 communication.

Communication interface between ALR121 and CO-920

The COM port of ALR121 in SCS is connected to the COM port of CO-920 by using RS-485 communication, and the two ports communicate with each other according to the Modbus protocol (RTU mode).

ALR121 (Modbus master) can access the I/O data of each ProSafe-SLS module that is connected to Y-net by using standard Modbus commands. It can also acquire ProSafe-SLS events from CO-920 by using expansion Modbus commands.

You need to download the subsystem communication program S_SLSMOD into ALR121. S_SLSMOD, which is a ProSafe-SLS communication program, can be used only by ALR121.

Setting the ProSafe-SLS time using an external clock

The ProSafe-SLS time can be set by using an external clock. When a change event involving a DI module associated with ProSafe-SLS time synchronization occurs, the CO-920 time is set to a fixed time.

D4.3 Data access

The ProSafe-RS can access input/output data of ProSafe-SLS by using the subsystem communication function. The Modbus protocol (RTU mode) is used for the communication protocol.

If the ProSafe-RS is integrated with a CENTUM system, the accessed data can be monitored using the HIS.

Handling of ProSafe-SLS communication data

The data that is collected by the ProSafe-RS by accessing the ProSafe-SLS can be handled by the communication input FBs and communication output FBs.

The subsystem communication FBs that can be used in connection with the ProSafe-SLS communication function are interference-free function blocks and cannot be used for input of safety loops.

A POU containing any subsystem communication FB that can be used under the ProSafe-SLS communication function must be approved by using the Integrity analyzer.

The following subsystem communication input FBs can be used in connection with the ProSafe-SLS communication function.

- SCI_B
- SCI_I

The following subsystem communication output FBs can be used in connection with the ProSafe-SLS communication function.

- SCO_B
- SCO_I

SEE ALSO

For more information about SCI_B, refer to:

9.1, “SCI_B (BOOL-type subsystem communication input)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about SCI_I , refer to:

9.2, “SCI_I (INTEGER-type subsystem communication input)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about SCO_B, refer to:

9.4, “SCO_B (BOOL-type subsystem communication output)” in POU Reference Manual (IM 32P03B20-01EN)

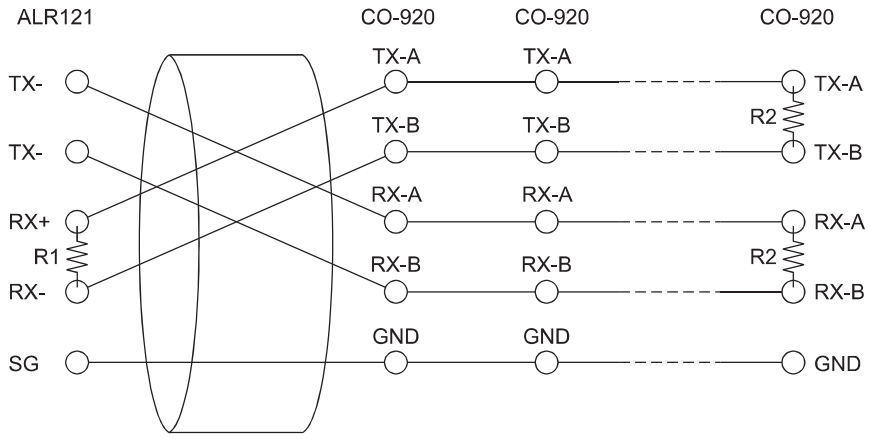
For more information about SCO_I, refer to:

9.5, “SCO_I (INTEGER-type subsystem communication output)” in POU Reference Manual (IM 32P03B20-01EN)

Connection interface of ProSafe-RS and ProSafe-SLS

Connect the ALR121 and CO-920 as a communication path for I/O data, events and ProSafe-SLS diagnostic information. Connect the two using 2-wire type or 4-wire type connection of RS-485 to a 1:n multi-drop configuration.

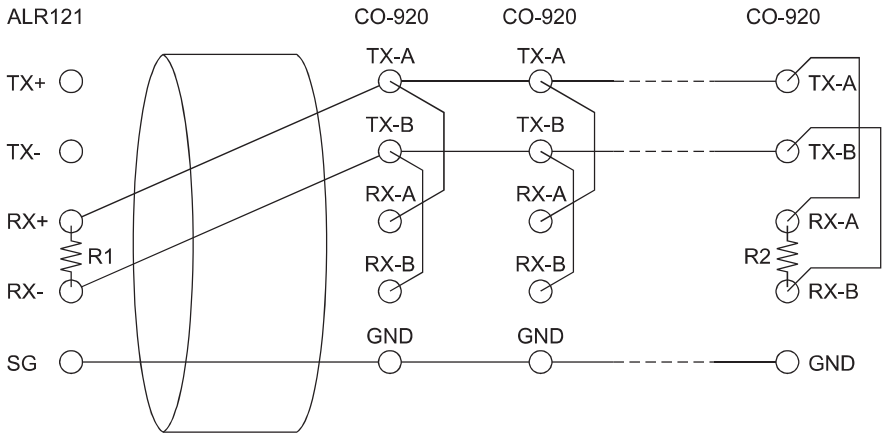
The following figure shows the 4-wire type connection of RS-485.



R1: Termination resistance of 120 ohm
R2: Termination resistance built in CO-920

Figure D4.3-1 1:n connection in 4-wire type of RS-485

The following figure shows the 2-wire type connection of RS-485.



R1: Termination resistance of 120 ohm
R2: Termination resistance built in CO-920

Figure D4.3-2 1:n connection in 2-wire type of RS-485

SEE ALSO For more information about connection method on the CO-920 side, refer to:

manual of CO-920

D4.4 Event acquisition

The SCS acquires events from the communication module of ProSafe-SLS (model: CO-920) through the communication module (model: ALR121). Acquired events are stored in the SOER event information storage area inside the SCS memory and integrated with existing SOE events. If a CENTUM system is integrated, acquired events can be viewed in the SOE Viewer of HIS.

You can not specify the events acquired from ProSafe-SLS as the trip signal of ProSafe-RS.

The Forcing function does not apply to events. Even if you lock the communication module (model: ALR121), events will remain unlocked. The SCS will continue to store events acquired from CO-920 into the SOE buffer.

SEE ALSO For more information about SOE event message acquired from the ProSafe-SLS, refer to:

"■ Event information displayed on SOE Viewer" on page D4-22

■ Basic event acquisition operation and time stamp

The subsystem communication program S_SLSMOD acquires events from the CO-920 of the specified station number based on the event acquisition communication definitions.

S_SLSMOD acquires events from the CO-920 periodically. If the subsystem communication period consists of one communication session for all communication definitions that are set for one ALR121 port, one event is acquired in one communication period.

Events are acquired into SCS in the order stored in the CO-920. The time stamps may become slightly imprecise for events that occur around when CO-920's time is set or around when time synchronization with SCS takes place.

■ SCS operation to acquire stored events

In the following situations, multiple events have already been stored in CO-920. The SCS acquires the stored events altogether.

- The SCS is connected to the CO-920 for the first time.
- The SCS changes the COM port to which the CO-920 is connected.
- The SCS, which was down for a long time but is finally recovered, is reconnected to the CO-920.
- The SCS is reconnected to the CO-920 after the communication was cut off for a long period of time because the faulty ALR121 was replaced, etc.
- Multiple events occur at the same time because ProSafe-SLS generated an error or shut down.

In order to acquire all stored events, the SCS continuously acquire events from CO-920 according to the communication definitions. The continuous acquisition of events begins from the next event after the last event acquired from CO-920. As the same with the normal communication, one event is acquired from CO-920 in one subsystem communication period.

■ Cautions when starting event acquisition

When the SCS continuously acquires multiple events that are already stored in the CO-920, it may take several hours for all events to be acquired, after the start of event acquisition, if many events are stored in the CO-920. In this case, a time lag of several hours may occur to acquire the latest event because the latest event of the CO-920 is acquired after the acquisition of all stored events is completed.

If events that are already stored in the ProSafe-SLS and not yet acquired by the ProSafe-RS are not needed, connect the COM-SET to the maintenance port of the CO-920 (port name:

COM1) and acquire the stored events from the CO-920, and then clear all events of the CO-920, so as to prevent these events from being acquired over a long period of time.

Events acquired by the COM-SET cannot be integrated with the SOE events of the ProSafe-RS.

Causes of event acquisition communication error

The following list describes why ALR121 sends a communication error code to the CPU:

- CO-920 is no longer responding.
  CO-920 may stop responding temporarily after being engineered from COM-SET while operating.
- An error occurred along the communication path between ALR121 and CO-920.
- A format error occurred in the response from CO-920.

IMPORTANT

Assume that ALR121 is disconnected from the SCS and then inserted again. An event acquired from ProSafe-SLS immediately before ALR121 is disconnected may be passed to the CPU module of the SCS redundantly after ALR121 is inserted into the SCS.

SEE ALSO For more information about communication error code, refer to:

"■ Communication error code" on page D2-3

Event time for SOE

The time information that is recorded at the time when an event occurs in ProSafe-SLS is the SOE event time. No new time information generates on the SCS side.

The SCS converts the event time of ProSafe-SLS to the ProSafe-RS time format, and then stores the converted time as an SOE event in the SOER event information storage memory.

D4.5 Time synchronization

All references to time in the explanation of time synchronization are described with Universal Time Coordinated (UTC).

To integrate events of ProSafe-SLS with the SOE of ProSafe-RS, it is necessary to synchronize the time of ProSafe-SLS with that of the SCS to align the time stamps of these events to those of ProSafe-RS.

The time can be synchronized by connecting the DO module of the SCS and the DI module of ProSafe-SLS.

Configuration for time synchronization

The following figure shows an example of a configuration for time synchronization using the DO module (model: SDV531).

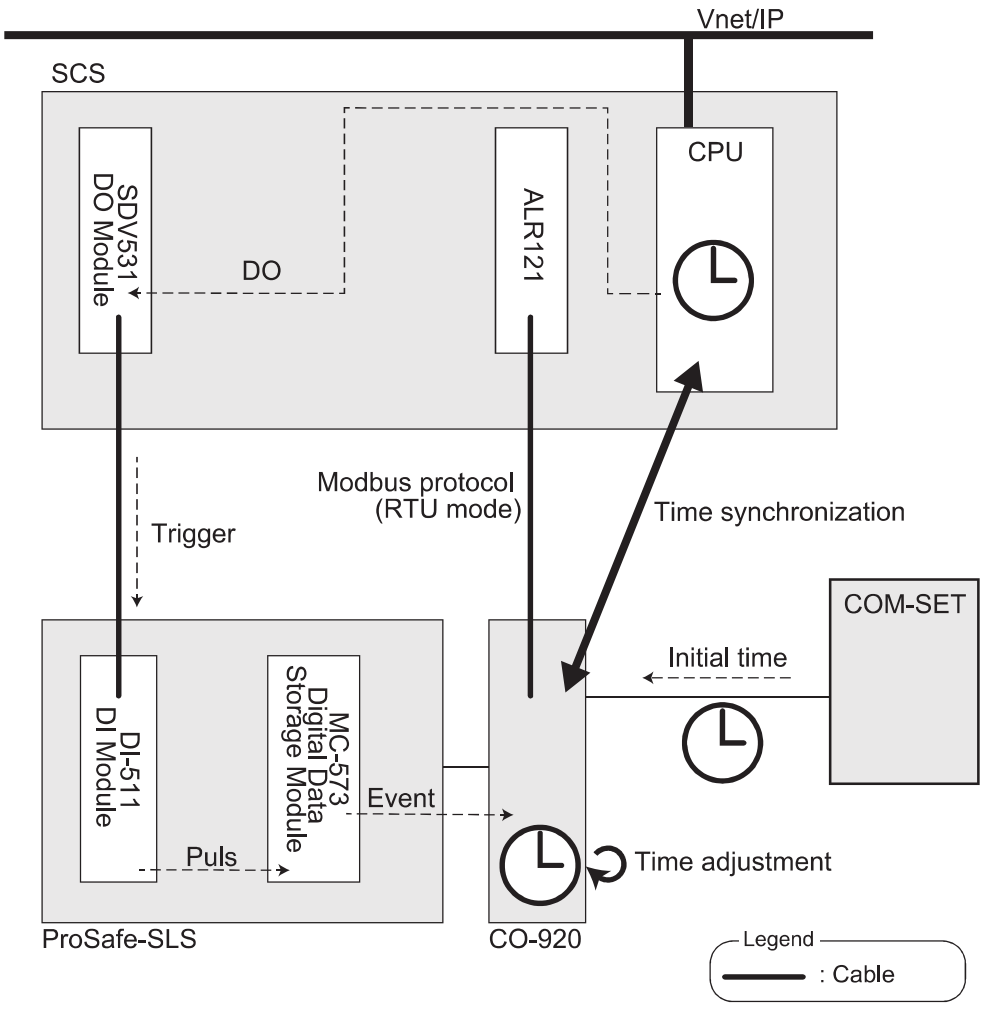


Figure D4.5-1 Configuration example for time synchronization of SCS and ProSafe-SLS

Connect the DO module of the SCS and the DI module of ProSafe-SLS.

To synchronize the time of the SCS with that of ProSafe-SLS, time synchronization parameters of CO-920 must be set from COM-SET. To set these parameters, connect COM-SET to the maintenance port of CO-920.

After the time synchronization parameters are set, cause a time synchronization event to generate periodically, for ProSafe-SLS, through the DO module and DI module, to allow for time synchronization.

It should be noted that, if multiple CO-920s are connected to the SCS, set the time synchronization parameters and also perform time synchronization through the DO module and DI module, for each CO-920.

Connection between ProSafe-RS DO module and ProSafe-SLS DI module

This section describes an example of connecting the DO module of SCS (model: SDV531 or SDV541) and DI module of ProSafe-SLS (model: DI-511) to synchronize the time of the SCS with that of the ProSafe-SLS. Bleeder resistors should be connected with the DI module in parallel to meet the minimum load current 35 mA of the DO module.

You have to prepare bleeder resistors of 730 ohm or less to do this.

A bleeder resistor of 680 ohm or less (5 W or 2 W) is recommended. When the 2-watt rated power resistor is used, the pulse width of the DO output must be set to one second or less.

Before any resistor other than the recommended one is used, please contact us.

SEE ALSO For more information about maximum length of the DI/DO cable connecting the SDV531/SDV541 and DI-511, refer to:

ProSafe-RS Outline of I/O Modules (for FIO) (GS 32P06K60-01EN)

Time synchronization setting

For the purpose of time synchronization, build an application logic, for the SCS, to output a time-setting pulse once a day.

The following list explains the configuration of ProSafe-SLS for time synchronization.

- Building a wired logic
  Build a wired logic so that a time-setting event is sent to the CO-920 from the DI module of ProSafe-SLS.
- Reflecting the COM-SET settings in CO-920
  COM-SET settings are as follows:
  - Selection of time setting method
  - Initial setting of date and time
    In COM-SET, set the initial time to which the CO-920 adjusts its time when a time-setting event occurs. Because the initial date and time are set for the purpose of time synchronization, they need not be set accurately.
  - Tag information settings
    In COM-SET, set the information of the tag that generates a time-setting event.

Mechanism of time synchronization

This section describes the mechanism of what happens after an application logic of the SCS is executed until the time of Pro-Safe SLS is synchronized with ProSafe-RS.

The following list shows an example where the time of the ProSafe-SLS is adjusted to that of the ProSafe-RS when the SCS's CPU time reaches time A.

1. When the SCS's CPU time reaches time A, the DO module (example of model: SDV531 or SDV541) of the SCS generates a pulse.
2. The pulse from the DO module is sent as an input to the DI module (model: DI-511) of ProSafe-SLS.
3. DI-511 sends an event, which is then received by the Digital Data Storage Module (model: MC-573).

4. MC-573 sends a time event to CO-920. CO-920 detects that it is a time event by checking the tag name that is contained in the event and sets its own clock to time A.

SEE ALSO For more information about engineering for time synchronization, refer to:

D4.14.3, “Engineering to configure applications on ProSafe-RS” on page D4-35

Time synchronization accuracy and calculation example

The accuracy of time synchronization of CO-920 with respect to the SCS depends on the output timing of the DO module of the SCS.

If time error is caused by the difference between the logic execution time and DO module output response time, time synchronization is always delayed by this time. If the time error is caused by other factors, time synchronization is slightly delayed or advanced.

The following list shows examples of time error calculation:

- Time error between the SCS and CO-920
  (SCS scan period) + (output response time of DO module) + (CO-920 scan period)
- Time error between CO-920s that are connected to the same SCS
  (CO-920 scan period)
- Time error between CO-920s that are connected to different SCSs
  (SCS scan period) + (CO-920 scan period)

D4.6 Alarm notification

The diagnostic information and events of ProSafe-SLS are not sent to the CENTUM system operator or ProSafe-RS as alarms or events. In order to send them to CENTUM HIS as alarms, build an application that evaluates the diagnostic information and data that are read from CO-920 and sends alarms by using annunciator FBs as necessary. If you create an application that uses SOE FBs, you can view the events through the SOE Viewer of CENTUM HIS.

From CO-920, the SCS can acquire the self-diagnostic information of Y-net and each module in ProSafe-SLS, the available space in the event buffer of CO-920 and other diagnostic information. The diagnostic information of CO-920 indicates the current statuses and values, and these statuses and values are retained while an error is present.

Alarms relating to the subsystem communication between the SCS and ProSafe-SLS are sent to HIS as subsystem communication system alarms, and to SENG, as diagnostic information messages.

To acquire diagnostic information from CO-920, perform engineering of CO-920 from COMSET.

For each system configuration, you must consider how errors should be determined by using the diagnostic information of CO-920 and how the determination result should be used. Perform engineering so that error alarms and recovery alarms are sent to the operator.

SEE ALSO

For more information about communication error code, refer to:

"■ Communication error code" on page D2-3

For more information about engineering for CO-920, refer to:

IM of ProSafe-SLS

D4.7 Communication specifications

This section describes the application capacity and transmission specifications that are required to build a system that uses the ProSafe-SLS communication function.

Application capacity

When you use the ProSafe-SLS communication function, you must determine the I/O data, diagnostic information, and events of ProSafe-SLS that are managed by ProSafe-RS. The following table shows the maximum capacity that is allowed for each application element.

Table D4.7-1 Application capacity

Application element	Maximum capacity	Description
Number of ALR121 that can be installed per SCS	4	(*1) (*2)
Number of communication data units per SCS	2000 or 500 data units (*3)	This specifies the number of data items that can be wired to subsystem communication FB instances. Maximum 256 words (4096 bits) are allowed for the total assignment size of discrete input/output.
Communication I/O size per SCS	1000 words	A word holds two bytes.
Size of data that can be communicated per ALR121	1000 words	-
Number of ports per ALR121	2 ports	-
Number of subsystem stations that SCS can communicate with per port	30 stations	One CO-920 is considered as a station.
Number of communication definitions per ALR121	Number of definitions that satisfies the following formula: (Number of SLSEVENT type communication definitions) x 2 + (Number of non-SLSEVENT type communication definitions) ≤ 128	-
Data size for event acquisition per ProSafe-SLS	24 words	To acquire the events from ProSafe-SLS, you must assign 24 words of communication definition for event acquisition per ProSafe-SLS.

*1: Total number of ALR111/ALR121/ALE111 for the subsystem communication that is mounted to the same SCS
*2: Communication modules for the Modbus slave communication and DNP3 communication are not included in the count.
*3: 2000 data units for SCSP3, SCSL2, SCSP2, SCSP1, SCSU1, and 500 data units for SCSV1.

Transmission specifications

The following table shows the transmission specifications for RS-485 communication that must be met in order to implement the ProSafe-SLS communication function.

Table D4.7-2 Transmission specifications

Setting items	Recommended setting	Required setting	Selection
Interface	-	RS-485	RS-422, RS-485

Continues on the next page

Table D4.7-2 Transmission specifications (Table continued)

Setting items		Recommended setting	Required setting	Selection
RS-422/RS-485 2-wire/4-wire		4-wire	-	2-wire, 4-wire
Transmission method		-	-	Half-duplex
Synchronization method		-	-	Start-stop synchronization
Baud rate (bps) (*1)		19200	-	1200, 2400, 4800, 9600, 19200, 38400
Transmission protocol		-	-	Modbus protocol (RTU mode)
Transmission code		-	-	Binary
Data type	Start bit	-	-	Fixed to 1.
	Data bit	-	8	7, 8
	Parity	Even (*2)	-	None, even, odd
	Stop bit	-	-	Fixed to 1.
Control line	RS control	-	-	Not used
	DR check	-	-	Not used
	CD check	-	-	Not used
Time monitoring	Transmission enable monitoring time	-	-	1000 ms
	Reception inter-character timer (ms)	10 (*3)	-	10 to 99999
	Generate an error upon detection of an inter-character monitoring timeout.	Do not generate an error (*3)	-	Do not generate an error
Text frame	Reception start character	-	-	None
	EOT character	-	-	None
XON/XOFF control		-	-	None
Response timeout (sec)		4	-	0 to 99
Communication retry		1 time	-	0 to 99 times
Interval of connection retries (sec)		30	-	0 to 999
Transmission wait time		-	-	1 sec
Option 1		-	-	Not used
Option 2		-	-	Not used
Option 3		-	-	Not used
Option 4		-	-	Not used

*1: The baud rate of the CO-920 is initially set to a value that is not included in the options. Ensure that the baud rate that is set for the CO-920 is the same as this baud rate setting.
*2: The initial setting of CO-920 parity is "None." It is recommended to set a parity to improve reliability. Ensure that the parity setting of the CO-920 matches this parity setting.
*3: Completion of reception is detected as an inter-character timeout. Setting a longer time for the inter-character timer delays the time to reception completion. As a guide, the timer is set to approx. 10 ms at 9600 bps. 10 ms corresponds to the time required for sending 10 characters when the baud rate is 9600 bps.

D4.8 ProSafe-SLS devices that SCS can access

With ProSafe-SLS communication, a device type is specified to access internal data in CO-920. The following list describes the types of devices:

- Bit devices
  Every bit of this data has a meaning.
- Word devices
  Every word of this data has a meaning. One word consists of 16 bits.
- Extended device
  Extended devices are specific to Modbus equipment. In CO-920, extended devices are those devices whose event data is stored in time series.

Communication module of ProSafe-SLS (model: CO-920) can be accessed from an external system according to the Modbus protocol (RTU mode).

Use standard Modbus commands to access the analog input module and digital I/O module of ProSafe-SLS from ProSafe-RS.

To access the devices, set "Device Address" and "Size" in the Safety Communication I/O Editor or Communication I/O Builder. The address format is as follows:

<Function code> + <Device type> + <Address within device>

To specify input relays 100012 to 100015, for example, set A100012 for "Device Address" and 1 for "Size." "A" of A100012 indicates a function code, "1" indicates a device type, and "00012" indicates an address within device.

The following table shows the devices that can be used in connection with the ProSafe-SLS communication function, address, and the Modbus protocol function code.

Table D4.8-1 Bit devices list

Device	Address			Modbus protocol function code (hexadecimal)	
	Function code	Device types of CO-920	Internal address of CO-920 device (to the extent specifiable)	Read	Write
Coil	A	0	00001-65536	01	0F
	B				05
	X			-	0F
	Y				05
Input relay	A	1	00001-65536	02	-

Table D4.8-2 Word devices list

Device	Address			Modbus protocol function code (hexadecimal)	
	Function code	Device types of CO-920	Internal address of CO-920 device (to the extent specifiable)	Read	Write
Input register	A	3	00001-65536	04	-

Continues on the next page

Table D4.8-2 Word devices list (Table continued)

Device	Address			Modbus protocol function code (hexadecimal)	
	Function code	Device types of CO-920	Internal address of CO-920 device (to the extent specifiable)	Read	Write
Holding register	A	4	00001-65536	03	10
	B				06
	C				10
	X			-	10
	Y				06
	Z				10

Meaning of function code

The meaning of each function code is as follows. The size is specified in the Safety Communication I/O Editor or Communication I/O Builder.

- A
  Read data for the specified size.

  Write data for the specified size. Readback is supported.
- B
  Read data for the specified size.

  Write data individually to each modified device in units of 1 bit for a bit device, or in units of 16 bits for a word device. With readback.
- C
  Read data for the specified size.

  Write data individually to each modified device in units of 32 bits. With readback.
- X
  Write data for the specified size when a change occurs. Readback is not supported.
- Y
  Write data individually to each modified device for the size of each device when a change occurs. Without readback.
- Z
  Write data individually to each modified device in units of 32 bits when a change occurs. Without readback.

List of function codes

The following table describes the function codes.

Table D4.8-3 List of function codes

Function code	Device	Read	Write	Readback
A	Bit devices	All data for one communication definition	All data for one communication definition	Yes
	Word devices	All data for one communication definition	All data for one communication definition	Yes

Continues on the next page

Table D4.8-3 List of function codes (Table continued)

Function code	Device	Read	Write	Readback
B	Bit devices	All data for one communication definition	In units of 1 bit	Yes
	Word devices	All data for one communication definition	In units of 16 bits	Yes
C	Word devices	All data for one communication definition	In units of 32 bits	Yes
X	Bit devices	-	All data for one communication definition	No
	Word devices	-	All data for one communication definition	No
Y	Bit devices	-	In units of 1 bit	No
	Word devices	-	In units of 16 bits	No
Z	Word devices	-	In units of 32 bits	No

If readback is enabled, data is read from ProSafe-SLS, and the read data is written to the SCS if the specified data type is "Input Specification." If the data type is "Output Specification," the read data is compared against the SCS data and sent to ProSafe-SLS if the data does not match.

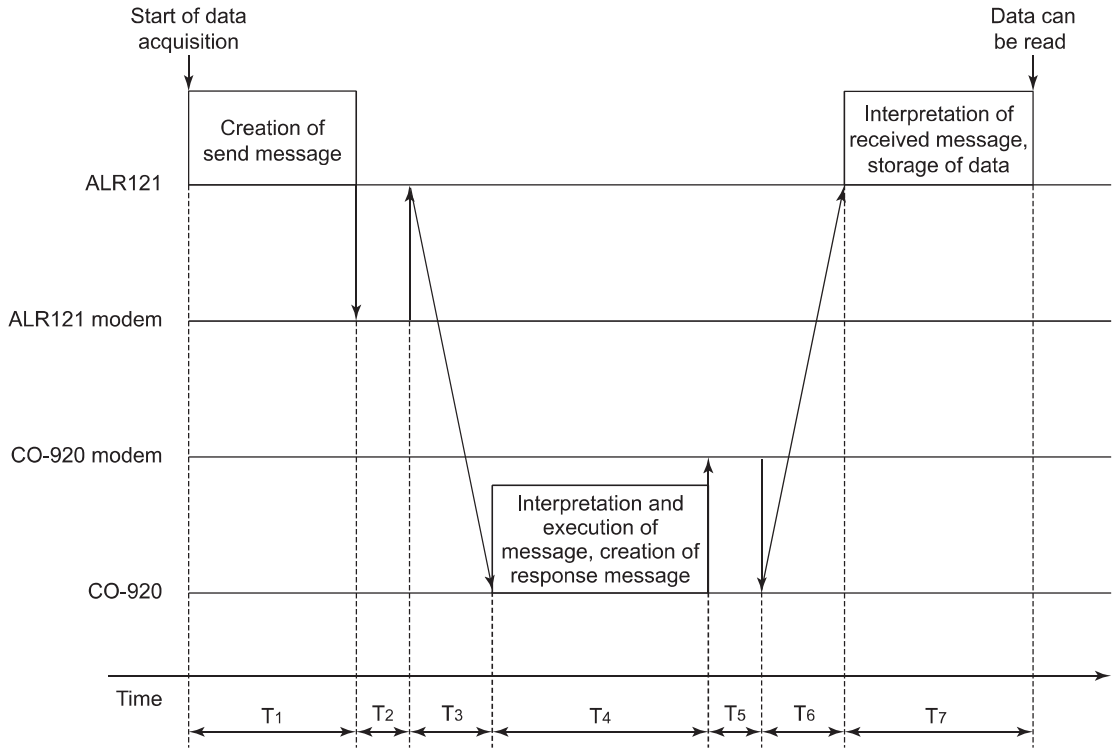
If readback is disabled, the SCS data is compared against the ALR121 data, and the data is sent to ProSafe-SLS only if a discrepancy is found.

SEE ALSO For more information about readback, refer to:

- "■ About readback communication operations" on page D2-33
- D2.5, "Readback communication" on page D2-20

D4.9 Communication time between communication module and CO-920

The communication time between the communication module of ProSafe-RS (model: ALR121) and CO-920 is the total period from T1 to T7 as shown in the following figure.



T1: Time for creating a send message: Approx. 10 ms
T2: Delay time of the ALR121 modem: Approx. 5 ms
T3: Time for transmitting the send message.
T4: Processing time in the Modbus PLC.
Time for interpreting and executing the received message and creating a response message.
Determined by the number of communication data items and number of scans performed by the Modbus PLC.
T5: Delay time of the Modbus PLC modem (T4 + T5): Approx. 3 ms
T6: Time for transmitting the response message.
T7: Time for interpreting the response message: Approx. 15 ms

Figure D4.9-1 Communication processing time in connection with the ProSafe-SLS communication function

The following shows how to calculate the communication time.

The transmission time for sending (T3) and receiving (T6) can be calculated by using the following formulas:

$$T3 \text{ or } T6 = \frac{1000 \times \text{Number of characters} \times \text{Number of bits per one character}}{\text{Baud rate}} \text{ (ms)}$$

Number of bits per one character = Number of start bits (1) + Number of data bits (8)
+ Number of parity bits (1)
+ Number of stop bits (1)

Start bit: Fixed at 1 bit
Data bits: Fixed at 8 bits (7 bits cannot be specified)
Parity bit: Set 1 if parity is even or odd, set 0 if parity is none
Stop bit: Fixed at 1 bit
Baud rate: 1200, 2400, 4800, 9600, 19200, 38400 bps

The following table shows the length of each frame that is transmitted by a Modbus-compliant device.

Table D4.9-1 Number of characters that can be transmitted

Device	Read		Write	
	Send	Response	Send	Response
Coil	Fixed to 8.	5 + Number of coils/ 8(*1)	9 + Number of coils/ 4(*1)	Fixed to 8.
Input relay	Fixed to 8.	5 + Number of relays/8(*1)	-	-
Input register	Fixed to 8.	5 + 2 x Number of registers	-	-
Holding register	Fixed to 8.	5 + 2 x Number of registers	9 + 2 x Number of registers	Fixed to 8.
Event	Fixed to 4.	5 + event (maximum 86)	-	-

*1: Fraction below the decimal point is rounded up.

D4.10 Data types handled by the ProSafe-SLS communication function

The following table shows the data types of subsystem communication that can be handled by the ProSafe-SLS communication function.

Table D4.10-1 Relationship between the data types of subsystem communication, and data types of the SO-920 and those of the SCS

Subsystem communication data type	CO-920 data type	SCS data type (subsystem communication FBs)
Discrete input	BOOL (bit)	SCI_B
Discrete output	BOOL (bit)	SCO_B
Analog input (16-bit unsigned integer)	16-bit unsigned integer	SCI_I
Analog output (16-bit unsigned integer)	16-bit unsigned integer	SCO_I
SLS event type	ASCII character string	N/A (*1)

*1: The SLS event type represents a data type used exclusively for acquiring ProSafe-SLS events. The SCS uses the SLS event type internally.
SLS events cannot be used in application logics.

D4.11 Message specifications

The SCS interprets the events that are acquired from ProSafe-SLS and stores them as SOE events. The stored events can be comprehensively managed with existing SCS events by using the SOE Viewer of SENG or SOE Viewer of CENTUM HIS.

The following table describes the event information that ProSafe-SLS issues.

Table D4.11-1 Event information issued by ProSafe-SLS

Event Information	ASCII format	Description
Event generation time	Set this information according to one of the following formats: • dd/mm/yyyy hh:mm:ss.msc • dd/mm/yy hh:mm:ss.msc The setting ranges for each element are as follows: dd: 01 to 31 mm: 01 to 12 yy: 00 to 99 yyyy: 0000 to 9999 hh: 00 to 23 mm: 00 to 59 ss: 00 to 59 msc: 000 to 999	Year, month, day, hours, minutes, seconds and milliseconds indicating when the event occurred. The description format of year varies depending on the format set for event character strings.
Tag name of ProSafe-SLS	ASCII character string with 25 characters Any empty digit in the 25-character tag name is filled by the ASCII character code 0x20 (SP).	ProSafe-SLS tag names associated with data at the source. The first 22 characters of the tag name of ProSafe-SLS are imported into the SOE of ProSafe-RS.
Description	ASCII character string with 25 characters Any empty digit in the 25-character description is filled by the ASCII character code 0x20 (SP).	Supplemental information regarding the tag name of ProSafe-SLS. This information is not imported into the SOE of ProSafe-RS.
Status	1 character type: 0 to 1 10 character type: 0 to 65535 The end of the 10-character status is filled by two space characters. Also, any non-character part at the beginning or end is filled by the ASCII character code 0x20 (SP).	Data value upon event generation. The range of values is as follows. 10 character type: 0 to 65535 1 character type: 0 or 1. (*1) When performing engineering on the CO-920, determine whether to use the 10 character type or 1 character type.

*1: Any 10-character value between 1 and 65535 is expressed as 1 based on the 1 character type.

Event information displayed on SOE Viewer

The SCS acquires ProSafe-SLS event information and displays it in the SOE Viewer. The following table shows the event information displayed in the SOE Viewer.

Table D4.11-2 SOE Viewer event information

Item	Description	Acquisition source of event information		
		CO-920	SCS	Subsystem communication function
Time Stamp	Date and time the event occurred Set the date format in the SOE Viewer Properties dialog box. The following format displays time: hh:mm:ss:ttt The meaning of each element is as follows: hh: Time (24 hours) mm: Minute ss: Second ttt: Millisecond	Event generation time	-	-
Quality	Empty	-	-	-
Type	SOER (fixed)	-	-	-
ID	EVT_TRUE (fixed)	-	-	-
Resource	Station name (SCSddss)	-	Station name	-
Reference (*1)	Node number (1 to 9, a to e, 1 hexadecimal character)	-	Node number	-
	Slot number (1 to 8, 1 character)	-	Slot number	-
	Port number (1 to 2, 1 character)	-	-	Port number
	Station number (01 to ff, 2 hexadecimal characters)	-	-	Station number
	Tag name of ProSafe-SLS (maximum 22 characters)	Tag name of ProSafe-SLS (first 22 of 25 characters)	-	-
Message	Data value (DINT type)	Status	-	-

*1: Display format: "SLS [Node number] [Slot number] [Port number] - [Station number]:[ProSafe-SLS tag name]"

Event display example of SOE Viewer and COM-SET

Assume that the ALR121 that is installed in slot 3 of SCS0101 node 10 acquired an event from the ProSafe-SLS of station number 24 that is connected to port 1 at 18 hours 30 minutes 15 seconds 123 milliseconds on February 24, 2015. Examples of how this is displayed in the SOE Viewer and on the COM-SET are provided in this section.

TIP

Empty fields in the table indicate that nothing is displayed for that item.

The tag name and value of the ProSafe-SLS event are DI511_1 and 1, respectively.

Table D4.11-3 Display example of SOE Viewer

Timestamp	Quality	Type	ID	Resource	Reference	Message
02/24/2015 18:30:15.123		SOER	EVT_TRUE	SCS0101	SLSa31-18:DI-511_1 (*1)	1

*1: "a" in hexadecimal notation indicates that the node number is 10. "18" in hexadecimal notation indicates that the station number is 24.

Table D4.11-4 Display example of COM-SET

Date/Time (*1)	Tag Name	Tag Description	Status
24/02/2015 18:30:15.123	DI-511_1	TAG1	1

*1: The specific value varies depending on the set format of event character string.

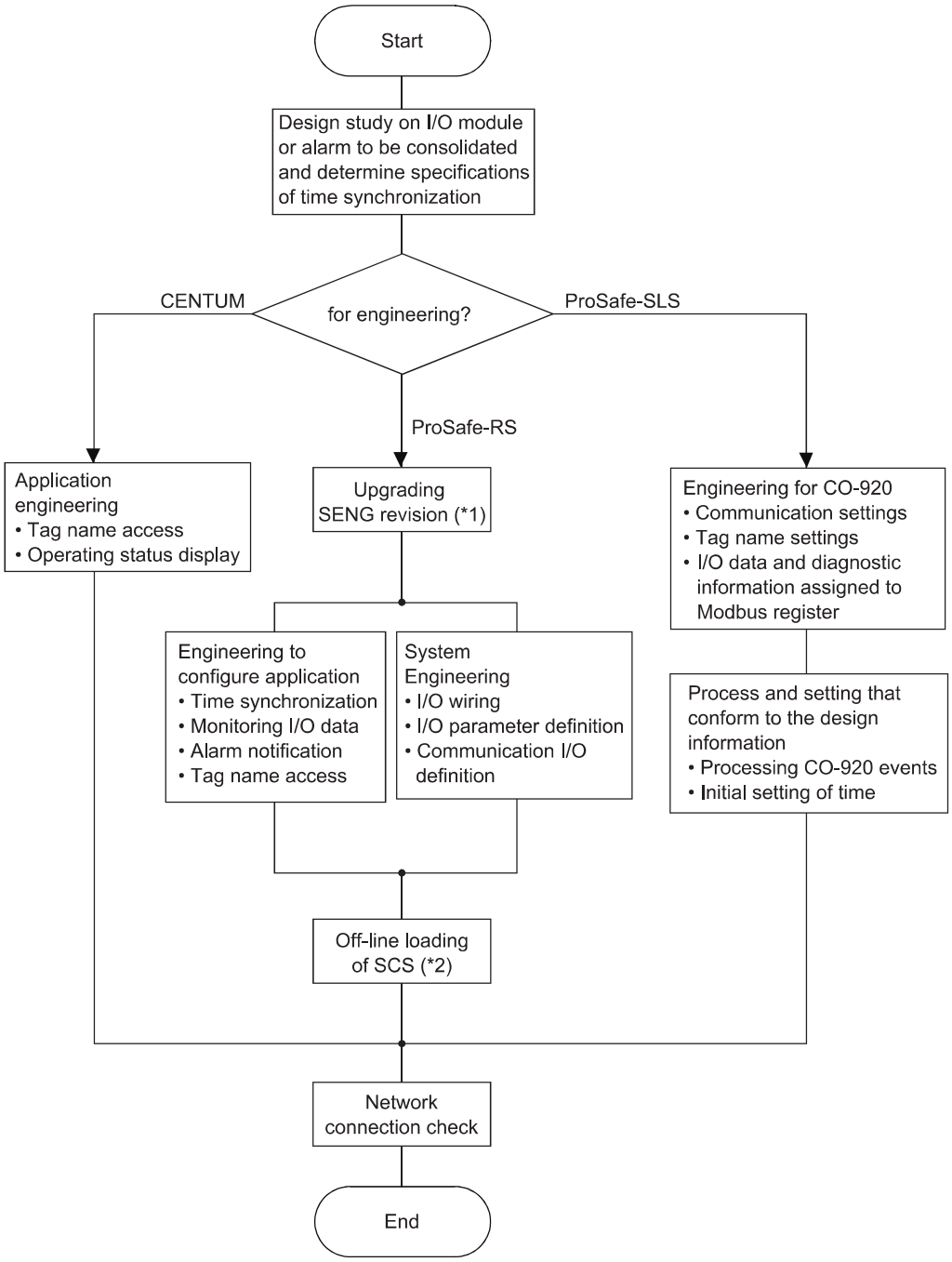
D4.12 Engineering flow and builders to be used

The following table shows the builders that must be set to use the ProSafe-SLS communication function.

Table D4.12-1 Related builders and window

Purpose	Name and builders and window	Role
Engineering	IOM Definition Editor or I/O Wiring View	Definition of communication device
	IOM Definition Editor or I/O Parameter Builder	Selection of communication program
		Setting of transmission definitions for each port
	Safety Communication I/O Editor or Comm. I/O Definition tab of Communication I/O Builder	Definition of communication definition
	Safety Communication I/O Editor or Comm. I/O Wiring tab of Communication I/O Builder	Assignment of communication I/O FB to communication data
Maintenance	Communication I/O Lock Window	Reference of logical data and physical data values of I/O variables. Execution of the Forcing function.

The following figure shows the engineering flow to be followed in order to implement the ProSafe-SLS communication function.



*1: You do not need to upgrade the revision for a new project. If you intend to upgrade the revision of existing project to use ProSafe-SLS functions, you must perform offline download.

*2: If you have performed offline download of the project database in R3.02.20 or later, you can perform online download.

Figure D4.12-1 Engineering flow for ProSafe-SLS communication function

SEE ALSO

For more information about Communication I/O Lock Window, refer to:

F8.11, “Communication I/O Lock window” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about AD Suite settings, refer to:

D., “Procedures to create applications using the I/O list engineering method” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about I/O Parameter Builder setting, refer to:

D1.4.1, “Settings using the I/O Parameter Builder” on page D1-22

For more information about communication I/O Builder setting, refer to:

D1.4.2, “Settings using the Communication I/O Builder” on page D1-28

For more information about engineering of subsystem communication modules using Safety Communication I/O Editor, refer to:

D1.5, “Engineering for subsystem communication modules” on page D1-37

D4.13 Determining ProSafe-SLS data to be managed by ProSafe-RS

When you use the ProSafe-SLS communication function, you must determine the I/O data, diagnostic information, events, and time synchronization of ProSafe-SLS that are managed by ProSafe-RS.

D4.13.1 Determination of data and event and diagnostic information of ProSafe-SLS to monitor

Internal error information of ProSafe-SLS and CO-920 are collectively referred to as diagnostic information of ProSafe-SLS. You must determine the diagnostic information of ProSafe-SLS that you want to monitor on ProSafe-RS. Diagnostic information can be handled as both Modbus communication data and events.

Errors of devices connected to ProSafe-SLS can also be handled as Modbus communication data and events.

Monitoring the data of ProSafe-SLS-connected devices

When handling the data of the devices that are connected to ProSafe-SLS, follow these instructions during engineering from COM-SET.

- In "Taglist part" of the TAG file of CO-920, enter the tag name to be monitored as information of the connected device.
- Set the "Data acquisition area (DAR)" field of the tag name to "YIS".

Determining diagnostic information of ProSafe-SLS to monitor

Diagnostic information of CO-920 includes self-diagnosis information of Y-net and each module in the ProSafe-SLS, available space of event buffer and other information of the CO-920. The diagnostic information of the CO-920 indicates the current statuses and values, and these statuses and values are retained while an error is present.

Some diagnostic information of ProSafe-SLS changes even when an error does not occur, and if such information is to be monitored as events, important events may remain unnoticed. Among the diagnostic information of ProSafe-SLS, therefore, make sure the following items are monitored:

- Communication status of COM port
- Y-net network integrity

If you want to select other items, investigate the need to do so by referring to the ProSafe-SLS manual.

Monitoring changes in diagnostic information of ProSafe-SLS

If the SCS receives diagnostic information of ProSafe-SLS through Modbus communication and diagnostic information changes multiple times at a rate faster than the communication cycle of the Modbus communication, the ALR121 may not be able to acquire the changes in diagnostic information, causing some missing data. Even the alarm notification application cannot send an alarm related to missing data.

Missing data will not occur at the SOE so long as diagnostic information of ProSafe-SLS is an input to the SCS as SLS events. In this case, SOE events are recorded even when no alarm is sent based on Modbus communication data.

To input changes in the applicable diagnostic information as SLS events, enable event generation when you set information on the tag names corresponding to the applicable diagnostic information of CO-920. To be specific, when performing engineering from the COM-SET, set the "Generate event" field of the tag name to monitor as diagnostic information, at "Taglist part" in the TAG file on the CO-920, to "Y."

After event generation is permitted, SOE is logged at the timing of a change on diagnostic information. On SOE Viewer, the tag name is indicated on Reference.

D4.13.2 Determining the time for time synchronization

To use the ProSafe-SLS communication function, time synchronization between ProSafe-SLS and SCS must be triggered by the output pulse from SCS once a day at a certain time. You need to specify the time for synchronization separately on ProSafe-SLS and SCS. Determine the time in universal time coordinated (UTC) before you start engineering.

D4.14 Engineering ProSafe-RS

This section describes the preparation and engineering of the ProSafe-RS that are required to use the ProSafe-SLS communication function.

D4.14.1 Preparation

If the software release number of ProSafe-RS is R3.02.10 or before, you must upgrade it to R3.02.20 or later.

TIP

The ProSafe-SLS communication function can also be used in existing SCS projects. After you upgraded SENG to R3.02.20 or later, you must specify related definitions to build and run offline download.

D4.14.2 System engineering of ProSafe-RS

This section describes the settings for ProSafe-RS wiring and builders required to use the ProSafe-SLS communication function. The following views and builders are used to configure the settings:

With RS original engineering

- I/O wiring view
- I/O parameter builder
- Communication I/O builder

With I/O list engineering

- IOM Definition Editor
- Safety Communication I/O Editor

When performing I/O list engineering, the views and builders used with RS original engineering will be display-only.

This section mainly describes for the case when performing RS original engineering. The setting item names displayed may differ between I/O list engineering and RS original engineering, but the settings are the same.

Setting the I/O Wiring View

Define "ALR121M" for the slots in which ALR121 is installed for the ProSafe-SLS communication.

ALR121 used for the ProSafe-SLS communication function supports only non-redundant configuration.

Set "IsRedundant" to "FALSE."

Setting the I/O Parameter Builder

On Module tab, set "Connection Device" to "S_SLSMOD."

Note the following points when setting the Port1 tab and Port2 tab:

- Ensure that communication settings for each ALR121 port match those for CO-920.
- "Baud Rate" on CO-920 is set to 57600 bps by default and not supported by the ProSafe-RS, thus the baud rate for CO-920 may need to be set again.
- "Parity" is set to "Even" by default. "None" is set to CO-920 by default. To ensure the communication reliability, "Even" is the recommended Parity setting to ALR121 and CO-920.
- Ensure that "Data Bits" is always set to 8 bit because Modbus protocol (RTU mode) is applied for communications.
- Set "2-Wire/4-Wire" according to the connection method for RS-485 communications between ALR121 and CO-920.
- You can leave the following items to the default setting:

  "Reception Inter-Character Time", "Response Timeout", "Communication Retry" and "Interval of Connection Retries"
- "Option1" to "Option4" are not applied to the ProSafe-SLS communication function. Set them to 0 on a constant basis.

Setting the Communication I/O Builder

To enable an SCS to acquire I/O data, diagnostic information and events from CO-920, set communication I/O definitions while considering the limitation on application capacity.

For Program Name, you must specify "S_SLSMOD", which is the program to communicate with ProSafe-SLS.

TIP

If any of the following conditions applies, you must correct the program name in the communication I/O builder. Otherwise, a build error will occur.

- The "Connection Device" definition of the ALR121M was changed in the I/O parameter builder
- The ALR121M defining the S_SLSMOD was deleted and the ALR111M was created at the same installation position by using the I/O wiring view

The following table describes the data types that you can assign in the communication I/O definitions.

Table D4.14.2-1 Accessible data types for ProSafe-RS through SLS communication function

Data type	Description
Input (16-Bit Unsigned)	Analog input (16-bit unsigned integer)
Output (16-Bit Unsigned)	Analog output (16-bit unsigned integer)
Input (Discrete)	Discrete input
Output (Discrete)	Discrete output
SLSEVENT	Event type applicable only in S_SLSMOD

Input (16-Bit Unsigned), Output (16-Bit Unsigned), Input (Discrete) and Output (Discrete) are assigned to the communication I/O definition in the same procedures as those in S_MODBUS.

When you assign SLSEVENT to a communication I/O definition, you must ensure that the following conditions are met:

- One Station Number of each port accepts only one definition.
- The size must be 24 words.
- Set the address of other devices to "SLSEVENT."

D4.14.3 Engineering to configure applications on ProSafe-RS

You must configure applications for time synchronization, I/O data monitoring, and alarm notification. Engineering for access by tag name is required to enable data monitoring through CENTUM HIS.

Configuring an application for time synchronization

To perform time synchronization between ProSafe-SLS and ProSafe-RS, configure an application on ProSafe-RS enabling ProSafe-RS DO module to output the trigger once a day to ProSafe-SLS DI module. Settings of Trigger, for example rising and/or falling edge of pulse must match the Trigger of time synchronization events on CO-920.

Example of application on ProSafe-RS

The following figure shows an example of application logic to output trigger from the SCS DO module at 3:00 universal time coordinated (UTC) every day.

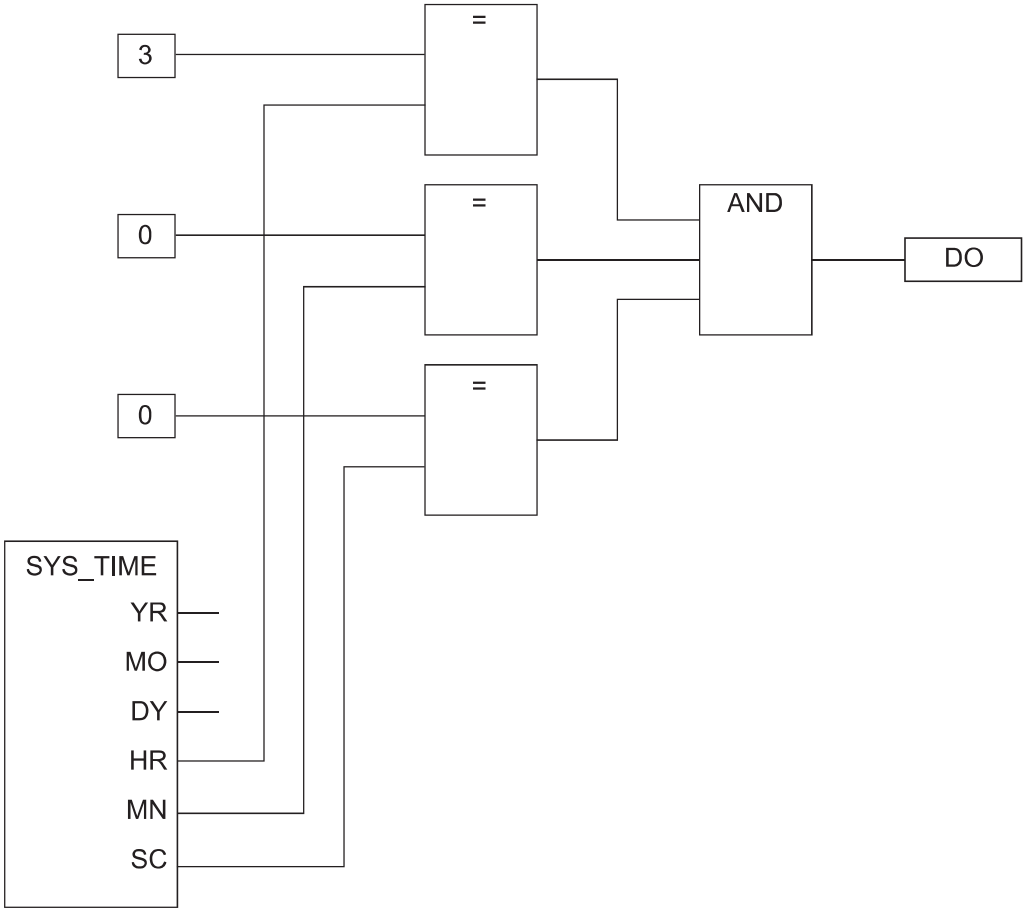


Figure D4.14.3-1 Example of creating an application logic to output trigger for time synchronization from DO

To apply the application logic provided as an example for time synchronization, engineering is required on ProSafe-SLS.

Example of engineering on ProSafe-SLS

On the ProSafe-SLS side, you must create the following application for time synchronization. You must set the time to Coordinated Universal Time (UTC).

1. Define a DI that applies the rising edge of pulse input as a time setting event to DI module on ProSafe-SLS.
2. The application must set the time of ProSafe-SLS to 3:00 when the rising edge of DI pulse is detected.

Engineering to monitor I/O data

The I/O data acquired from ProSafe-SLS can be handled as subsystem communication data on ProSafe-RS. On ProSafe-RS, create an application to monitor the subsystem communication data.

In order to enable monitoring on HIS, you must also create an application for integration with CENTUM.

Configuring an application for alarm notification

The following figure shows an example of ProSafe-RS application that notifies an alarm to HIS at an error of a certain I/O module on ProSafe-SLS and that outputs recovery alarm.

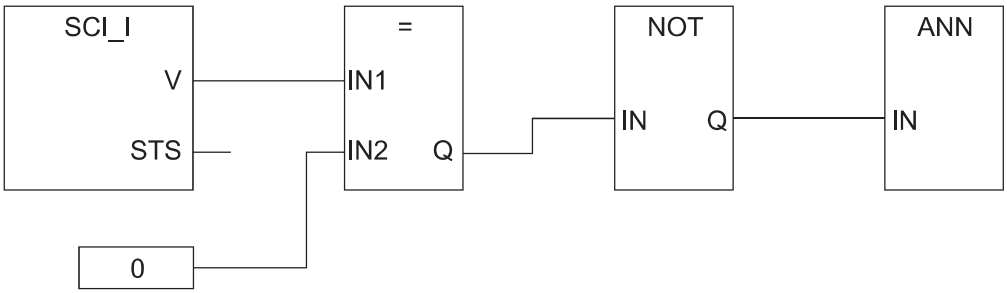


Figure D4.14.3-2 Example of application to notify ProSafe-SLS error alarm

This application uses an SCI_I function block to read the data status of a certain I/O module as a DINT-type value.

The DINT value is non-zero when the I/O module has failed and while the module remain failed. The value becomes 0 when the module recovers.

Engineering for tag name access

To enable CENTUM HIS to access I/O data acquired from CO-920, you must define tag names on SENG.

D4.15 Engineering for ProSafe-SLS

You must perform the following tasks for ProSafe-SLS engineering:

- Initial configuration required to operate CO-920
- Processing of events in CO-920
- Initial time setting of CO-920
- Engineering required to set the time by DI input

D4.15.1 Initial configuration required to operate CO-920

You can use COM-SET to edit the communication setting file and tag name setting file in order to perform initial configuration required to operate CO-920.

Flow of initial configuration of C-920

Follow these steps to configure CO-920 by using COM-SET:

1. Connect COM-SET to the RS-232C port of CO-920.
2. Edit CNF file and TAG file, and compile the edited texts on COM-SET.
3. Download the compiled binary data from COM-SET to CO-920.
4. After the download is complete, reset and restart CO-920 from COM-SET. Communication between the ALR121 and CO-920 is disabled while the CO-920 is being reset and restarted. If CO-920 is running, you must be careful for any affects on a system of upstream connection.

Setting communication

When you set the communication for CO-920 and SCS, you must ensure that the communication parameters of CO-920 and SCS match.

Among communication settings, you must be careful particularly with baud rate and parity settings.

SCS does not support the default baud rate settings (57600 bps) for CO-920. By default, the parity setting of CO-920 is None, which is different from the default setting of SCS (Even).

Editing the CNF file

The CNF file contains I/O data, diagnostic information, time synchronization and the information relative to communication settings of each port and they are described in System part, Communication part, and Data acquisition part.

System part

In communication with ProSafe-RS, set External Clock to "Y" and Time to the target time for time synchronization from SCS. Make Trigger slope match to DO wave that is applied to the trigger for time synchronization on SCS.

Communication part

In Communication part, make sure to include the descriptions of the setting information related to the RS-232C port (COM1), RS-422/RS-485 ports (COM2, COM3) and event text formats.

Modbus slave address is equivalent to Station Number for subsystem communication on ProSafe-RS. It must match the Station Number that is set at ProSafe-RS engineering.

Baud rate, Word length, Parity, and Stop bits are communication settings of RS-485. You must ensure that these settings match the subsystem communication settings specified during ProSafe-RS engineering.

For Event format, we recommend that you use Format 11, which does not contain Description and has 10-character status string.

Data acquisition part

In Data acquisition part, you must set the behavior of CO-920 when it acquires data from each I/O module.

Set the Module type, Network address, and I/O type for each YIS-net module that is installed.

Editing the TAG file

The TAG file contains the Description corresponding to tag name and the information about Modbus register assignment for Tag name monitored on ProSafe-RS and they are described in Taglist part.

Setting items of Taglist part and their details are provided as follows:

- I/O data or Tag name for diagnostic information is set to TAG_NAME. Recommended maximum characters are 22 for a Tag name because SOE on SCS reads up to 22 characters. Duplicate tag names are not permitted within one CO-920.
- The SOE of the SCS does not read TAG_DESCRIPTION. Include the necessary information in the tag name.
- Specify the data source or the initial value of the corresponding Tag name to TAG_SOURCE.
- Specify the Modbus register address to which Tag name is assigned to TAG_LOGIC_ADDRESS. Each TAG_LOGIC_ADDRESS corresponds to the Logic address of Modbus register that is set on CNF file.

You must consider the previous descriptions and ensure that the following requirements are satisfied to set ProSafe-SLS tag name.

- Maximum 22 characters are allowed.
- Overview of an event can be determined.

Assigning I/O data to Modbus register

Assign the I/O data of ProSafe-SLS monitored on ProSafe-RS to Modbus register on CO-920.

Assigning diagnostic information to Modbus register

If you need to send alarms when errors are detected in ProSafe-SLS, assign diagnostic information of ProSafe-SLS to the Modbus register on CO-920. Create an SCS application that references this information and sends an alarm when the judgment shows an error.

D4.15.2 Processing of events in CO-920

If events are stored on CO-920 before events are acquired from ProSafe-RS, SCS requires a long time to acquire events. To avoid slow event acquisition, process the events according to the policy during design study.

TIP

For example, ALR121 contains communication definitions as much as the maximum application capacity and event acquisition runs only for one communication definition, approximately maximum 15 hours is expected for SCS to acquire 10000 events from a CO-920.

Acquiring or deleting events stored in CO-920

SCS starts acquiring at the event next to the last one acquired from CO-920.

If you do not need the events that ProSafe-SLS generated before you connect ProSafe-RS, acquire all events from COM-SET and delete them in advance.

How to acquire events that are stored in CO-920

Before you connect SCS to CO-920, connect COM-SET to the maintenance port (COM1) of CO-920 and acquire all events from CO-920.

TIP

Even though all events are acquired from the maintenance port (COM1) of CO-920, locations of event read pointer for COM2 and COM3 remain unchanged.

If you connect a system for event acquisition to COM2 and COM3 and acquire events, the events on CO-920 disappear.

Events are stored in the rotary buffer on CO-920 and they remain until they are overwritten with new events.

How to delete events that are stored in CO-920

On COM-SET menu, select [ProSafe-SSCC] > [Reset] to delete all events.

This action resets CO-920 and CO-920 cannot communicate with ProSafe-RS for several seconds.

D4.15.3 Initial time setting of CO-920

You must use Coordinated Universal Time (UTC) when you perform time setting engineering to use the SLS communication function.

Before you connect DO module on SCS to DI module on ProSafe-SLS for time synchronization, you must specify year, month, day, hour, minute, and second from COM-SET to CO-920 to make CO-920 time match to SCS time. The time to match should be specified according to the information in the design study.

If time synchronization is performed between SCS and ProSafe-SLS, CO-920 receives DO output from SCS as a trigger and corrects the time to the predefined time. When this happens, the date is corrected within 12 hours gap between the current time and the setting time. For that reason, the time difference between SCS and CO-920 must be less than 12 hours before time synchronization is performed.

The following figure shows an image of correcting date.

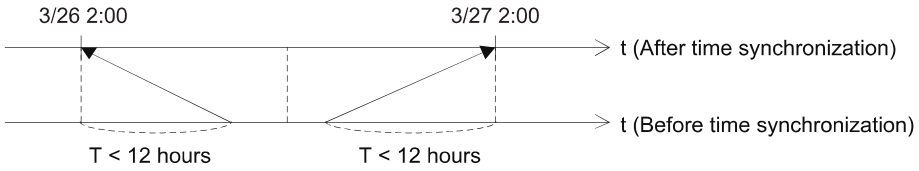


Figure D4.15.3-1 Image of correcting date

D4.15.4 Engineering required to set the time by DI input

If you want to use the application logic for time synchronization created on ProSafe-RS to perform time synchronization for ProSafe-SLS, you also need to perform engineering on ProSafe-SLS.

D4.16 Engineering for CENTUM

If your system is integrated with CENTUM, you must perform engineering to enable access by tag name and build an application to display the operating status so that the ProSafe-SLS communication function can be used.

Tag name access

To attain the access to tag names that are assigned to I/O data of CO-920 and defined in ProSafe-RS, perform the tag name access engineering.

Configuring application to show operating status

Because the ProSafe-SLS and CO-920 are devices on the other end of subsystem communication for the SCS, they are not displayed in the operating status display windows of the HIS and SENG. If necessary, engineer the CENTUM Integrated System so that, for example, ProSafe-SLS or CO-920 data that is read by using subsystem communication is determined and displayed in graphics accordingly.

D4.17 Application Examples of the ProSafe-SLS communication function

The ProSafe-SLS communication function cannot directly send diagnostic information of ProSafe-SLS or errors in devices that are connected to ProSafe-SLS as alarms. ProSafe-SLS events are acquired and recorded as SOE events of the SCS, but they are not sent as alarms to HIS. You can refer to these events through the SOE Viewer or the SOE OPC server.

To notify the operator, as alarms, of diagnostic information of ProSafe-SLS or errors of devices connected to ProSafe-SLS, you must enable such data to be acquired from the CO-920 as Modbus communication data. In addition, create in the SCS a determination logic that uses this data, and create an application that uses the ANN FB or annunciator FB to notify the operator of error alarms and recovery alarms.

Application to send ProSafe-SLS alarms to HIS

The SCS judges the diagnostic information that is read from CO-920 and device data connected to ProSafe-SLS as Modbus communication data. For the system integrated with CENTUM, you can send the judged results of the SCS to HIS by using annunciator FBs. HIS handles the received alarms as process alarms.

By configuring CO-920 to generate an event when the value of the diagnostic information associated with the corresponding alarm has changed, you can manage changes in the diagnostic information as events.

The following figure shows an example of how an alarm is sent to HIS when there is an error in ProSafe-SLS.

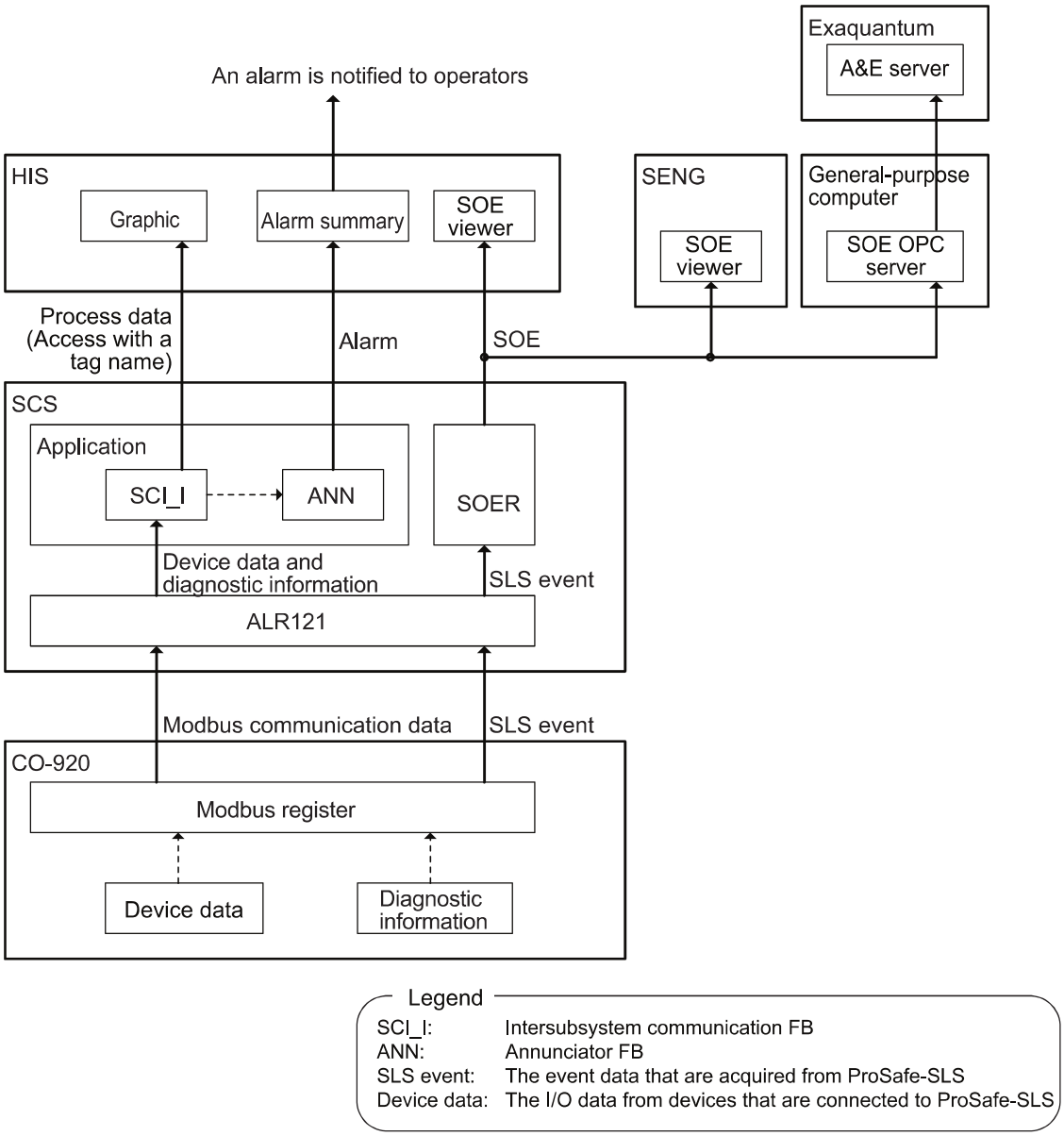


Figure D4.17-1 Example of how to send ProSafe-SLS alarms to HIS

Application to send ProSafe-SLS alarms to CI Server or FAST/TOOLS

In the CI Server integration environment, you must create an application on CI Server that enables CI Server to acquire, through SCS, the diagnostic information of CO-920 and data of devices that are connected to the ProSafe-SLS, judge them, and send alarms to the operator. In the FAST/TOOLS integration environment, create a similar application on FAST/TOOLS.

The following figure shows an example of an application that prompts the CI Server to notify ProSafe-SLS alarms to the operator in the CI Server integration environment.

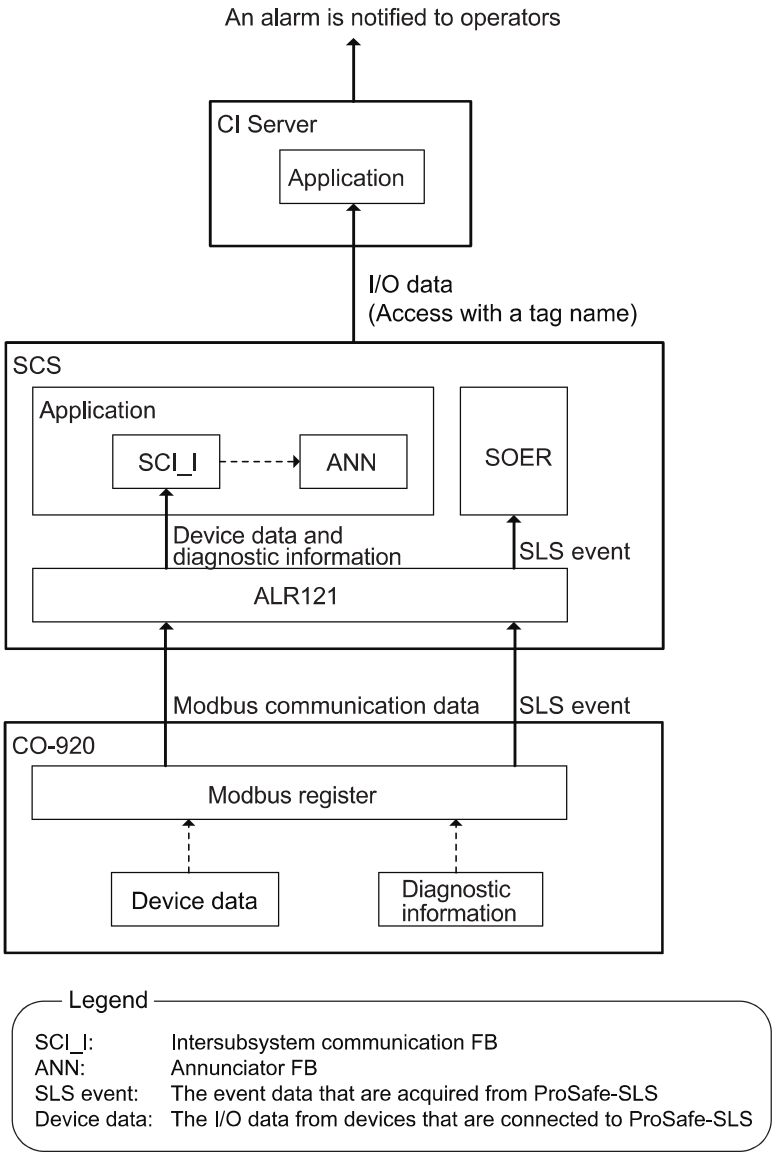


Figure D4.17-2 Example of notifying ProSafe-SLS alarms to CI Server

Application to indicate ProSafe-SLS alarms by using field devices

You can notify users of ProSafe-SLS alarms by using field devices such as alarm lamps. In such a case, you must create an application that sends the result of diagnostic information judged by SCS from a DO module to the field devices.

The following figure shows an example of how to indicate ProSafe-SLS alarms by using field devices.

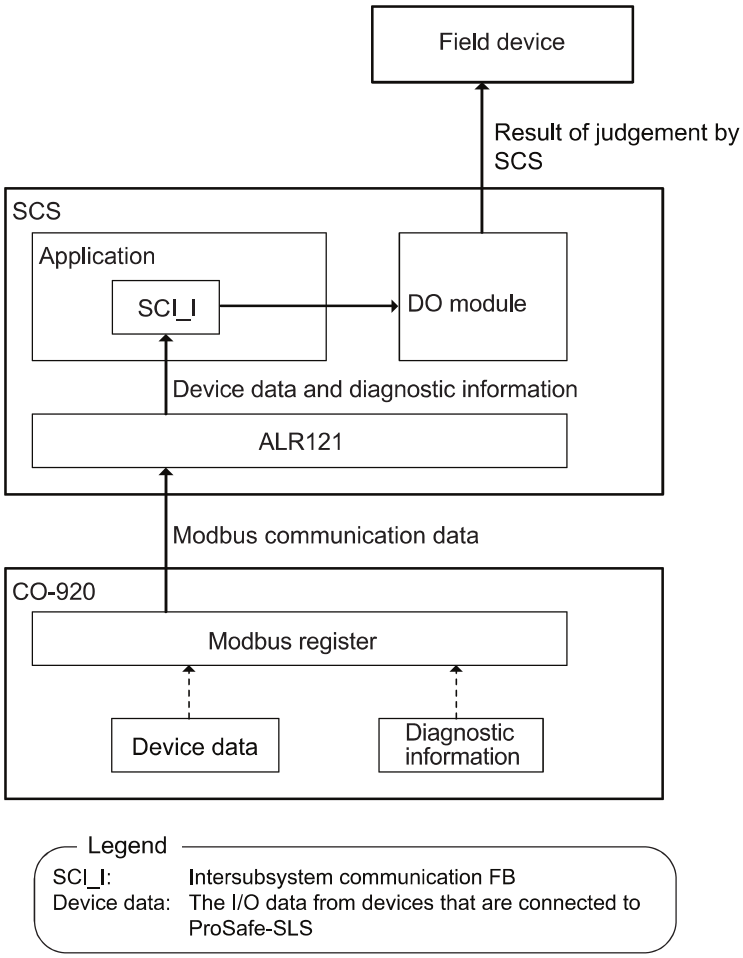


Figure D4.17-3 Example of how to indicate ProSafe-SLS alarms by using field devices

E. Safety subsystem communication

Safety subsystem communication is a function for safe communication where the safety control station (hereinafter referred to as SCS) of ProSafe-RS behaves as the master and communicates with subsystem devices that support safety subsystem communication.

Safety subsystem communication includes fire and gas communication.

E1. Fire and gas communication

Fire and gas communication is a function where the S2LP131 fire and gas communication module is installed on the SCS (SCSP3) to implement safe communication between the SCS and GS01 wireless gas detectors through the YFGW410 field wireless management station and YFGW510 field wireless access point.

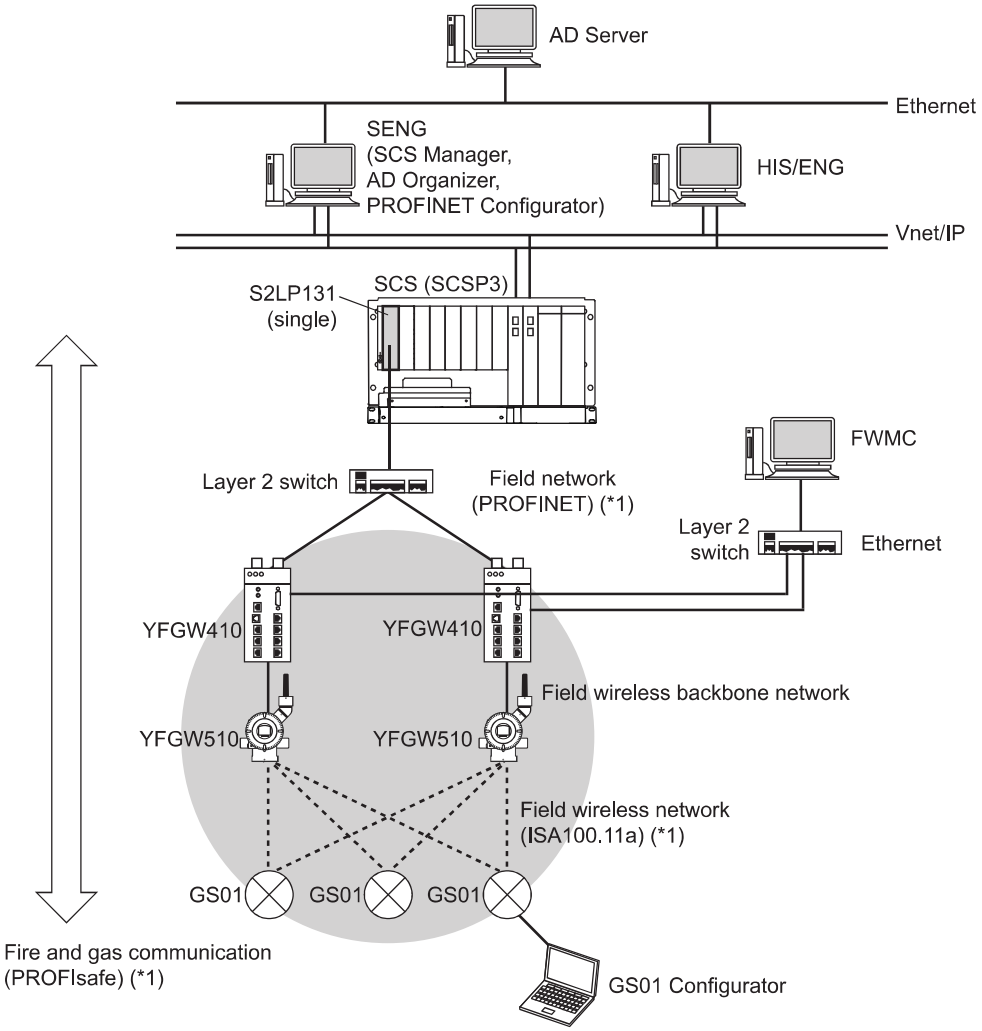
Fire and gas communication handles non-safety data used with interference-free functions in addition to safety data used with safety communication.

E1.1 System overview

This section describes the system configuration, components, structure of functions, and operating environment required for fire and gas communication.

E1.1.1 System configuration and components

The following figure shows an example of a configuration for the fire and gas communication system.



*1: For fire and gas communication, PROFINET is used as the field network between SCS and YFGW410 and ISA100.11.a as the field wireless network. In addition, the PROFIsafe protocol is used for the safety layer of fire and gas communication.

Figure E1.1.1-1 Fire and gas communication system configuration example

This section describes the components used in fire and gas communication.

SCS

You can realize safe fire and gas communication between the SCS and GS01 wireless gas detectors by installing the S2LP131 fire and gas communication module on the SCS (SCSP3). Communication with GS01 wireless gas detectors is routed through the YFGW410 field wireless management station and YFGW510 field wireless access point. The gas concentration of a safe GS01 can be handled as input data for a safety application by using fire and gas communication. In addition, you can also obtain interference-free diagnosis information of the YFGW410, YFGW510, and GS01.

S2LP131

S2LP131 is a communication module for fire and gas communication. S2LP131 is installed on the SCS and can connect to multiple YFGW410 through layer 2 switches. (*1) Communication between S2LP131 and YFGW410 uses the PROFINET protocol. Note that you cannot use S2LP131 in a dual-redundant configuration.

*1: Layer 2 switches used with PROFINET must be compliant with the PROFINET installation standards.

SENG

SENG is configured of AD Organizer and SCS Manager. Engineering for fire and gas communication uses AD Organizer to define S2LP131 and communication I/O. In addition, you can set the parameters used by PROFINET and PROFIsafe by using PROFINET Configurator started from AD Organizer. You can display the operating status and alarm messages by using SCS Maintenance Support Tool for maintenance of fire and gas communication.

HIS/ENG

When ProSafe-RS is integrated with CENTUM, you can display the operating status and alarm messages related to S2LP131 in the operation and monitoring windows on HIS.

AD server

AD server is a server that manages engineering data.

YFGW410

YFGW410 is a field wireless management station compliant with wireless communication standard ISA 100.11a. In addition to configuring and managing field wireless networks, it has a gateway function for accessing wireless field devices from the ProSafe-RS system. When communicating with wireless gas detector GS01, access is made through YFGW410. You can use YFGW410 in a dual-redundant configuration.

SEE ALSO

For more information about how to use YFGW410, refer to:

YFGW410 Field Wireless Management Station (IM 01W02D01-01EN)

For more information about how to use the PROFINET interface of YFGW410, refer to:

YFGW410 PROFINET Interface (IM 01W02D01-21EN)

For more information about how to configure PROFINET, refer to:

PROFINET installation guide / security guide issued by PROFIBUS & PROFINET international

YFGW510

YFGW510 is a field wireless access point compliant with wireless communication standard ISA 100.11a. Ethernet is used for the connection between YFGW410 and YFGW510. YFGW410 accesses GS01, which is a wireless field device, through YFGW510.

TIP

An optical network communication option is available with YFGW510, which enables connection to YFGW410 through the YFGW610 field wireless media converter, which is an optical network / metal network converter. This is effective in cases when YFGW410 is far away from YFGW510, when the noise environment is poor, and when measures against lighting are required.

SEE ALSO For more information about how to use YFGW510, refer to:

YFGW510 Field Wireless Access Point (IM 01W02E01-01EN)

For more information about how to use YFGW610, refer to:

YFGW610 Field Wireless Media Converter (IM 01W02D02-01EN)

FWMC

FWMC (Field Wireless Management Console) is a console for YFGW410 and is configured of a configurator and monitor which are used for the following purposes:

- Configurator
  Engineering for constructing a field wireless system
- Monitor
  Status monitoring of YFGW410, YFGW510, and wireless field devices configuring a field wireless system

The configurator is also used for mapping of PROFINET and wireless definitions for fire and gas communication with upper level controllers.

SEE ALSO For more information about how to use FWMC, refer to:

- YFGW410 Field Wireless Management Station (IM 01W02D01-01EN)
- YFGW410 PROFINET Interface (IM 01W02D01-21EN)

GS01

GS01 is a GasSecure AS wireless gas detector compliant with wireless communication standard ISA100.11a. GS01 has acquired SIL2 and uses the PROFIsafe protocol for the safety layer.

GS01 Configurator

You can use GS01 Configurator for provisioning in relation to GS01 and to set safety parameters.

SEE ALSO For more information about how to use GS01 and GS01 Configurator, refer to:

GS01 user's manual from GasSecure AS

E1.1.2 Structure of functions

The following figure shows the structure of fire and gas communication functions.

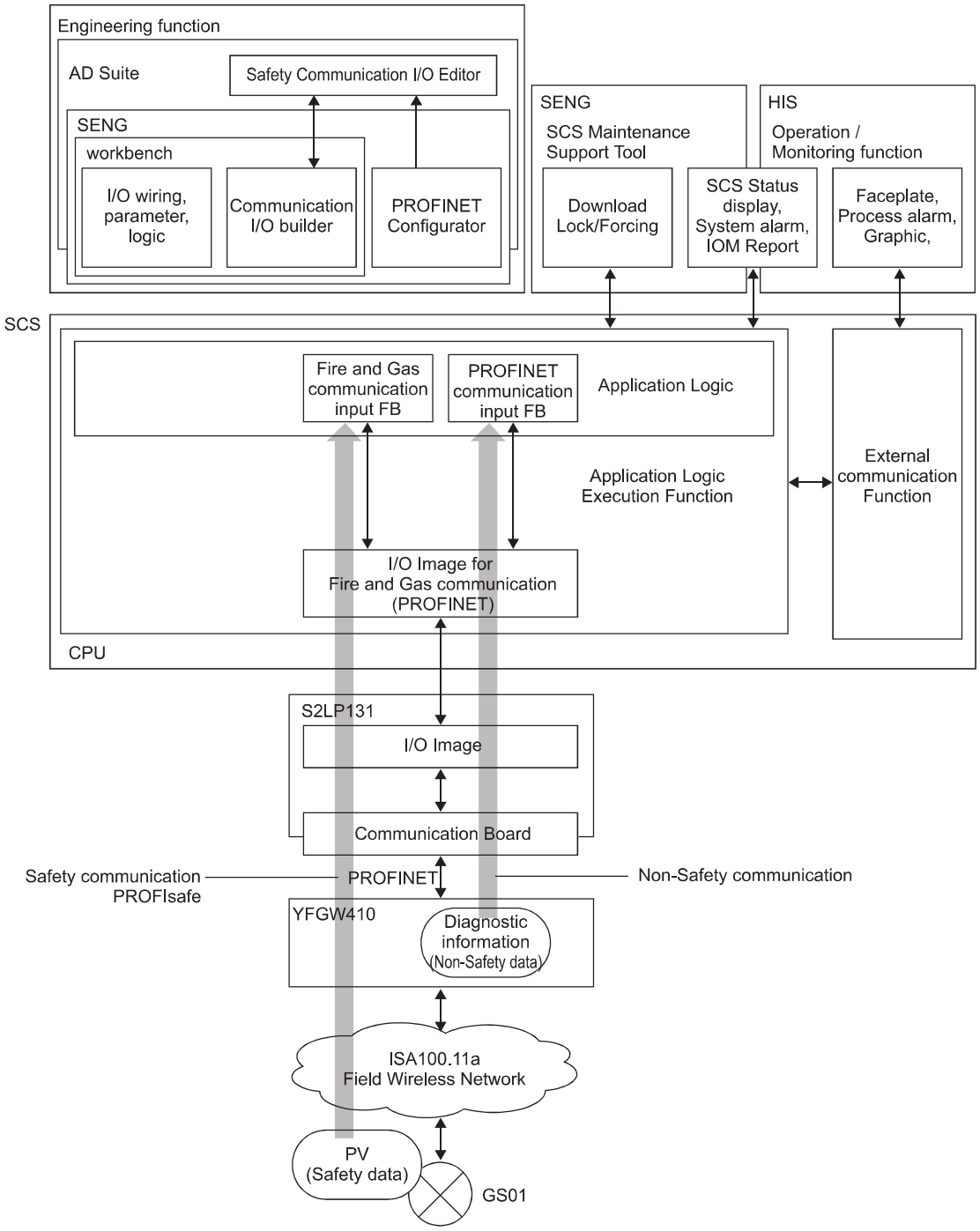


Figure E1.1.2-1 Structure of fire and gas communication functions

S2LP131

S2LP131 passes on the I/O data sent and received with PROFINET communication between YFGW410 as the I/O image for fire and gas communication of the SCS.

Application logic execution function (CPU)

The application logic execution function involves the CPU of the SCS accessing S2LP131 and exchanging data through the PROFINET communication I/O data area.

I/O data comprises safety data communicated using the PROFIsafe protocol (PV), and non-safety data (YFGW410, YFGW510, and GS01 diagnosis information). Safety data is data used with safety communication. Non-safety data is data used with interference-free functions.

Safety data is entered into the fire and gas communication input FB through the safety layer (PROFIsafe). Non-safety data is entered into the interference-free PROFINET communication input FB.

In addition, the application logic execution function performs downloads to S2LP131 and status monitoring of S2LP131 and notifies alarm messages.

When ProSafe-RS is integrated with CENTUM, you can access the I/O data from HIS through the external communication function.

Engineering function (SENG, AD Suite)

With the engineering function, you can use Safety Communication I/O Editor of AD Suite to define S2LP131 and start PROFINET Configurator and Communication I/O Builder.

You can use PROFINET Configurator to set the parameters of PROFINET and PROFIsafe to S2LP131.

When creating a safety application, you can use the fire and gas communication input FB and then use the gas concentration information obtained from GS01 with the safety application.

The database created with these definitions are downloaded to the SCS and S2LP131.

You can also create a PROFINET-ISA100 mapping file from the wireless definition information exported from YFGW410. By importing the PROFINET-ISA100 mapping file, you can set the assignment of the PROFINET modules set on the SCS to YFGW410.

Operation and monitoring function (HIS, SENG)

With HIS and SENG, the operating status of S2LP131 and system alarms are displayed.

By defining tag names with SENG, you can display I/O data values of S2LP131 on HIS through access to the SCS using the tag names.

With SENG, you can perform IOM download to S2LP131 and obtain IOM reports for trouble analysis. In addition, when performing maintenance or making an online change, you can perform locking or forcing of I/O data handled by S2LP131.

E1.1.3 Operating environment

The hardware environment and software environment required for the fire and gas communication function are as follows:

- Hardware environment

  Station: S2SC70S, S2SC70D

  Communication module: S2LP131 fire and gas communication module

  Can be installed on an CPU node, I/O node

- Software environment

  ProSafe-RS: R4.03.10 or later

  CENTUM VP: R6.05 or later

  YFGW410: Firmware Rev R2.01.04 or later

E1.2 Fire and gas communication function specifications

Fire and gas communication is a function for safety communication between the SCS and GS01 through YFGW410 and YFGW510 from the S2LP131 installed on the SCS.

PROFINET is used for communication between the S2LP131 and YFGW410. With PROFINET, S2LP131 of the SCS acts as the PROFINET IO-controller while YFGW410 acts as the PROFINET IO-device.

ISA100.11a is used for communication between YFGW510 and GS01.

PROFIsafe is used for safety communication between the SCS and GS01. With safety communication between the SCS and GS01, devices such as S2LP131, YFGW410, and YFGW510 as well as networks such as PROFINET and ISA100.11a are handled as communication paths.

This section explains PROFINET.

E1.2.1 Data I/O function of PROFINET

With PROFINET, communication is conducted by exchanging data between the PROFINET IO-controller and the PROFINET IO-device.

The following figure illustrates the flow of I/O data in PROFINET.

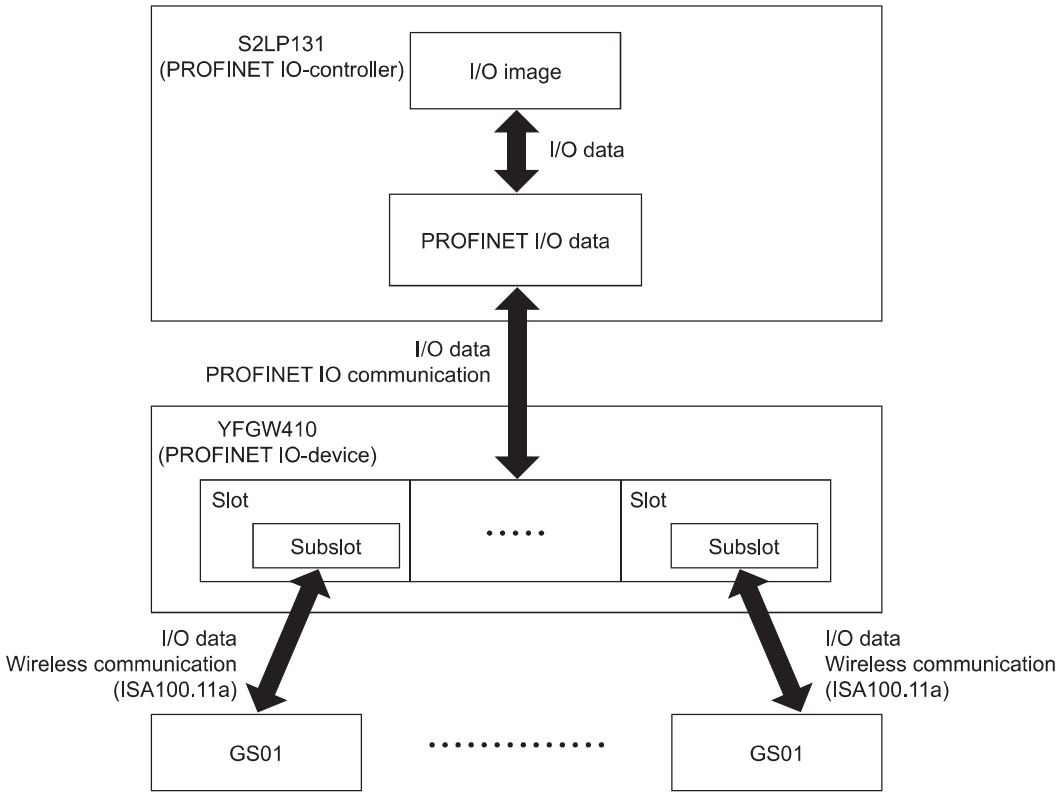


Figure E1.2.1-1 Flow of I/O data in PROFINET

In order to exchange data, input data is periodically forwarded from the PROFINET IO-device to the PROFINET IO-controller while output data is forwarded from the PROFINET IO-controller to the PROFINET IO-device. I/O data exchanged is assigned to addresses referred to as PROFINET slots and subslots.

Input data from GS01 is assigned to YFGW410 slots and subslots.

With S2LP131, input data of GS01 is read from the YFGW410 slots and subslots according to definition information set using AD Suite.

I/O data is first stored in the PROFINET I/O data area of S2LP131, and then stored in the I/O image area where SCS can reference and set data.

E1.2.2 PROFINET modules used with fire and gas communication

With PROFINET, the I/O data used in the data exchange is referred to as modules (hereinafter referred to as PROFINET modules). With fire and gas communication, you can define the PROFINET modules to acquire by using PROFINET Configurator.

The following table shows the PROFINET modules used with fire and gas communication.

Table E1.2.2-1 PROFINET modules used with fire and gas communication

Module ID	Data type	Description
GS01_SAFE_RS	• Input (Unsigned 8 + Float 32 + information for Safety Measure of PROFIsafe) • Output (Information for Safety Measure of PROFIsafe)	PV value (gas concentration) protected with PROFIsafe. The range of WD_Time is set for ProSafe-RS connections.
DIAG_STATUS	Input (Unsigned 32)	GS01 self-diagnosis information. This is created by GS01.
GW_STATUS	Input (Unsigned 16)	The operating status of YFGW410. This is created by YFGW410.
BBR_STATUS	Input (Unsigned 16)	The operating status of YFGW510. This is created by YFGW410.
BATTERY_LIFE	Input (Integer 16)	The remaining battery level of GS01. This is created by GS01.

For more information about the data structure and stored image, refer to the description of PROFINET modules.

TIP

S2LP131 is not compatible with the PROFINET module for output.

The following table shows the PROFINET modules that are not used with fire and gas communication.

IMPORTANT

Although the PROFINET modules in the following table will appear in PROFINET Configurator, do not use these with fire and gas communication.

Table E1.2.2-2 PROFINET modules not used with fire and gas communication

Module ID	Description
GS01_SAFE	Use GS01_SAFE_RS instead of GS01_SAFE.
GS01_SAFE_2	Use GS01_SAFE_RS instead of GS01_SAFE_2.
GS01_REGULAR	-
PV	-
OP	-
READBACK	-
PV_B	-
OP_B	-
READBACK_B	-

SEE ALSO For more information about how to operate PROFINET Configurator, refer to:

E1.5.2, “Applying settings by using PROFINET Configurator” on page E1-34

GS01_SAFE_RS

GS01_SAFE_RS is the PV value (gas concentration) protected with PROFIsafe of GS01. The following figure shows the data structure of GS01_SAFE_RS.

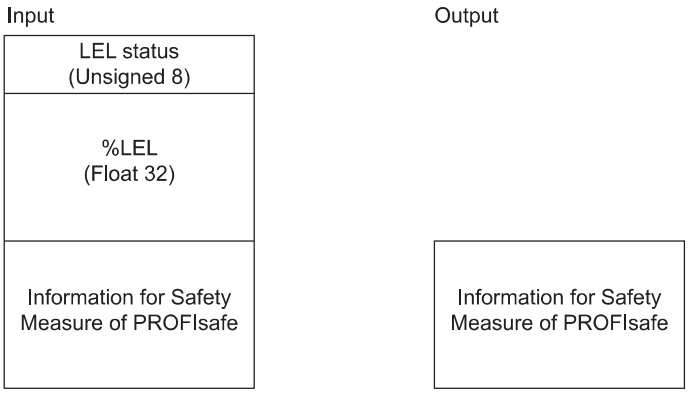


Figure E1.2.2-1 Data structure of GS01_SAFE_RS

When GS01_SAFE_RS is read, the gas concentration of GS01 is stored to SCS as follows.

%XWnnnn	0	LEL Status
%XWnnnn+1	0	
%XWnnnn+2 %XWnnnn+3	% LEL	
%XWnnnn+4 %XWnnnn+5 %XWnnnn+6 %XWnnnn+7	Information for Safety Measure of PROFIsafe	

nnnn: Odd number between 0001 and 3993 inclusive

Figure E1.2.2-2 GS01_SAFE_RS stored image

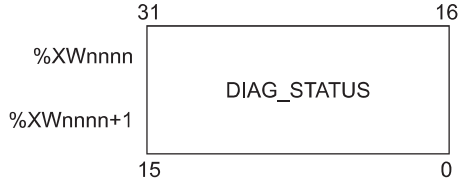
The meaning of each field of GS01_SAFE_RS data is as follows:

%LEL: The ratio of the concentration value to the LEL (Lower Explosion Limit) of the combustible gas expressed in percentage.

LEL Status: Information indicating the quality of the LEL

DIAG_STATUS

When the self-diagnosis information (DIAG_STATUS) of wireless field devices (GS01) is read, status information is stored in the SCS as follows.



nnnn: Odd number between 0001 and 3999 inclusive

Figure E1.2.2-3 DIAG_STATUS stored image

The following table describes the meaning of each DIAG_STATUS bit.

Table E1.2.2-3 Meaning of each DIAG_STATUS bit

Bits	Contents
Bit31 (MSB)	Failure status
Bit30	Function check status
Bit29	Out of specification status
Bit28	Maintenance required status
Bit27	Faults in electronics
Bit26	Faults in sensor or actuator element
Bit25	Installation, calibration problem
Bit24	Out of service
Bit23	Outside sensor limits
Bit22	Environment conditions out of device specifications
Bit21	Fault prediction: maintenance required
Bit20	Power is critically low: maintenance required immediately
Bit19	Power is low: maintenance required soon
Bit18	Software update incomplete
Bit17	Simulation is active
Bit16 to Bit08	Reserved by WCI
Bit07 to Bit01	Vendor specific area
Bit00	Detailed information available 1: available 0: not available

SEE ALSO For more information about GS01 self-diagnosis information details, refer to:

GS01 user's manual from GasSecure AS

GW_STATUS

When the device status (GW_STATUS) is read from a YFGW410 field wireless management station, status information is stored in the SCS as follows.

%XWnnnn	GW_STATUS
%XWnnnn+1	0

nnnn: Odd number between 0001 and 3999 inclusive

Figure E1.2.2-4 GW_STATUS stored image

The following table describes the meaning of each GW_STATUS bit.

Table E1.2.2-4 Meaning of each GW_STATUS bit

Bits	Contents
Bit15 (MSB)	GW1 Side Abnormal 0: Normal, 1: Abnormal

Continues on the next page

Table E1.2.2-4 Meaning of each GW_STATUS bit (Table continued)

Bits	Contents
Bit14	GW2 Side Abnormal (*1) 0: Normal, 1: Abnormal
Bit13 to Bit12	GW1 Side Status 0: Ready (initial status) 1: Active (operating as the active gateway) 2: Standby (operating as the standby gateway) 3: Not used
Bit11 to Bit10	GW2 Side Status (*2) 0: Ready (initial status) 1: Active (operating as the active gateway) 2: Standby (operating as the standby gateway) 3: Not used
Bit09	Field Wireless Device Status 0: Normal (All the wireless field devices are properly connected on the field wireless network.) 1: Abnormal (At least one wireless field device is not properly connected on the field wireless network.)
Bit08 to Bit00	Reserved Always 0

*1: If YFGW410 is in non-redundant configuration, GW2 Side Abnormal is 0.
*2: If YFGW410 is in non-redundant configuration, GW2 Side Status is 3.

BBR_STATUS

When the device status (BBR_STATUS) is read from a YFGW510 field wireless access point, status information is stored in the SCS as follows.

%XWnnnn	BBR_STATUS
%XWnnnn+1	0

nnnn: Odd number between 0001 and 3999 inclusive

Figure E1.2.2-5 BBR_STATUS stored image

The following table describes the meaning of each BBR_STATUS bit.

Table E1.2.2-5 Meaning of each BBR_STATUS bit

Bits	Contents
Bit15 (MSB)	Status of field wireless access point 0: Joined, 1: Not Joined
Bit14 to Bit00	Reserved Always 0

BATTERY_LIFE

When the remaining battery level (BATTERY_LIFE) of wireless field devices (GS01) is read, status information is stored in the SCS as follows.

%XWnnnn	BATTERY_LIFE
%XWnnnn+1	0

nnnn: Odd number between 0001 and 3999 inclusive

Figure E1.2.2-6 BATTERY_LIFE stored image

The following table shows the details of BATTERY_LIFE data.

Table E1.2.2-6 BATTERY_LIFE data details

Field name	Description
Remaining battery level	>0: Days, <0: Hours, 0x7FFF: Unlimited

E1.2.3 FB to connect to PROFINET modules

Use the FB shown in the following table when obtaining a PROFINET module with the SCS.

Table E1.2.3-1 FB to connect to PROFINET modules used with fire and gas communication

Module ID	Data type	FB	Description
GS01_SAFE_RS	Input (Unsigned 8)	PSI_I	Data quality status (*1) (*2)
	Input (Float 32)	PSI_R	Gas concentration (*2)
DIAG_STATUS	Input (Unsigned 32)	PNI_I	GS01 self-diagnosis information
GW_STATUS	Input (Unsigned 16)	PNI_I	Operating status of YFGW410
BBR_STATUS	Input (Unsigned 16)	PNI_I	Operating status of YFGW510
BATTERY_LIFE	Input (Integer 16)	PNI_I	Remaining battery level of GS01

*1: The data quality status is a value that indicates the quality of the gas concentration. This is defined by ISA100.11a.
*2: Define the signals of both the data quality status and gas concentration and wire the FB when obtaining GS01_SAFE_RS. Both signals are required in order to determine the quality of the gas concentration.

When multiple signals have been defined to a PROFINET module, engineer as follows:

- Register the signal you want to obtain in the I/O list.
- Register the signals of the same PROFINET module to the same communication definition.
- Wire a FB for every signal you want to obtain.

SEE ALSO

For more information about PSI_I details, refer to:

5.19, “PSI_I (integer-type fire and gas communication input)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about PSI_R details, refer to:

5.20, “PSI_R (real-type fire and gas communication input)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about PNI_I details, refer to:

8.6, “PNI_I (integer-type PROFINET communication input)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about PNI_R details, refer to:

8.7, “PNI_R (real-type PROFINET communication input)” in POU Reference Manual (IM 32P03B20-01EN)

E1.3 Safety communication of fire and gas communication

The I/O function of fire and gas communication performs safety communication between the CPU module of the SCS and GS01. With this function, you can incorporate the gas concentration, which is safety data of GS01, into the safety loop.

Similar to other I/O functions, the data I/O function used by fire and gas communication behaves as the SCS application logic execution function.

This section explains the safety communication of fire and gas communication.

E1.3.1 Flow of data for the fire and gas communication I/O

The I/O function of fire and gas communication involves the SCS accessing S2LP131 and obtaining safety data and non-safety data from GS01. You can reference data obtained from GS01 from the application logic through the FB.

Fire and gas communication I/O data consists of safety data and non-safety data. Safety data and non-safety data are obtained through the PROFINET modules used for data exchange on PROFINET.

The following table shows the PROFINET modules and the types of data.

Table E1.3.1-1 PROFINET modules and types of data

Module ID	Type of data	Description
GS01_SAFE_RS	Safety data	PV value (gas concentration) protected with PROFIsafe.
DIAG_STATUS	Non-safety data	GS01 self-diagnosis information.
GW_STATUS	Non-safety data	The operating status of YFGW410.
BBR_STATUS	Non-safety data	The operating status of YFGW510.
BATTERY_LIFE	Non-safety data	The remaining battery level of GS01.

Operating the data status

The SCS sets the data status of fire and gas communication. The behavior varies for safety data and non-safety data.

- Safety data
  The safety layer of the SCS confirms the safety communication with GS01. When an error is detected with the safety layer, the SCS sets the status of the safety data in the safety communication I/O data area to error.
- Non-safety data
  S2LP131 detects communication errors of the field wireless systems under YFGW410 and notifies these errors to the SCS. The SCS that has been notified with a communication error sets the status of the non-safety data in the safety communication I/O data area to error.

Conversion of real-type input data

When the safety communication I/O data is real-type input data and the value is Not-A-Number (NaN), infinity, or subnormal, the safety communication I/O data I/O function of SCS converts the physical data to logical data as shown in the following figure and pass it to the application Logic.

This processing is performed in common to both safety data and non-safety data.

However, only NaN is supported for the gas concentration of GS01.

Table E1.3.1-2 Data conversion for real-type input data with NaN, infinity, or subnormal values

Physical data	Logical data
Value: NaN Data status: GOOD	Value: pre-defined input value at fault Data status: BAD
Value: NaN Data status: BAD	

Continues on the next page

Table E1.3.1-2 Data conversion for real-type input data with NaN, infinity, or subnormal values (Table continued)

Physical data	Logical data
Value: infinity Data status: GOOD	Value: pre-defined input value at fault Data status: BAD
Value: infinity Data status: BAD	
Value: subnormal Data status: GOOD	Value: 0.0 Data status: GOOD
Value: subnormal Data status: BAD	Value: pre-defined input value at fault Data status: BAD

Display of NaN, infinity, or subnormal values

When the value of physical data of safety communication I/O data is NaN, infinity, or subnormal, the value is displayed in the Communication I/O Lock window as shown in the following table.

Table E1.3.1-3 Display format for physical data with a NaN, infinity, or subnormal value

Display format	NaN			Positive infinity	Negative infinity	Subnormal
Displayed with 5 decimal places	1.#QNAN	-1.#QNAN	-1.#IND0	1.#INF0	-1.#INF0	0.00000

E1.3.2 Data and status upon starting the SCS

Fire and gas communication is initialized when the SCS is started. The SCS completes start-up after waiting for the fire and gas communication startup time to elapse.

When fire and gas communication is restored prior to the fire and gas communication startup time elapsing, the status of the safety data related to GS01 upon startup of the SCS is set to GOOD.

When fire and gas communication is not restored even after the fire and gas communication startup time has elapsed, the status of the safety data related to GS01 upon startup of the SCS is set to BAD.

■ Fire and gas communication startup time

The fire and gas communication startup time is valid when S2LP131 is defined.

You can change the fire and gas communication startup time with Command Line on the SCS tab of SCS Constants Builder.

SEE ALSO For more information about fire and gas communication startup time details, refer to:

"● Command Line" in "■ SCS tab" in C1.2.6, "SCS Constants Builder" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

E1.3.3 Functions and roles of the safety layer

Safety data used with safety communication and non-safety data used with interference-free functions can be handled with the I/O function of fire and gas communication. Because fire and gas communication handles safety data, the safety layer within the SCS has a safety measure compliant with the PROFIsafe communication protocol.

The safety layer serves the following roles:

- Monitoring of fire and gas communication
- Passing of safety data to safety applications

Monitoring of fire and gas communication

The safety layer of the SCS monitors whether the SCS is receiving safety data from GS01 properly by fire and gas communication.

The validity of the safety data is checked by using procedures compliant with the PROFIsafe communication protocol. When a communication frame error occurs or safety data cannot be received properly for a certain amount of time, the SCS determines that a fire and gas communication error has occurred and alerts a system alarm.

Passing of safety data to safety applications

The SCS passes the safety data, obtained from the I/O image of S2LP131 and checked for validity, to the safety communication I/O data area so that it can be referenced from safety applications.

SEE ALSO For more information about differences between safety subsystem communication I/O, subsystem communication I/O, and AIO/DIO modules I/O, refer to:

Appendix 1.1, “Differences between safety subsystem communication I/O, subsystem communication I/O, and AIO/DIO modules I/O” on page App.1-2

E1.4 Monitoring of fire and gas communication

With fire and gas communication, S2LP131 monitors interference-free functions while safety functions are monitored by the safety layer of the SCS.

E1.4.1 Behavior when an error occurs

S2LP131 monitors the status of the devices used for fire and gas communication and the status of the communication path and notifies the status of normal or error to the SCS. When an error has occurred, a system alarm is alerted from the SCS. The system alarm that is alerted is an IOM Fail, Configuration Error, or SS-SCPATH Error.

The following table shows the relationship between the subjects of status monitoring by S2LP131, system alarms, communication definitions, and applications.

Table E1.4.1-1 Relationship between the subjects of status monitoring by S2LP131, system alarms, communication definitions, and applications

Monitoring subject		System alarm alerted upon error	Communication definition for alerting alarm	Application for monitoring
(1)	Status of S2LP131 (hardware, software errors)	IOM Fail	Not required	Not required
	Status of S2LP131 (configuration error) (*1)	IOM Fail and Configuration Error, or SS-SCPATH system alarm	Required	Not required
(2)	Status of communication board	IOM Fail	Not required	Not required
(3)	Status of communication with PROFINET IO-device	SS-SCPATH system alarms	Required	Not required
(4)	Status of YFGW410 (*2)	SS-SCPATH system alarms	Required	Not required
(5)	Status of YFGW510 (*3)	SS-SCPATH system alarms	Required	Not required
(6)	Communication status of GS01 (communication error)	SS-SCPATH system alarms	Required	Not required
	Status of GS01 (self-diagnosis error) (*4)	An alarm will not be alerted due to not be subject to monitoring.	Required	Required

*1: When the definition information downloaded to S2LP131 has any of the following errors, an IOM Fail and Configuration Error are alerted as the conditions for normally starting S2LP131 are not satisfied.
- IOM definition error (sum value error)
- Communication definition error (sum value error)
- PROFINET definition error (no definition, date discrepancy)

When the conditions for normally starting S2LP131 have been satisfied but the communication definition is invalid, an SS-SCPATH system alarm is alerted. Specifically, this is when a non-supported data type is used.

*2: When GW_STATUS is assigned to %XW, an SS-SCPATH system alarm regarding the YFGW410 error is alerted.

*3: When BBR_STATUS is assigned to %XW, an SS-SCPATH system alarm regarding the YFGW510 error is alerted.

*4: A system alarm will not be alerted when a self-diagnosis error occurs. When monitoring self-diagnosis errors of GS01, in addition to the DIAG_STATUS communication definition, you must build an application to monitor this communication definition. However, when an GS01 communication error, etc. occurs and DIAG_STATUS cannot be obtained, an SS-SCPATH system alarm in relation to the DIAG_STATUS communication definition will be alerted.

(1) Status of S2LP131

S2LP131 checks the following statuses of S2LP131 and notifies the SCS if there is an error.

- Self-diagnosis of S2LP131
- Errors or invalid definition information downloaded to S2LP131

(2) Status of communication board

S2LP131 checks the status of communication board and notifies the SCS if there is an error.

(3) Status of communication with PROFINET IO-device

S2LP131 checks the status of communication with the PROFINET IO-device and detects the following errors. The detected errors are notified to the SCS.

- PROFINET IO-device configuration discrepancy
- Unable to communicate with the PROFINET IO-device

- Error status of PROFINET

(4) Status of YFGW410

S2LP131 checks GW_STATUS and detects the following errors. The detected errors are notified to the SCS.

- GW1 system error
- GW2 system error
- Control right switched
- The active/standby operation of the redundant YFGW410 is unstable (which YFGW410 is active or standby is unknown).

(5) Status of YFGW510

S2LP131 monitors BBR_STATUS and detects the following errors. The detected errors are notified to the SCS.

- YFGW510 has not joined the network

(6) Communication status of GS01

S2LP131 monitors the communication status of PROFINET. If there is an error, an error code indicating the communication error with GS01 is notified to the SCS.

Behavior when a communication error occurs with YFGW410

When the dual-redundant YFGW switching time is set to a value other than 0 and S2LP131 detects a communication error with YFGW410, the communication error with YFGW410 will not be notified from S2LP131 to the SCS during the dual-redundant YFGW switching time. The dual-redundant YFGW switching time is valid only when using YFGW410.

Communication errors will not be notified in the following cases:

(1) Switching of a dual-redundant YFGW410 occurred

(2) A path error occurred between a dual-redundant YFGW410 and S2LP131

(3) A path error occurred between a single YFGW410 and S2LP131

The following table shows the details of safety data and non-safety data when a communication error has occurred. Cases (1) through (3) in the table correspond to Cases (1) through (3) when communication errors are not notified.

Table E1.4.1-2 Safety data and non-safety data when a communication error has occurred

Case		Safety data	Non-safety data
(1)	PROFINET communication is being restored during dual-redundant YFGW switching time	The value of the logical data retains the previous value. The data status of the logical data varies depending on whether an error has been detected with the Safety Measure of PROFIsafe by the safety layer of the SCS. • When an error has not been detected, the data status is GOOD. • When an error has been detected, the data status is BAD and an SS-SCOM system alarm is alerted.	The value of the logical data and the data status retains the previous value.
	When PROFINET communication is restored within the dual-redundant YFGW switching time	Update of the logical data resumes.	Update of the logical data resumes.
	When PROFINET communication is not restored within the dual-redundant YFGW switching time	The value of the logical data becomes the specified input value at error occurrence. The data status of the logical data becomes BAD at the timing when an error is detected with the Safety Measure of PROFIsafe by the safety layer of the SCS and then an SS-SCOM system alarm is alerted.	The value of the logical data becomes the specified input value at error occurrence, the data status becomes BAD, and an SS-SCPATH system alarm is alerted.
(2), (3)	During dual-redundant YFGW switching time	The value of the logical data retains the previous value. The data status of the logical data varies depending on whether an error has been detected with the Safety Measure of PROFIsafe by the safety layer of the SCS. • When an error has not been detected, the data status is GOOD. • When an error has been detected, the data status is BAD and an SS-SCOM system alarm is alerted.	The value of the logical data and the data status retains the previous value.
	After dual-redundant YFGW switching time	The data status of the logical data becomes BAD at the timing when an error is detected with the Safety Measure of PROFIsafe by the safety layer of the SCS and then an SS-SCOM system alarm is alerted. At that time, the value of the logical data becomes the specified input value at error occurrence.	The value of the logical data becomes the specified input value at error occurrence, the data status becomes BAD, and an SS-SCPATH system alarm is alerted.

Dual-redundant YFGW switching time

The dual-redundant YFGW switching time is the time it takes to switch YFGW410 when YFGW410 is in a dual-redundant configuration. Set a value to Dual-Redundant YFGW Switching Time in IOM Definition Editor of AD Suite. The value set in AD Suite is reflected into I/O Parameter Builder of SENG.

- Default value: 5 seconds
- Valid range: Integer between 0 to 99 seconds

IMPORTANT

- If all YFGW410 that connect to S2LP131 are of a single configuration, set the dual-redundant YFGW switching time to 0.
- Changes of the setting value for the dual-redundant YFGW switching time can be downloaded online to the SCS. However, S2LP131 restarts when you perform an online download to the SCS.

E1.4.2 Fire and gas communication status notification

Errors related to fire and gas communication are notified with the system alarms of safety subsystem communication path errors (SS-SCPATH Error) and safety subsystem communication errors (SS-SCOM Error).

TIP

Errors related to fire and gas communication are not notified with the system alarms of existing subsystem communication errors (SS-COM Error).

SEE ALSO

For more information about I/O module errors, refer to:

Message Number 0081 in 3.1, “Safety Control Station Error Occurrence and Recovery Messages (Message Numbers 0001 through 0094)” in Messages Reference Manual (IM 32P02B10-01EN)

For more information about SS-SCOM Error details, refer to:

Message Number 4209 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)

For more information about SS-SCPATH Error details, refer to:

Message Number 4211 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)

Scope of SS-SCPATH Error and SS-SCOM Error monitoring

The following figure shows the scope of SS-SCPATH Error and SS-SCOM Error monitoring.

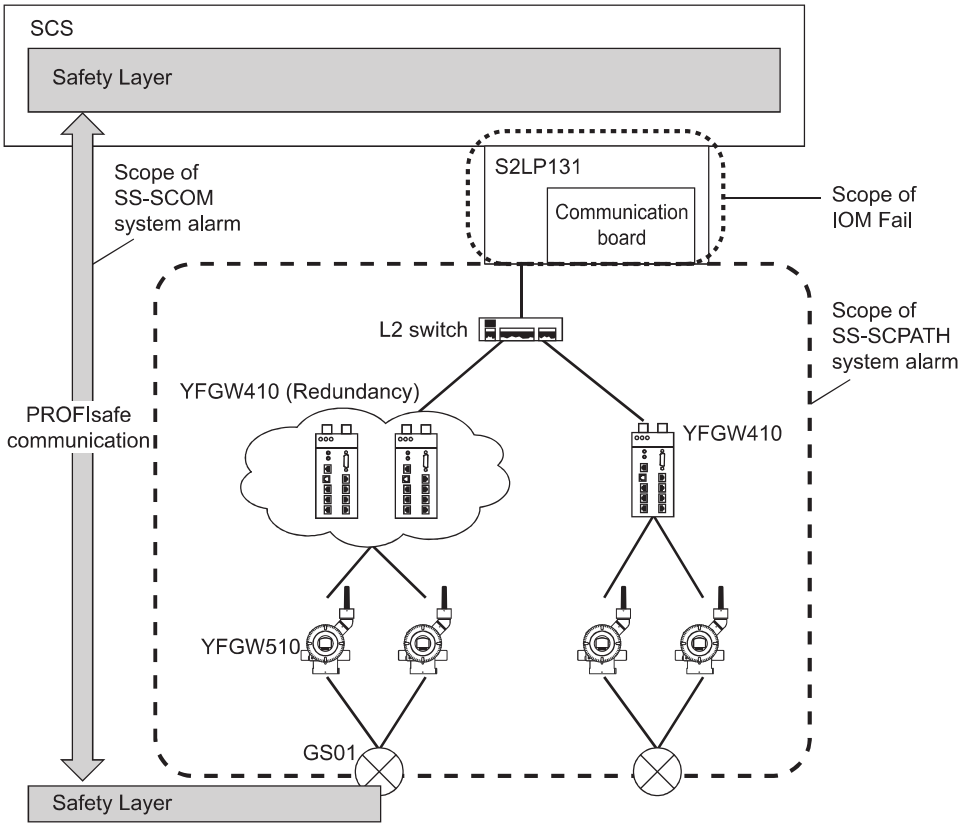


Figure E1.4.2-1 Scope of subjects of operation and monitoring messages

The scope of SS-SCPATH Errors is communication path errors of the fire and gas communication system. This includes errors of the devices and communication paths leading up to S2LP131, YFGW410, YFGW510, and GS01.

The scope of SS-SCOM Errors is safety communication errors of the fire and gas communication system. Safety communication of fire and gas communication refers to the communication between the safety layer of the SCS and GS01.

Safety subsystem communication path errors (SS-SCPATH Error)

SS-SCPATH Errors notify path errors of fire and gas communication. The errors that can be detected are as follows:

- Configuration errors (errors of definition information downloaded to S2LP131)
- Communication errors with PROFINET IO-devices
- YFGW410 errors
- YFGW510 errors
- GS01 communication errors

Safety subsystem communication errors (SS-SCOM Error)

SS-SCOM Errors notify safety communication errors of fire and gas communication. The errors that can be detected are as follows:

- GS01 failed.
- The SCS received irregular safety data from GS01.
- GS01 could not receive safety data from the SCS properly.
- The SCS could not receive a response to a request to GS01.

E1.5 Engineering for fire and gas communication

You can only perform engineering for fire and gas communication through I/O list engineering using IOM Definition Editor and Safety Communication I/O Editor of AD Suite. In addition, you can also create applications by using iDefine.

Flow of engineering for fire and gas communication modules

This section describes the flow of engineering with I/O list engineering for fire and gas communication modules.

Upon newly creating or importing a safety communication I/O list, reflect the settings of the field wireless system devices onto the safety communication I/O list with PROFINET Configurator and then use YFGW-PROFINET Configuration Support Tool to reflect the assignment of PROFINET modules onto YFGW410.

Help files are provided for information on how to use PROFINET Configurator.

The Help files can be found in the following location:

```
<Drive of ProSafe-RS software medium>:\ProSafe-RS\PDFFILE\PROFINET_Configurator\en\
```

The following files are included:

- SYCONnet netFrame YOKOGAWA S2LP131.pdf
- SYCONnet netDevice YOKOGAWA S2LP131.pdf
- PROFINET IO Controller YOKOGAWA S2LP131 DTM.pdf
- YOKOGAWA PROFINET IO Generic Device DTM.pdf

The following image shows the scope of explanations covered by each of the Help files.

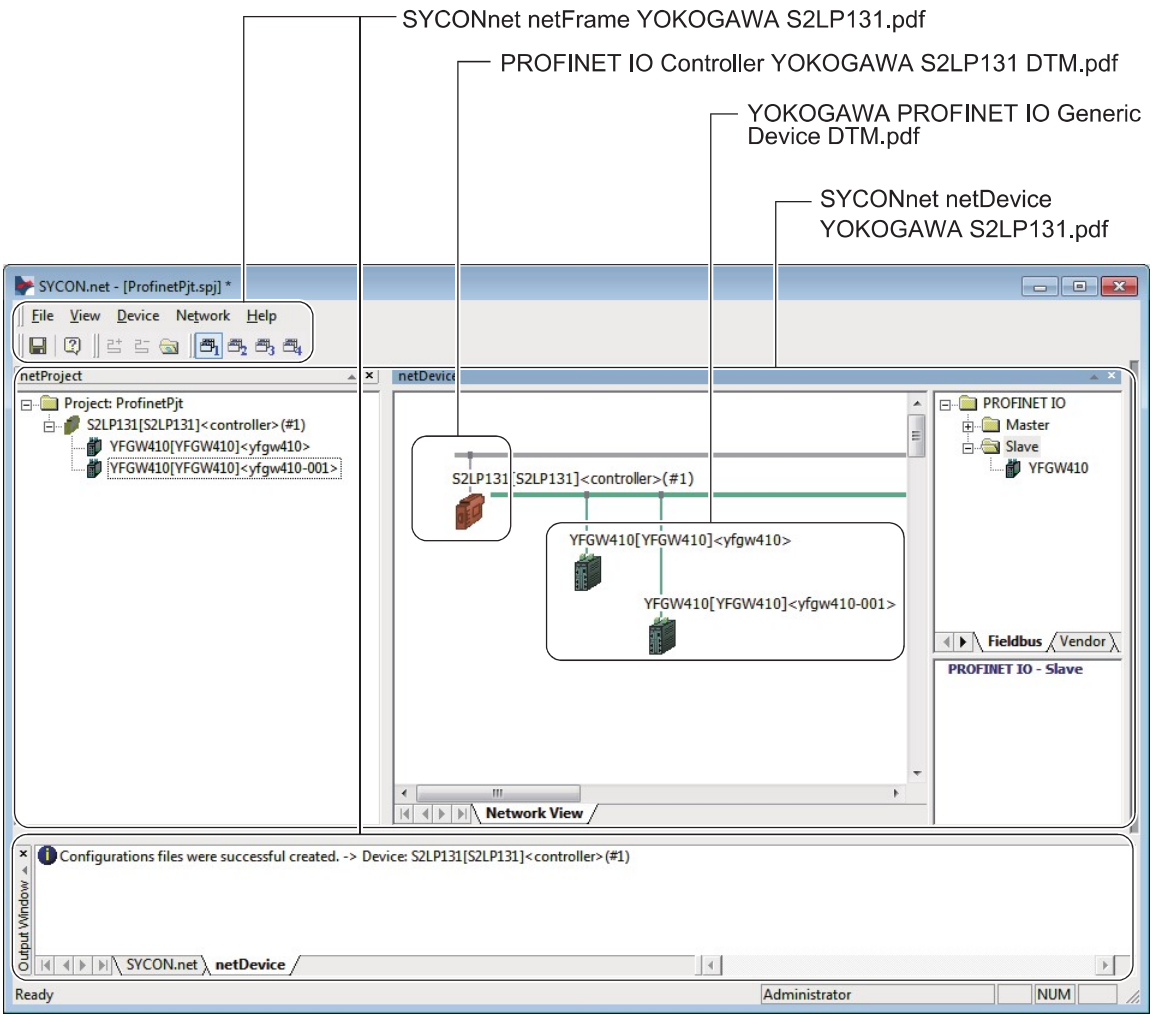


Figure E1.5-1 Areas explained in the Help files

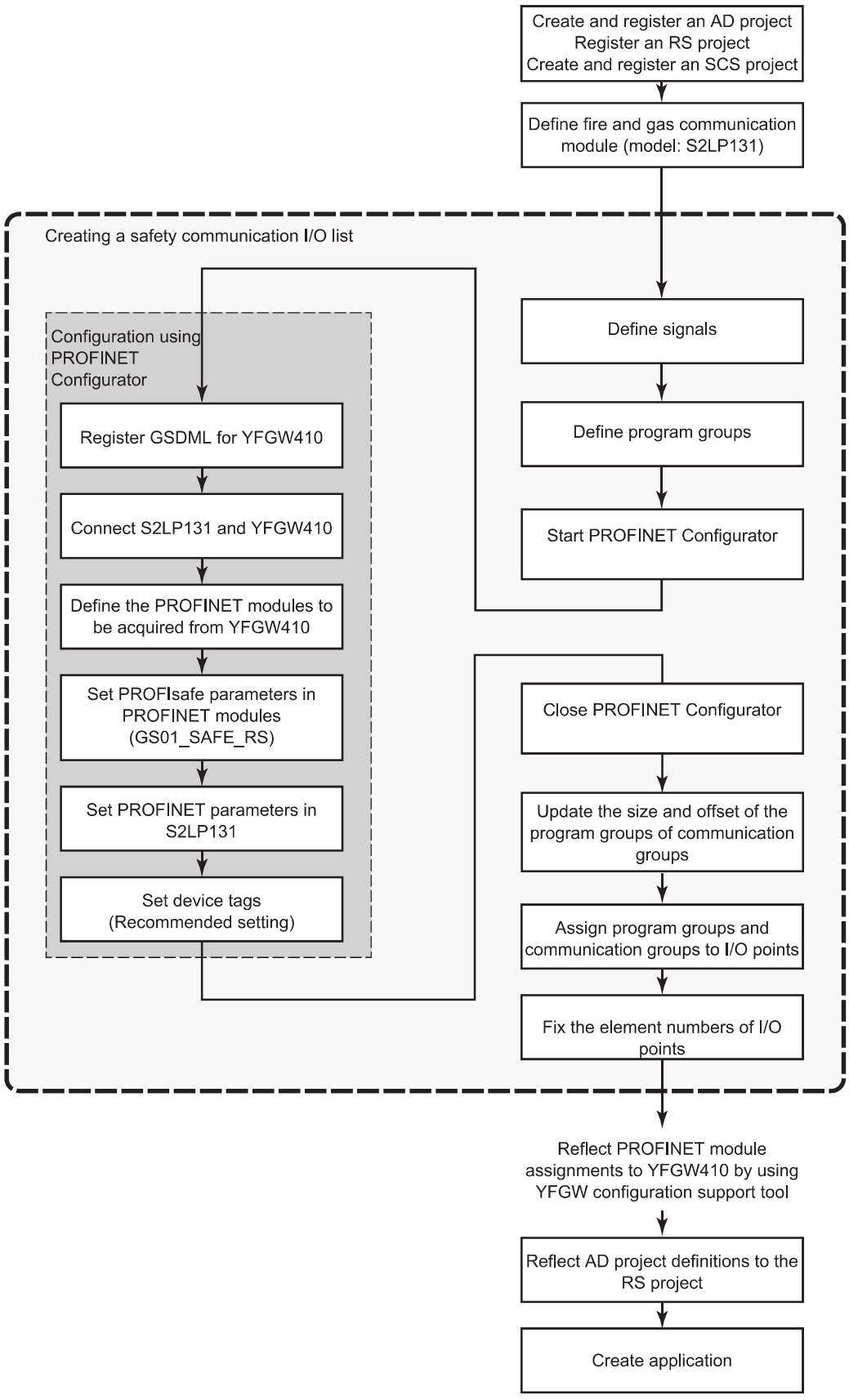


Figure E1.5-2 Flow of engineering for fire and gas communication modules

Defining a fire and gas communication module (S2LP131)

If you are not defining I/O modules by using a safety communication I/O list, create a node and I/O module by using the IOM Definition Editor to define the fire and gas communication module:

SEE ALSO

For more information about how to create nodes, refer to:

"● Creating a node" in "■ Creating the node and I/O module based on safety I/O list" in D3.4, "Creating the node and I/O module" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about how to define I/O modules, refer to:

"● Creating an I/O module" in "■ Creating the node and I/O module based on safety I/O list" in D3.4, "Creating the node and I/O module" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

E1.5.1 Creating a safety communication I/O list

Prepare a safety communication I/O list for defining fire and gas communication. You can either import a safety communication I/O list or create a safety communication I/O list by using Safety Communication I/O Editor.

After creating the safety communication I/O list, set the following items:

1. Define the signal of S2LP131.
2. Define the program group.
3. Select the program group and start PROFINET Configurator.

Defining the signal of S2LP131

Decide the P&ID Tag, I/O Type, Signal Protocol, I/O Tag, and Data Type for the I/O points you want to receive the values for by using an FB through the applicable S2LP131. Set the instance of the FB as the I/O Tag.

IMPORTANT

When setting the instance of PSI_I or PSI_R as the I/O Tag, set the Signal Protocol to PROFIsafe. When setting the instance of PNI_I or PNI_R as the I/O Tag, set the Signal Protocol to PROFINET.

Defining the program group

Define the program group to be subject to PROFINET Configurator and set the following parameters in the grid of the program group:

- Program Protocol: PROFINET
- Connection Device Type: PROFINET

Selecting the program group and starting PROFINET Configurator

From the scope of the SCS Project, start Safety Communication I/O Editor. In the program definition grid, select the line where S2LP131 is defined as the IOM type and start PROFINET Configurator from the context menu that appears when right-clicking.

E1.5.2 Applying settings by using PROFINET Configurator

PROFINET Configurator creates a PROFINET definition file for downloading onto S2LP131. The information included in the PROFINET definition file is reflected in Safety Communication I/O Editor. Also take note that the content of the file will not be overwritten with operations of Safety Communication I/O Editor.

Starting PROFINET Configurator

This section explains the precautions and procedures for starting PROFINET Configurator used in combination with Safety Communication I/O Editor.

Precautions when starting PROFINET Configurator

- On a single SENG, only one PROFINET Configurator can be used at a time. On a SENG where CENTUM VP is coexisting, PROFIBUS-DP Configurator of CENTUM VP cannot be used at the same time either.
- Implement engineering using PROFINET Configurator per one S2LP131 module.
- Be sure to check-out the safety communication I/O file in advance before starting PROFINET Configurator.
- The information defined with PROFINET Configurator is reflected onto PROFINET Configuration managed by AD Organizer. PROFINET Configuration is automatically checked-out when starting PROFINET Configurator.

Procedures for starting PROFINET Configurator

PROFINET Configurator is started from the context menu of Safety Communication I/O Editor. Part of the cells in Safety Communication I/O Editor onto which data is reflected from PROFINET Configurator will be read-only while PROFINET Configurator is running.

In the program definition list or communication definition list, right-click on the cell where S2LP131 is the IOM type and PROFINET is defined to the program protocol and select [Launch PROFINET Configurator].

Performing engineering with PROFINET Configurator

Perform settings in the following manner using PROFINET Configurator.

1. Register GSDML of YFGW410.
2. Connect S2LP131 with YFGW410.
3. Define the PROFINET modules to obtain through YFGW410.
4. Set the parameters of PROFIsafe to the PROFINET modules.
5. Set the parameters of PROFINET to S2LP131.
6. Set the device tag of the PROFINET modules.

Registering GSDML of YFGW410

Register GSDML of YFGW410 when adding a PROFINET IO-device in PROFINET Configurator. This task is not necessary when GSDML of YFGW410 has already been registered to PROFINET Configurator.

TIP

GSDML is a GSD file created using a language called Generic Station Description Markup Language. Information such as device capabilities and data structures is defined.

SEE ALSO For more information about registration procedures for GSDML of YFGW410, refer to:

5.2.1 “Load Device Catalog” in SYCONnet netDevice YOKOGAWA S2LP131.pdf

Connecting S2LP131 with YFGW410

Assign the PROFINET module held by the PROFINET IO-device to the PROFINET slot and sub slot of the PROFINET IO-device.

Modules that support PROFIsafe are included in the PROFINET modules that can be assigned.

- As shown in the following image, drag and drop YFGW410 to the Master bus line to connect with S2LP131.

TIP If nothing is displayed in the Device Catalog area of PROFINET Configurator, select [Network] > [Device Catalog] from the menu bar of PROFINET Configurator and click the [Reload Catalog] button to refresh the Device Catalog.

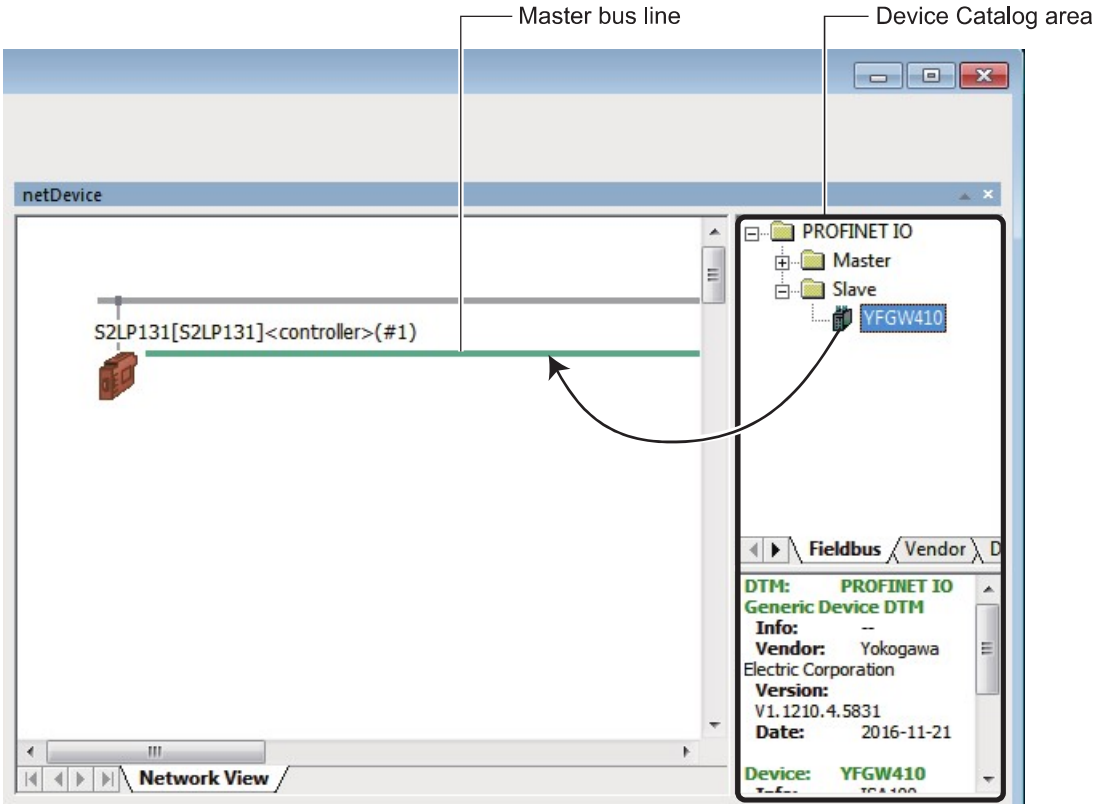


Figure E1.5.2-1 How to connect S2LP131 with YFGW410

SEE ALSO For more information about procedures for connecting S2LP131 with YFGW410, refer to:

5.4 “Insert Device in Project” of SYCONnet netDevice YOKOGAWA S2LP131.pdf

Defining the PROFINET module to obtain through YFGW410

Define the PROFINET modules to obtain through YFGW410.

IMPORTANT

Make the slot and sub slot numbers of the PROFINET module configured with PROFINET Configurator match the slot and sub slot numbers of the PROFINET module configured with FWMC. If these numbers do not match, it will not be possible to properly obtain the corresponding PROFINET module. The data status of the safety subsystem communication I/O definition corresponding to such PROFINET module will display an error.

Mismatches can be prevented by using YFGW-PROFINET Configuration Support Tool after closing PROFINET Configurator.

SEE ALSO For more information about how to define a PROFINET module, refer to:

3.4, “Modules” in YOKOGAWA PROFINET IO Generic Device DTM.pdf

Setting the parameters of PROFIsafe to the PROFINET module

You must perform settings of PROFIsafe if the wireless field device assigned with PROFINET Configurator supports the PROFIsafe protocol.

- Set the F-Parameter of PROFIsafe. The default value is obtained from the GSDML file for YFGW410 and displayed.
  The F-Parameters that can be set will vary depending on the PROFIsafe device. In addition, when you connect GS01 through YFGW410, the high and low limits of the settable F-Parameter values are described in the GSDML of YFGW410. For this reason, refer to the instruction manuals of both GS01 and YFGW410 to find the F-Parameters that can be set with GS01.

IMPORTANT

Make the F-Parameter set using PROFINET Configurator match the F-Parameter set using GS01 Configurator. If these do not match, it will not be possible to properly obtain GS01_SAFE_RS. The data status of the safety subsystem communication definition corresponding to such PROFINET module will display an error.

SEE ALSO For more information about how to set the parameters of PROFIsafe, refer to:

3.5, “Submodule Parameters” in YOKOGAWA PROFINET IO Generic Device DTM.pdf

For more information about the F-Parameters that can be set with GS01, refer to:

- GS01 user's manual from GasSecure AS
- YFGW410 PROFINET Interface (IM 01W02D01-21EN)

Setting the parameters of PROFINET to S2LP131

Set the following parameters of PROFINET to S2LP131:

- IP address, subnet mask, and default gateway of S2LP131
- PROFINET name of YFGW410 being connected
- Cycle of PROFINET I/O communication with YFGW410 being connected

IMPORTANT

- Make the PROFINET name of YFGW410 be the same value as the name set with FWMC. PROFINET communication between S2LP131 and YFGW410 can only be established when these names are of the same value. If PROFINET communication cannot be established, the data status of all safety subsystem communication definitions related to the corresponding YFGW410 will display an error.
- When you set the cycle of PROFINET I/O communication with YFGW410 (Updating Time and Watchdog Time), you must refer to the instruction manual of YFGW410.
- Do not use DCP Set of PROFINET in relation to YFGW410. The default setting of PROFINET Configurator is set to not use DCP Set in relation to YFGW410. Do not change this setting.

SEE ALSO

For more information about how to set the IP address, subnet mask, and default gateway of S2LP131, refer to:

4.3, “Controller Network Settings” in PROFINET IO Controller YOKOGAWA S2LP131 DTM.pdf

For more information about how to set the PROFINET name of YFGW410 being connected, refer to:

4.4, “Device Table” in PROFINET IO Controller YOKOGAWA S2LP131 DTM.pdf

For more information about the setting values for the cycle of PROFINET I/O communication with YFGW410 to be connected, refer to:

YFGW410 PROFINET Interface (IM 01W02D01-21EN)

For more information about how to set the cycle of PROFINET I/O communication with YFGW410 to be connected, refer to:

4.7, “Station Timing” in PROFINET IO Controller YOKOGAWA S2LP131 DTM.pdf

Setting the device tag of the PROFINET module

You can set a tag of your choice in relation to the PROFINET module by using PROFINET Configurator. The tag that has been set is reflected onto Communication Group and PROFINET Device Slot Tag under Communication Definition in the safety communication I/O list.

Communication Group is included in the messages of system alarms such as SS-SCOM and SS-SCPATH. For this reason, setting Communication Group with a string that includes the device tag will make it easier to identify the source of an alarm.

Setting PROFINET Device Slot Tag with a device tag will make it easier to grasp the correspondence between the communication definition and PROFINET module.

For this reason, it is recommended to set a device tag to the PROFINET module.

1. In PROFINET Configurator, double-click on S2LP131.
   The following window appears.

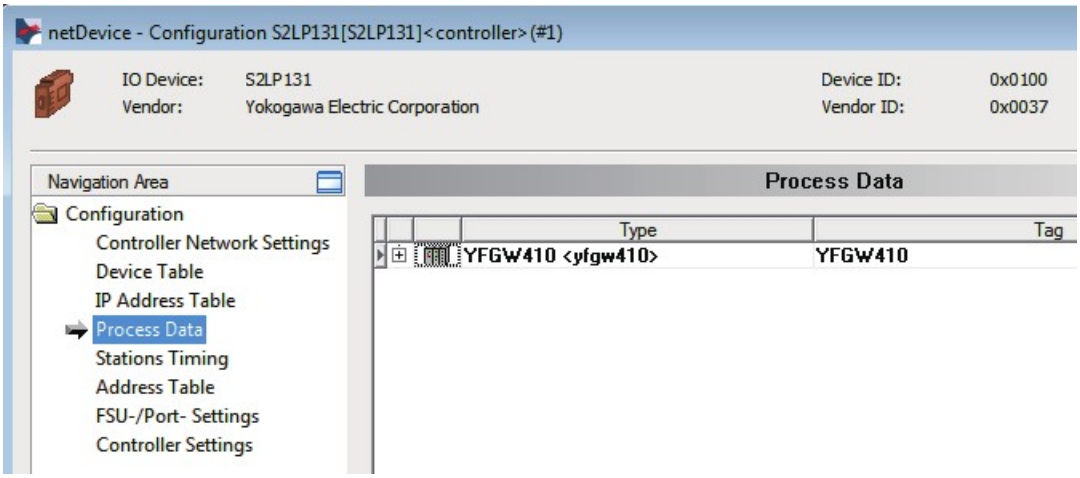


Figure E1.5.2-2 Display example of S2LP131

2. In the Navigation Area, select [Process Data].
3. Select [+].
   The list of PROFINET modules appears.

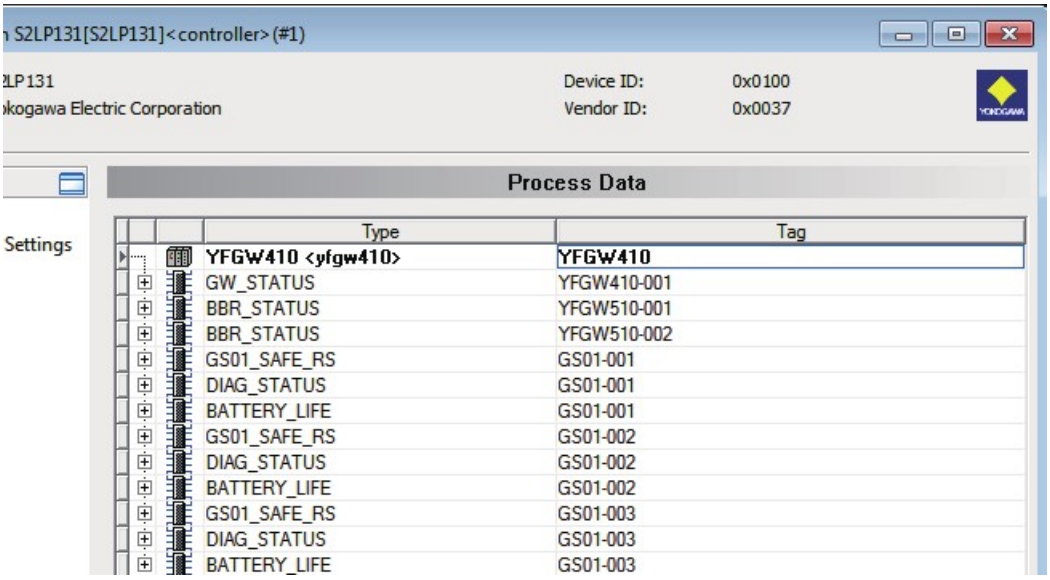


Figure E1.5.2-3 Display example of PROFINET modules

4. Enter the device tag in Tag of the displayed PROFINET modules.
   Use single-byte characters for the device tag. Normal operation cannot be guaranteed if any double-byte characters are used.
5. Click [OK].
   The window closes.

● Ending PROFINET Configurator

By ending PROFINET Configurator after saving the setting details, the set details are loaded into Safety Communication I/O Editor and reflected onto their corresponding cells.

E1.5.3 Applying settings after ending PROFINET Configurator

When PROFINET Configurator is ended, the program group is refreshed and the communication group is added. Communication definitions are added for every PN-Submodule defined with PROFINET Configurator. The format for the [Communication Group] column of communication definitions is [PN-Device Slot Tag] [PN-Module].

Example) When [PN-Device Slot Tag] is GS0101 and [PN-Module] is GS01_SAFE_RS

```
GS0101 GS01_SAFE_RS
```

Proceed to perform the following settings using Safety Communication I/O Editor:

1. Refresh the size and offset of the communication group and the program group.
2. Assign the program group and communication group to I/O points.
3. Establish element numbers for the I/O points.

Refreshing the size and offset of the communication group and the program group

Follow these steps to refresh the size and offset of the communication group and the program group:

1. Refreshing the size and offset of the communication group
   Click [Calculate] for the communication group.

   The results from PROFINET Configurator are imported and the size and offset of the communication group are refreshed.
2. Refreshing the size of the program group
   Click [Calculate].

   The results from PROFINET Configurator are imported and the size of the program group is refreshed.
3. Refreshing the offset of the program group
   When there are multiple S2LP131, in the [Offset] column of the program group, enter an offset value so that the areas of %XW assigned to each S2LP131 do not overlap.

Assigning the program group and communication group to I/O points

Items set with PROFINET Configurator are reflected onto Program Definition and Communication Definition of Safety Communication I/O Editor. Follow these steps to assign the program group and communication group to I/O points in the signal definition of Safety Communication I/O Editor:

1. From the signal definition of Safety Communication I/O Editor, select the I/O point to assign and click [Program Group] to select the program group to assign to the applicable S2LP131.
2. Click [Communication Group] of the I/O point and select the communication groups to assign.

TIP Up to 200 communication groups for the PROFINET protocol can be assigned for each S2LP131.

Defining PN-Data

Follow these steps to define [PN-Data] of an I/O point:

1. Click the column for [PN-Data] of the I/O point.

The Text IDs of the I/O Data defined to the PROFINET Submodule with PROFINET Configurator appear in a drop-down list.

2. Select a Text ID displayed in the list. The signal for which to retrieve values through the function block defined in the I/O Tag of the I/O point is decided.
   The values are refreshed for the Position and Data Type of the I/O point for which PN-Data has been decided and become read only.

Establishing element numbers for the I/O points

Follow these steps to establish element numbers:

1. Click [Update Element] in the toolbar of Safety Communication I/O Editor.
   The integrity of I/O information is confirmed and [Element] of the I/O points are updated.
2. If there is a need to fix the element numbers for the I/O points, change [Fix Element] in the signal definition list to [Yes].
   The element numbers for the I/O points become fixed.

Precautions regarding operation of Safety Communication I/O Editor and PROFINET Configurator

This section describes the definitions related to PROFINET as well as operations and precautions when changing the definitions.

Precautions when the mounting position of S2LP131 has been changed with IOM Definition Editor

When the mounting position of S2LP131 is changed with IOM Definition Editor, among the details defined with Safety Communication I/O Editor, details related to the PROFINET of the S2LP131 that has been changed will be cleared. However, Data Name and Data Type of the signal group definition related to the S2LP131 will not be cleared.

In such case, the details of the PROFINET definition file will be reflected onto related cells by running Read PROFINET Configurator Result or Launch PROFINET Configurator with Safety Communication I/O Editor.

Precaution for GS01-compatible engineering

- Checking for setting changes of GS01
  Check if there are changes in the following definitions and as necessary, correct Communication Group, and reflect these onto the signal. The following items of the existing communication definition are refreshed. Even if the item is read only, an asterisk (*) will be shown if it has been changed. Check the differences by going back and forth between clicking Undo and clicking Read PROFINET Configuration Result.
  - Connection Device Tag
    YFGW410 to which GS01 belongs
  - PROFINET Device Slot Tag
    Tag name of GS01
  - PROFINET Module Name
    Data name of GS01
- Moving and restoring settings of PROFINET Configurator
  The following function allows you to move and restore items while including settings of PROFINET Configurator:
  - SCS project export/import function
  - AD project export/import function
  - AD server backup/restore function

- SCS Manager version control function

The following function does not allows you to move and restore items while including settings of PROFINET Configurator:

- Safety communication I/O list export/import function

Loading the PROFINET definition file with Safety Communication I/O Editor

Follow these steps to load the PROFINET definition file into Safety Communication I/O Editor.

1. As necessary, check-out the PROFINET definition file.

TIP

The PROFINET definition file is automatically checked-out when starting PROFINET Configurator. Perform a check-out if the file has been checked-in or the check-out status has been forcibly released after starting PROFINET Configurator.

2. In the sub menu of Safety Communication I/O Editor, click [Read PROFINET Configurator Result].
   The details of the PROFINET definition file are reflected onto the corresponding cells in Safety Communication I/O Editor.

TIP

This menu is enabled when Safety Communication I/O Editor is started with the scope of the SCS and a cell related to S2LP131 in the program group definition is selected.

E1.5.4 Reflecting items onto the SCS project

Perform the reflection process in order to reflect the items set with the safety communication I/O list onto the applicable SCS using RS Generation Manager.

The items set with the safety communication I/O list are reflected onto their corresponding SCS projects. Along with this, an FB instance for fire and gas communication is created in the SCS project according to the data type of the signal of the safety communication I/O list. FB for fire and gas communication consist of the two types which are FB for PROFINET and FB for PROFIsafe.

In addition, the set items are reflected onto the communication definition and wiring definition of Communication I/O Builder while the FB instances for PROFINET and PROFIsafe can be assigned to element number %XB.

FB for PROFIsafe can be used with safety applications. FB for PROFINET cannot be used with safety applications due to being interference-free.

TIP

Check whether or not Interference-free FB are being used with safety applications by using Integrity Analyzer.

E1.6 YFGW-PROFINET Configuration Support Tool

This tool is used to reflect the assignment of PROFINET modules set on the SCS side onto the YFGW side when performing engineering for fire and gas communication modules. In addition, this tool allows you to compare the settings for PROFINET on the SCS side and the YFGW410 side. However, a comparison of whether or not the F-Parameter values for PROFIsafe are the same on the YFGW side and the SCS side cannot be performed.

E1.6.1 Overview of YFGW-PROFINET Configuration Support Tool

This tool loads the engineering data from SENG and the engineering data from Field Wireless Management Console (hereinafter referred to as FWMC) and exports a PROFINET-ISA100 mapping file. The PROFINET assignment information defined with SENG can be reflected on-to YFGW410 by loading this mapping file with FWMC.

When to use YFGW-PROFINET Configuration Support Tool

The following figure shows the timing at which to use YFGW-PROFINET Configuration Support Tool in the flow of engineering for fire and gas communication.

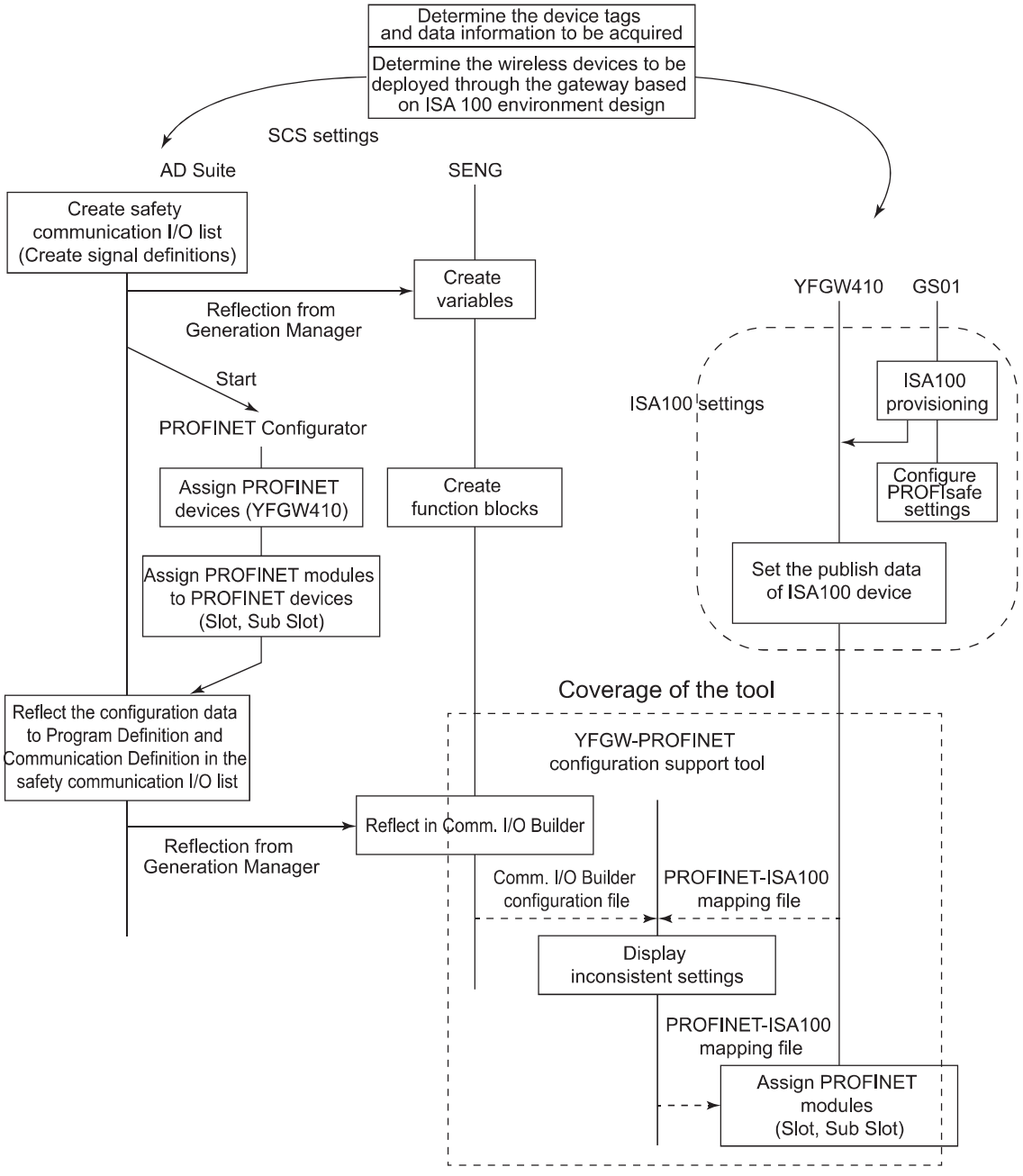


Figure E1.6.1-1 Flow of engineering

Preconditions for use of the tool

Satisfy the following conditions on the SENG side and FWMC side prior to using the tool.

SENG side

Complete each of the following settings before exporting the CSV file:

- Complete settings with PROFINET Configurator.
  - Set the Device Tag of wireless field devices with PROFINET Configurator.
  - Set the Device Tag of YFGW410 as the Station Name.
  - Assign the gas concentration data assigned to GS01, the Backbone Router (hereinafter referred to as BBR), and the status of the GW to the Slot and Sub Slot of the PROFINET of YFGW410.
- Reflect the information of PROFINET Configurator onto Safety Communication I/O Editor. Using PROFINET Configurator, the Device Tag set to each wireless field device is correctly assigned as the Device Tag of the corresponding I/O point.
- Perform a reflection with AD Organizer and reflect data onto Communication I/O Builder.

FWMC side

Decide the following information and share it between SCS engineers and field wireless system engineers:

- The design of the field wireless system has been completed, device tag names have been set for gas detector GS01, GW, and BBR, and what kind of data will be obtained from each device is decided.
- The GW to which GS01 will belong is decided.
- The F-Parameter information of PROFIsafe is decided for every GS01. In particular, F_Dest_Add is decided. Instead of using a part of the information unique to each device (EUI-64), decide unique addresses including the SCS PROFIsafe address of F_Source_Add for the PROFIsafe addresses of GS01 by such as numbering them in order from 1 to 65534.

Files related to the tool

The following files are required in order to use this tool:

- CSV file exported from Communication I/O Builder
- PROFINET-ISA100 mapping file in the CSV format exported from FWMC

The following information included in each CSV file are subject to this tool.

Information of the CSV file exported from Communication I/O Builder

Multiple YFGW410 are defined to Communication I/O Builder and the following information is defined for every YFGW410:

- Device Tag (when the Device Tag of each wireless field device has been set with PROFINET Configurator)
- PROFINET module name
- PROFINET module size
- PROFINET Slot and Sub Slot numbers

Information of the PROFINET-ISA100 mapping file

Once settings for the ISA100 publishing data have been completed, export the PROFINET-ISA100 mapping file in the CSV format. The PROFINET-ISA100 mapping file contains the following publishing data for every ISA100 device. Because the values on the SCS side are imported through the tool, it is OK for the PROFINET Slot and Sub Slot numbers to be in an undefined state.

- Host name and IP address of YFGW410
- Device Tag
- ISA100 Data Name
- Data size
- PROFINET Slot and Sub Slot numbers

E1.6.2 Using YFGW-PROFINET Configuration Support Tool

The procedures using this tool are as follows. Follow the order in which to import the CSV files into the tool. Prepare the following files before starting the tool:

- CSV file exported from Communication I/O Builder
- PROFINET-ISA100 mapping file exported from FWMC

1. Start the tool.
2. Using the tool, load the CSV file exported from Communication I/O Builder.
3. Using the tool, load the PROFINET-ISA100 mapping file.
4. Check the integrity of the engineering results on the SCS side and the FWMC side.
5. Export the PROFINET-ISA100 mapping file.
6. Export a report.

If an excess or deficiency of the PROFINET settings has been found, export a report from the tool and perform engineering again on the SCS side and FWMC side while referring to this report.

Check the details with the tool and export the PROFINET-ISA100 mapping file from the tool. Information of the Slot and Sub Slot set on the SCS side is incorporated into the PROFINET-ISA100 mapping file. This information can be reflected onto YFGW410 by importing the exported results with FWMC.

Starting the tool

Start YFGW-PROFINET Configuration Support Tool.

Importing the CSV file exported from Communication I/O Builder

1. After processing a reflection with Generation Manager, start Communication I/O Builder and export the CSV file.
2. In the tool, select [File] > [Open Communication I/O Builder file].
3. With the Select File dialog box that appears, load the exported CSV file.

Loading the file will result in an error if the CSV file does not have settings for PROFINET.

The following image is an example of what you will see after loading the CSV file.

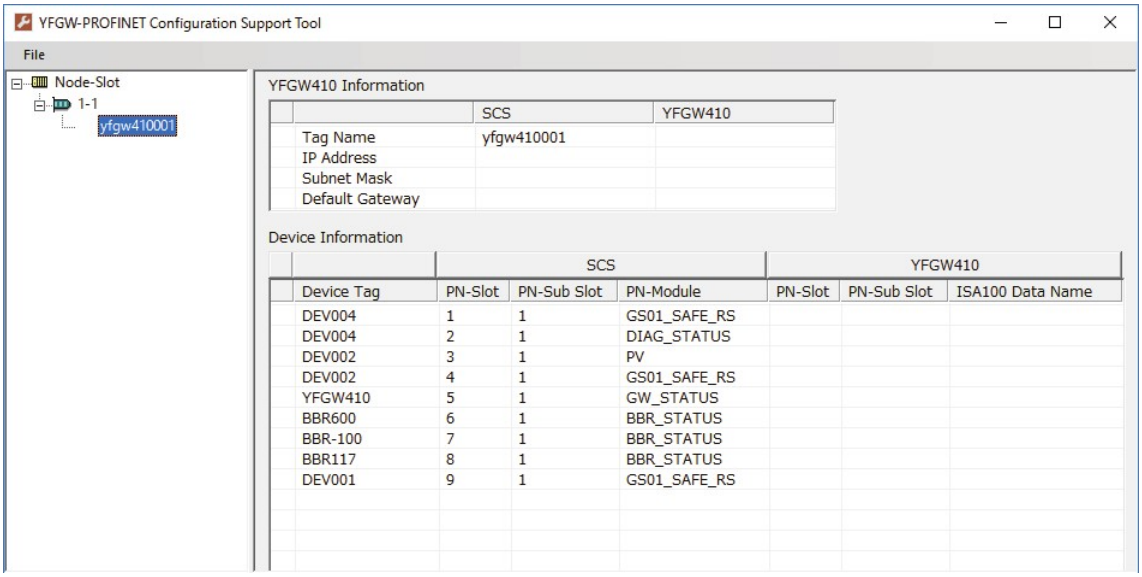


Figure E1.6.2-1 State where information from Communication I/O Builder has been reflected

Loading the PROFINET-ISA100 mapping file

Follow these steps to load the PROFINET-ISA100 mapping file exported from FWMC:

1. In the tool, select [Menu] > [Open PROFINET-ISA100 mapping file].
2. With the Select File dialog box that appears, load the exported PROFINET-ISA100 mapping file.
3. Information of the YFGW410 corresponding to the loaded PROFINET-ISA100 mapping file appears.

If the host name of YFGW410 in the PROFINET-ISA100 mapping file is not included in the information of the SCS side loaded into the tool, an error dialog will appear and the display will not be refreshed.

TIP

Loading of the file will result in an error if you attempt to load the PROFINET-ISA100 mapping file before the CSV file exported from Communication I/O Builder.

Checking the integrity of the engineering results on the SCS side and the FWMC side

After loading the files, check the differences between the settings on the SCS side and the YFGW410 side.

If non-matching items exist, the non-matching items of the individual data on the right pane are shown in blue along with a mark indicating a non-match at the beginning of the column.

Marks indicating a non-match are also added to YFGW410 in the tree on the left pane. The marks that appear are different between YFGW410 having one or more differences that require correction and YFGW410 only having differences that do not require correction. Specific examples are explained in the sections that follow.

Displaying the IP address of YFGW410

- When the Mode of YFGW410 is set to No DCP SET (Correct setting)
  Because the Mode of YFGW410 is set to No DCP SET by PROFINET Configurator, there are no values for the IP address, subnet mask, and default gateway of YFGW410 on the SCS side. Such cases are not acknowledged as a non-match, and the mapping file can be exported.

YFGW410 Information

	SCS	YFGW410
Tag Name	yfgw410001	YFGW410001
IP Address		192.168.0.101
Subnet Mask		255.255.255.0
Default Gateway		192.168.0.1

Figure E1.6.2-2 Displaying the IP address setting (Correct setting)

- When the Mode of YFGW410 is not set to No DCP SET (Wrong setting)
  If the Mode of YFGW410 is set to a mode other than No DCP SET by PROFINET Configurator, there are values for the IP address, subnet mask, and default gateway of YFGW410 on the SCS side. This setting is wrong regardless of whether the values are matching or non-matching with the YFGW410 side. In this case, set the Mode to No DCP SET by using PROFINET Configurator.

YFGW410 Information

	SCS	YFGW410
Tag Name	yfgw410001	YFGW410001
IP Address	192.168.0.101	192.168.0.101
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.0.1	192.168.0.1

Figure E1.6.2-3 Displaying the IP address setting (Wrong setting)

When the PROFINET Slot and Sub Slot numbers do not match

When the PROFINET Slot and Sub Slot numbers do not match, this will be shown as illustrated in the following image. The PROFINET-ISA100 mapping file can be exported in such cases. The Slot and Sub Slot numbers on the SCS side are exported to the file.

Device Information

	SCS			YFGW410		
Device Tag	PN-Slot	PN-Sub Slot	PN-Module	PN-Slot	PN-Sub Slot	ISA100 Data Name
DEV004	1	1	GS01_SAFE_RS			SafeData
DEV004	2	1	DIAG_STATUS			DIAG_STATUS
DEV002	3	1	PV			PV
DEV002	4	1	GS01_SAFE_RS			SafeData
YFGW410	5	1	GW_STATUS			GW_STATUS
BBR600	6	1	BBR_STATUS			BBR_STATUS
BBR-100	7	1	BBR_STATUS			BBR_STATUS
BBR117	8	1	BBR_STATUS			BBR_STATUS
DEV001	9	1	GS01_SAFE_RS			SafeData

Figure E1.6.2-4 Non-match of Slot and Sub Slot numbers

TIP

In this example, the mark at the beginning of the column indicate that a correction is not required despite there being differences between the settings on the SCS side and the YFGW410 side. If there are only differences that do not require correction, the assignment of PROFINET modules on the SCS side can be reflected onto the YFGW410 side using the exported mapping file. When there are only differences that do not require correction, the mark indicating that a correction is not required will also appear for the YFGW410 in the tree on the left pane.

When a Device Tag that exists on the YFGW410 side does not exist on the SCS side

Device Tag, ISA100 Data Name, Slot, and Sub Slot included on the YFGW410 side only are shown as illustrated in the following image. In this case, the PROFINET-ISA100 mapping file can be exported while including Device Tag information that exists on the YFGW410 side. However, the values on the SCS side will be exported for the Slot and Sub Slot numbers in the file. In this example, Slot and Sub Slot of DEV001 are cleared.

Device Information

		SCS			YFGW410		
	Device Tag	PN-Slot	PN-Sub Slot	PN-Module	PN-Slot	PN-Sub Slot	ISA100 Data Name
	DEV004	1	1	GS01_SAFE_RS	1	1	SafeData
	DEV004	2	1	DIAG_STATUS	2	1	DIAG_STATUS
	DEV002	3	1	PV	3	1	PV
	DEV002	4	1	GS01_SAFE_RS	4	1	SafeData
	YFGW410	5	1	GW_STATUS	5	1	GW_STATUS
	BBR600	6	1	BBR_STATUS	6	1	BBR_STATUS
Δ	DEV001				7	1	SafeData
Δ	DEV001						SafeData
Δ	DEV001						DIAG_STATUS

Figure E1.6.2-5 When a Device Tag on the YFGW410 side does not exist on the SCS

When a Device Tag that exists on the SCS side does not exist on the YFGW410 side

Device Tag, Slot, Sub Slot, and PROFINET Module Name included on the SCS side only are shown as illustrated in the following image.

In this case, the PROFINET-ISA100 mapping file is exported without including the Device Tag information that exists on the SCS side only.

Device Information

		SCS			YFGW410		
	Device Tag	PN-Slot	PN-Sub Slot	PN-Module	PN-Slot	PN-Sub Slot	ISA100 Data Name
	DEV004	1	1	GS01_SAFE_RS	1	1	SafeData
	DEV004	2	1	DIAG_STATUS	2	1	DIAG_STATUS
	DEV002	3	1	PV	3	1	PV
	DEV002	4	1	GS01_SAFE_RS	4	1	SafeData
	YFGW410	5	1	GW_STATUS	5	1	GW_STATUS
	BBR600	6	1	BBR_STATUS	6	1	BBR_STATUS
Δ	BBR-100	7	1	BBR_STATUS			
Δ	BBR117	8	1	BBR_STATUS			
Δ	DEV001	9	1	GS01_SAFE_RS			

Figure E1.6.2-6 When a Device Tag on the SCS side does not exist on YFGW410

When a PROFINET Module corresponding to ISA100 Data Name cannot be identified

When a PROFINET Module on the SCS side corresponding to ISA100 Data Name on the YFGW410 side cannot be identified, Device Tag and ISA100 Data Name are shown as illustrated in the following image. This includes cases such as when not using this data with SCS or when excessive publishing data has been assigned to YFGW410.

In such case, the PROFINET-ISA100 mapping file can be exported while including data that exists on the YFGW410 side only.

Device Information

		SCS			YFGW410		
	Device Tag	PN-Slot	PN-Sub Slot	PN-Module	PN-Slot	PN-Sub Slot	ISA100 Data Name
	DEV004	1	1	GS01_SAFE_RS	1	1	SafeData
	DEV004	2	1	DIAG_STATUS	2	1	DIAG_STATUS
	DEV002	3	1	PV	3	1	PV
	DEV002	4	1	GS01_SAFE_RS	4	1	SafeData
	BBR600	5	1	BBR_STATUS	5	1	BBR_STATUS
	BBR-100	6	1	BBR_STATUS			BBR_STATUS
Δ	YFGW410						GW_STATUS
Δ	DEV001						DIAG_STATUS
Δ	DEV003						DIAG_STATUS

Figure E1.6.2-7 When data of YFGW410 does not exist in PROFINET Module Name of SCS

When ISA100 Data corresponding to a PROFINET Module Name cannot be identified

When an ISA100 Data Name on the YFGW410 side corresponding to a PROFINET Module on the SCS side cannot be identified, Device Tag, PROFINET Module Name, Slot, and Sub Slot are shown as illustrated in the following image.

This includes cases such as when PROFINET modules have been excessively assigned on the SCS side or when you have forgotten to set publishing data to YFGW410.

In this case, a PROFINET-ISA100 mapping file that does not include module information that exists on the SCS side only can be exported.

Device Information

		SCS			YFGW410		
	Device Tag	PN-Slot	PN-Sub Slot	PN-Module	PN-Slot	PN-Sub Slot	ISA100 Data Name
	DEV004	1	1	GS01_SAFE_RS	1	1	SafeData
	DEV004	2	1	DIAG_STATUS	2	1	DIAG_STATUS
	DEV002	3	1	PV	3	1	PV
	DEV002	4	1	GS01_SAFE_RS	4	1	SafeData
	YFGW410	5	1	GW_STATUS	5	1	GW_STATUS
	BBR600	6	1	BBR_STATUS	6	1	BBR_STATUS
	BBR-100	7	1	BBR_STATUS	7	1	BBR_STATUS
Δ	BBR117	8	1	BBR_STATUS			
	DEV001	9	1	GS01_SAFE_RS			SafeData

Figure E1.6.2-8 When a Module Name on the SCS side does not exist in the publishing data of YFGW410

When there is a non-match

The following will occur if multiple types of non-matches occur at the same time.

In cases when only Slot and Sub Slot on the SCS side and YFGW410 side are different, the values on the SCS side are exported to the PROFINET-ISA100 mapping file. Import the file with FWMC and continue with engineering.

The following occurs when an actual device is operated using the exported PROFINET-ISA100 mapping file in a state where any other non-match is included:

- When there is more information on the YFGW410 side than the SCS side
  This creates a state where settings on the YFGW410 side are not assigned to PROFINET. However, information engineered on the SCS side is all included. An SCS communication error will not occur. However, communication will not be performed with devices for which there is a non-match.
- When there is more information on the SCS side than the YFGW410 side
  This creates a state where assignment of PROFINET on the SCS side is excessive. Because there is no corresponding PROFINET setting on the YFGW410 side, the communi-

cation status with SCS becomes Bad when trying to communicate and therefore none of the values will be obtained.

Exporting the PROFINET-ISA100 mapping file

Follow these steps to export the PROFINET-ISA100 mapping file.

1. From the [File] menu in the tool, select [Save PROFINET-ISA100 mapping file].
2. With the Save As dialog box that appears, export the PROFINET-ISA100 mapping file.

IMPORTANT

If the Mode of YFGW410 has been set to a mode other than No DCP SET by PROFINET Configurator, the following dialog box appears when you select [Save PROFINET-ISA100 mapping file] and the PROFINET-ISA100 mapping file cannot be exported.

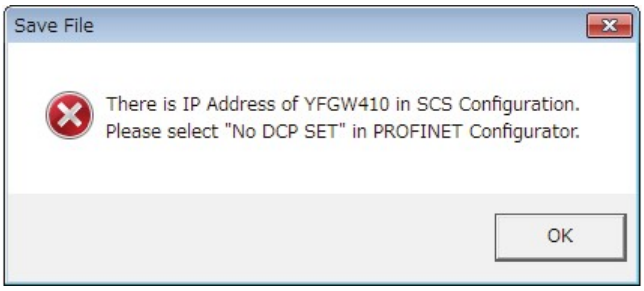


Figure E1.6.2-9 Error dialog box

In this case, set the Mode of YFGW410 to No DCP SET by using PROFINET Configurator, and perform the operation again.

Exporting a report

The details shown in the tool can be exported as a CSV file. Information on differences is expressed in the following manner:

- When there are no differences: 0
- When there are differences that can be ignored: 1
- When there are differences that cannot be ignored: 2

Follow these steps to export the report:

1. From the [File] menu in the tool, select [Save Report].
2. With the Save As dialog box that appears, export the report.

E1.7 Application logic for obtaining the gas concentration of GS01

You must create an application logic in order to obtain the gas concentration of GS01.

This section describes the precautions to take and the method to use when creating the application logic.

The examples of application logic described here are created based on the following Safety Manual of GS01:

GasSecure GS01 Wireless Infrared Hydrocarbon Gas Detector Safety Manual

Document ID: 21440

Release: 1

Version: 81

The application logics are created with reference to the gas concentration values that GS01 sends upon the statuses of Fail safe detected (SD), Fail safe undetected (SU), Fail dangerous detected (DD), and Fail dangerous undetected (DU), which are shown in the Safety Manual. The specifications may differ for each GS01 revision. So, confirm the specification with the latest edition of GS01 Safety Manual and create your application logic.

Physical data and logical data upon various events

Wire PSI_R and PSI_I to GS01_SAFE_RS. Then, a gas concentration is input to PSI_R and the data quality status to PSI_I.

The following figure shows the relationship between the physical data and logical data of GS01_SAFE_RS when a safety communication error, GS01 failure, or gas generation occurs.

Table E1.7-1 Physical data and logical data of GS01_SAFE_RS upon various events

Event	Physical data	Logical data
Safety communication error	• PSI_R (gas concentration) PSI_R.v: Previous value PSI_R.sts: BAD • PSI_I (data quality status) PSI_I.v: Previous value PSI_I.sts: BAD	• PSI_R (gas concentration) PSI_R.v: Pre-defined input value at fault (*1) PSI_R.sts: BAD • PSI_I (data quality status) PSI_I.v: Pre-defined input value at fault (*1) PSI_I.sts: BAD
GS01 failure	• PSI_R (gas concentration) PSI_R.v: NaN (*2) PSI_R.sts: GOOD • PSI_I (data quality status) PSI_I.v: BAD (*2) PSI_I.sts: GOOD	• PSI_R (gas concentration) PSI_R.v: Pre-defined input value at fault (*1) PSI_R.sts: BAD • PSI_I (data quality status) PSI_I.v: BAD PSI_I.sts: GOOD
Gas generation	• PSI_R (gas concentration) PSI_R.v: Gas concentration PSI_R.sts: GOOD • PSI_I (data quality status) PSI_I.v: Data quality status (*2) PSI_I.sts: GOOD	• PSI_R (gas concentration) PSI_R.v: Gas concentration PSI_R.sts: GOOD • PSI_I (data quality status) PSI_I.v: Data quality status PSI_I.sts: GOOD

*1: This is the value set in the Safety Communication I/O Editor of AD Organizer.
*2: For the details, refer to the user's manual of GS01.

Example of application logic

The following figure shows an example of application logic where GASDTR, PSI_R, and PSI_I are used to create a user-defined function block (UDFB).

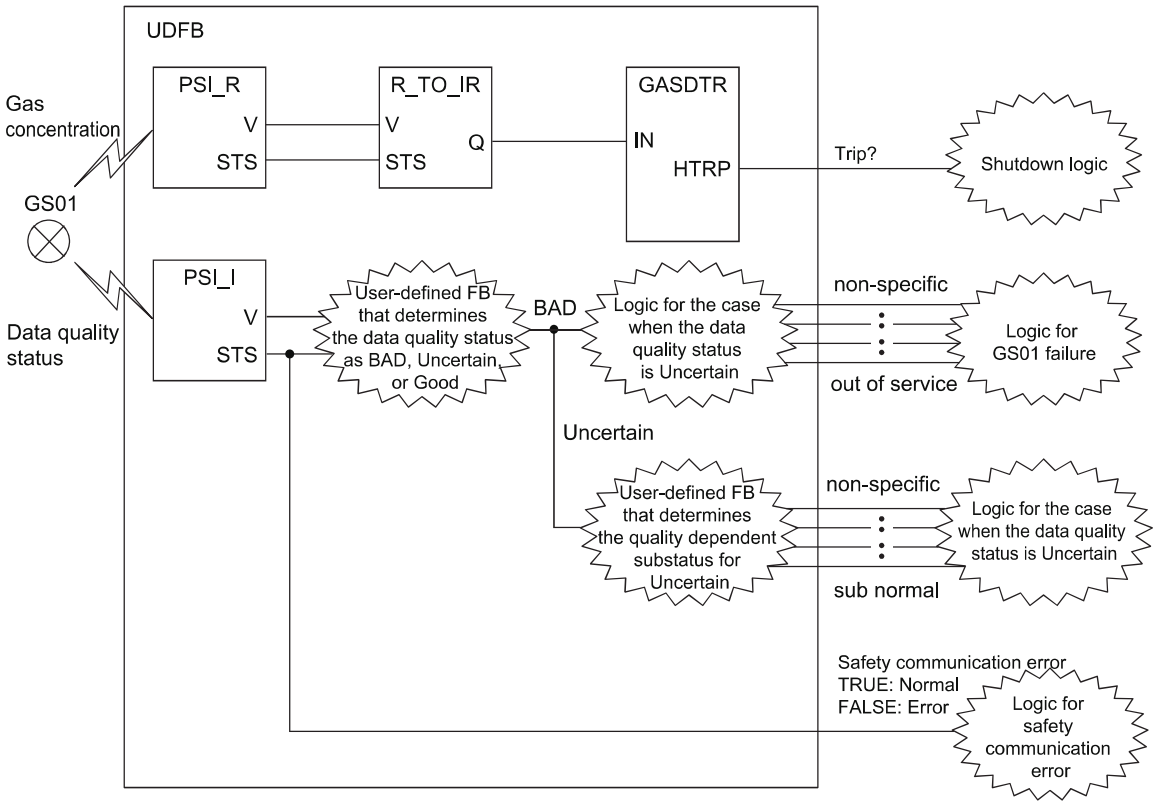


Figure E1.7-1 Example of application logic

- PSI_R usage
  PSI_R receives a gas concentration value. The gas concentration value is input to the IN terminal of GASDTR. However, since GASDTR expects that the input from the IN terminal is IO_REAL type data, PSI_R.v and PSI_R.sts need to be converted to IO_REAL type before they are input. For conversion to IO_REAL type, use a safety function block such as R_TO_IR.

- PSI_I usage
  PSI_I receives a data quality status value. The data quality status consists of Quality (Good/Bad/Uncertain), which indicates a category, Quality dependent substatus (detailed information for the category), and Limit condition (additional information for the category). For the specification of data quality status of GS01, refer to the user's manual of GS01.

  On detecting a failure of itself, GS01 sets the data quality status value to BAD. Therefore, you can use the value of PSI_I.v to find whether GS01 has failed. You can also use the value of Quality dependent substatus in addition to the Quality of the data quality status to identify the type of GS01 failure to create application logic that can perform different processing for each type of GS01 failure.

  The data quality status may have Uncertain as a Quality value. If the data value exceeds the sensor rage or temperature range, GS01 sets the data quality status to Uncertain. In this case, GS01 has not failed but a certain event has occurred, preventing GS01 from setting the data quality status to Good. You can create application logic that determines whether the data quality status of GS01 is Uncertain through the PSI_I.v value, and notifies the operators for each Quality dependent substatus of Uncertain.

  For the specification of data quality status of GS01, such as the Quality dependent substatuses that GS01 supports, contact the manufacturer of GS01.

PSI_I.sts is used to find the presence of safety communication errors. With PSI_R.sts, you cannot distinguish a safety communication error and a GS01 failure.

Example of application logic with/without use of the fault check function of GASDTR

GS01 reflects the information about its own fault in the data quality status of gas concentration. The data quality status of gas concentration can be obtained through PSI_I.

This section describes examples of application logic where the fault check function of GASDTR is used or not used.

Using the fault check function of GASDTR

The following figure shows an example of application logic where the fault check function of GASDTR is used.

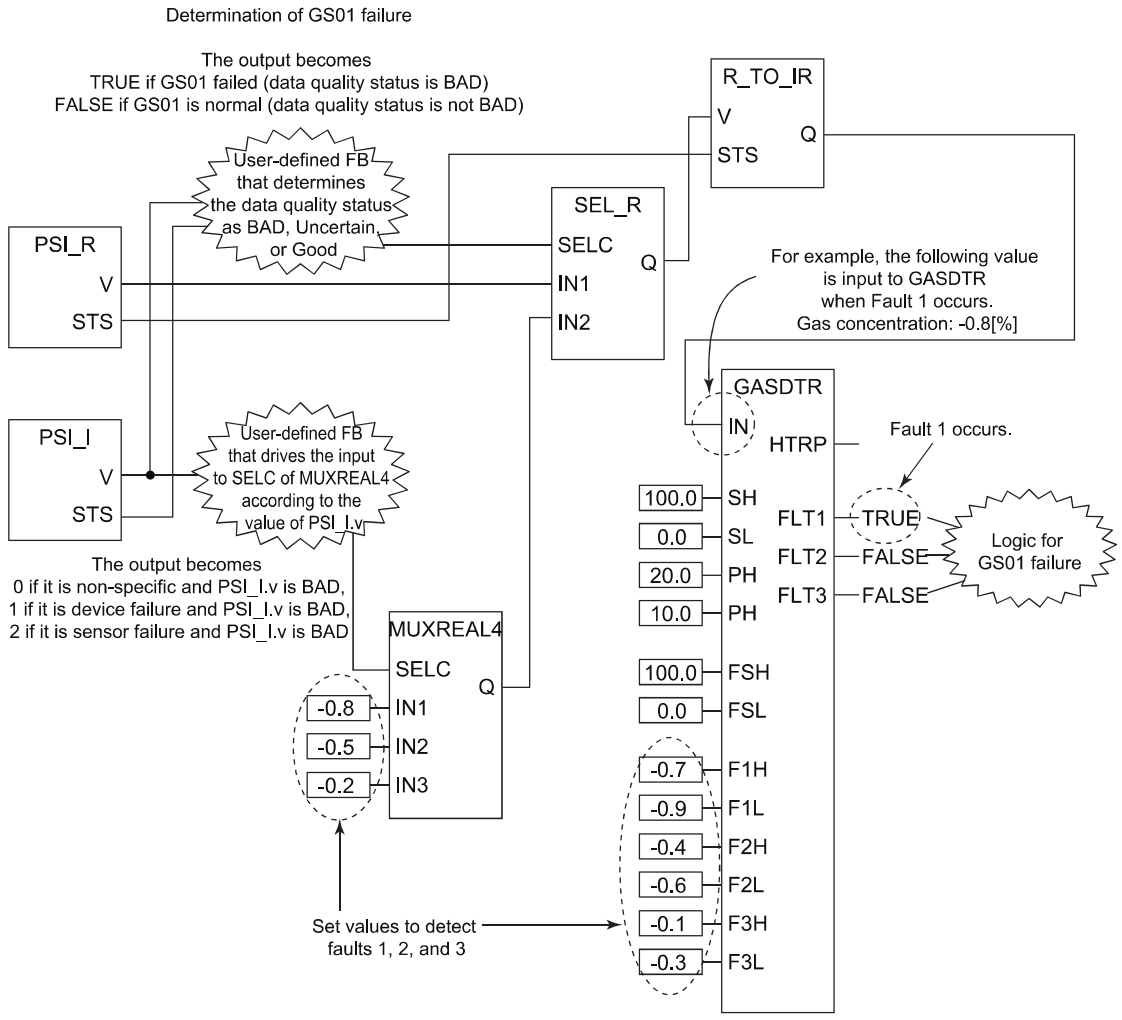


Figure E1.7-2 Example of application logic with use of the fault check function of GASDTR

This figure shows an example where the Quality dependent substatus for Quality = Bad of the data quality status is assumed as follows: “non-specific” is fault 1, “device failure” is fault 2, and “sensor failure” is fault 3.

For example, the application logic operates as follows if fault 1 occurs:

The output from MUXREAL4 is -0.8 and input to SEL_R. TRUE is input to SELC of SEL_R, and therefore SEL_R outputs -0.8. The input to GASDTR is -0.8, and therefore GASDTR detects fault 1.

In addition, since a GS01 failure is reflected in FLT1, FLT2, and FLT3, you can use FLT1, FLT2, and FLT3 as input to the application logic that operates upon a GS01 failure.

Note that if you create the application logic shown in the example, the alarm status of the mapping block for GASDTR will be IOP when a fault occurs in GS01.

IMPORTANT

Although there are eight Quality dependent substatuses of data quality status, GASDTR can handle only three faults. Therefore, the following considerations are required:

- Handle up to three faults out of the Quality dependent substatuses that GS01 supports.
- Consolidate the eight Quality dependent substatuses into three faults.

SEE ALSO For more information about precautions when using the fault check function of GASDTR, refer to:

"● Precautions when setting HH, LL, PH, PL, F1L, F1H, F2L, F2H, F3L, and F3H" in "■ Description" in 5.18, "GASDTR (analog input function block for gas and flame detectors)" in POU Reference Manual (IM 32P03B20-01EN)

Not using the fault check function of GASDTR

If you do not use the fault check function of GASDTR to obtain faults of GS01, disable the fault check function of GASDTR.

You can disable the fault check function of GASDTR by setting the following values to the fault check input terminals of GASDTR.

- FSH/FSL
  Set the gas concentration range of GS01.
  Example:

  FSH=100.0, FSL=0.0

- F1H/F1L/F2H/F2L/F3H/F3L
  Set a value that GS01 never sends. Set the same value for all terminals.

  Example:

  F1H = F1L = F2H = F2L = F3H = F3L = -9999.9

- IDF1/IDF2/IDF3
  Set a null character.

E1.8 Precautions for engineering

This section explains the precautions to take when performing engineering for fire and gas communication.

Downloading to S2LP131

Downloading the following data to S2LP131 starts S2LP131:

- AP program: The firmware of S2LP131.
- PROFINET definition: Definition information regarding PROFINET created with PROFINET Configurator.
- IOM definition: IOM definition information of S2LP131 set with IOM Definition Editor.
- Communication I/O definition: Communication I/O definition information of S2LP131 set with Safety Communication I/O Editor.

The following table shows the relationship between the download operation and the data that is downloaded to S2LP131.

Table E1.8-1 Relationship between the download operation and the data that is loaded onto S2LP131

Download operation	AP program	PROFINET definition	IOM definition	Communication I/O definition
Offline download to the SCS	Yes	No	Yes	Yes
Online download to the SCS	Yes (*1)	Yes (*1)	Yes (*1)	Yes (*1)
IOM download	Yes	Yes	Yes	Yes

*1: Data will be downloaded if there is a difference.

IMPORTANT

- You cannot use automatic IOM download with S2LP131.
- Downloading the PROFINET definition will take up to two minutes from the start of download to when S2LP131 starts. During this time, PROFINET IO communication between S2LP131 and the PROFINET IO-device is suspended. When not downloading the PROFINET definition, S2LP131 starts after four to five seconds from the start of download.

E1.9 Error handling action

This section describes the behavior of S2LP131 when an error occurs with S2LP131 and when an error occurs on an upper level of S2LP131.

Behavior when an S2LP131 error occurs

The following table shows the behavior of S2LP131 when an S2LP131 error occurs.

Table E1.9-1 Error handling action of S2LP131

Event	Behavior of S2LP131
S2LP131 Fail	Stops operation. To restore, remove the cause of the error and perform an IOM download.
Communication board fail	Stops operation. You can obtain details of the cause of error in the IOM Report. To restore, replace S2LP131 and then perform an IOM download.
When starting S2LP131	Loads input data from the PROFINET IO-device.
When recovering from the S2LP131 error	
When recovering from an PROFINET communication error between S2LP131 and YFGW410	

Behavior when an error occurs on an upper level of S2LP131

The following table shows the behavior of S2LP131 when an error occurs on an upper level of S2LP131.

Table E1.9-2 Fallback behavior of S2LP131

Event	Behavior of S2LP131
SCS Fail ESB bus both end Fail	Loads input data from the PROFINET IO-device.
When recovering from the above error	

E1.10 Troubleshooting

When an error occurs with a communication module or field wireless system used in fire and gas communication, the SCS notifies system alarms of safety subsystem communication path errors (SS-SCPATH Error) and safety subsystem communication errors (SS-SCOM Error). Communication module errors, field wireless system errors, and communication errors can be confirmed in the Diagnostic Information window on SENG and the operation and monitoring windows on HIS. Fire and gas communication can respond with system alarms to errors that occur in the system.

SEE ALSO

For more information about I/O module error messages and troubleshooting, refer to:

Message Number 0081 in 3.1, “Safety Control Station Error Occurrence and Recovery Messages (Message Numbers 0001 through 0094)” in Messages Reference Manual (IM 32P02B10-01EN)

For more information about SS-SCOM Error messages and troubleshooting, refer to:

Message Number 4209 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)

For more information about SS-SCPATH Error messages and troubleshooting, refer to:

Message Number 4211 in 2.1, “System Alarms (Message Numbers 4101 through 4222)” in Messages Reference Manual (IM 32P02B10-01EN)

Analysis of error occurrence factors due to combinations of an SS-SCOM Error and SS-SCPATH Error

When a safety subsystem communication error (SS-SCOM Error) alarm is alerted, this may be accompanied by the alarm of a safety subsystem communication path error (SS-SCPATH Error). Checking the details of both alarms will enable you to identify the cause of the error occurrence. This is because an SS-SCOM Error is a system alarm regarding safety communication between the SCS and devices while SS-SCPATH Error is a system alarm regarding errors of the path of safety communication.

This section describes how to identify the cause of error occurrence by using actual error codes as example. Even when the combination of error codes is that which is not shown in the examples, you can identify the cause of error occurrence in a similar manner to the following examples:

Example 1

```
SCS0101 SS-SCPATH Error FIO NODE 01 SLOT 01 PORT 01 07PI118 Code=A3B0
SCS0101 SS-SCOM Error FIO NODE 01 SLOT 01 PORT 01 07PI118 Code=5A04
```

When in addition to an SS-SCOM Error indicating no response of the safety communication, an SS-SCPATH Error indicating no response is simultaneously alerted, it is likely that there is an error with the communication path between S2LP131 and YFGW410. Confirm the status of the communication path.

Example 2

```
SCS0101 SS-SCOM Error FIO NODE 01 SLOT 01 PORT 01 07PI118 Code=5A04
```

When an SS-SCOM Error indicating no response of the safety communication is alerted alone, it is likely that there is an internal error with the CPU module of the SCS or a device. Confirm the diagnosis information of the SCS or the device diagnosis information of the corresponding device.

Example 3

```
SCS0101 SS-SCPATH Error FIO NODE 01 SLOT 01 PORT 01 07PI118 Code=A396
SCS0101 SS-SCOM Error FIO NODE 01 SLOT 01 PORT 01 07PI118 Code=5A02
```

When in addition to an SS-SCOM Error indicating that the safety communication has received faulty data, an SS-SCPATH Error indicating an wireless communication error is simultaneously alerted, it is likely that there is an internal error with a device inclusive of its communication unit. Confirm the device diagnosis information of the corresponding device.

Example 4

```
SCS0101 SS-SCPATH Error FIO NODE 01 SLOT 01 PORT 01 07PI118 Code=A396
SCS0101 SS-SCOM Error FIO NODE 01 SLOT 01 PORT 01 07PI118 Code=5A04
```

When in addition to an SS-SCOM Error indicating no response of the safety communication, an SS-SCPATH Error indicating an wireless communication error is alerted, it is likely that there is an error with the communication path between a device and YFGW510. Confirm the status of the communication path.

Precautions for adding devices

When you add a device (PROFINET IO-device) to the same subnet while S2LP131 is running, do not use an IP address duplicated with S2LP131 or other existing devices. If there is a duplicate IP address, not only the device having the duplicate address but also other devices may be affected.

This section describes the behavior of devices when the IP address of an added device is duplicated with S2LP131 or another existing device by mistake.

When the IP address of the added device is duplicated with S2LP131

While S2LP131 is running, if the IP address of the device (PROFINET IO-device) that has been added to the same subnet is duplicated with S2LP131, the devices will behave as follows:

- Communication between S2LP131 and the existing devices continues. However, if a communication error occurs between S2LP131 and an existing device, the communication will not be resumed even if the direct cause of the error is eliminated. You cannot find out the cause that is preventing the resumption of communication from the system alarms or status lamps on S2LP131. In this case, you must correct the IP address setting or disconnect the device with a duplicate IP address from the network.

TIP

You cannot find out the cause that is preventing the resumption of communication from the system alarms or status lamps on S2LP131.

- S2LP131 and the added device cannot communicate with each other.

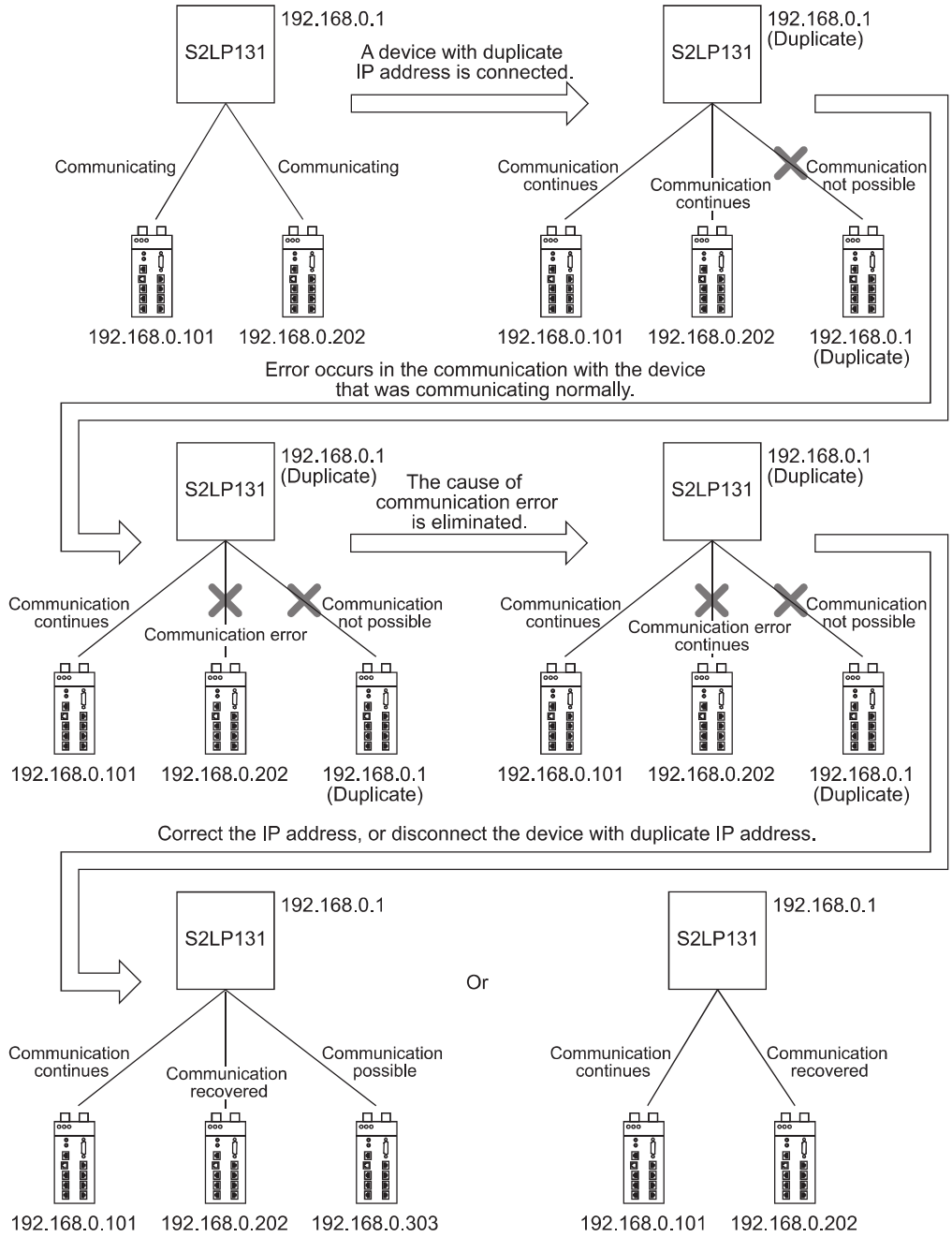


Figure E1.10-1 Behavior when S2LP131 and a device have a duplicate IP address

TIP

When S2LP131 is started, if a device having an IP address duplicated with S2LP131 exists in the same subnet, a system alarm No.0081 I/O module failure (Code=C58E) is generated.

When the IP address of the added device is duplicated with an existing device

If the IP address of the added device (PROFINET IO-device) is duplicated with an existing device, the devices will behave as described below. In such a case, you must correct the IP address setting or disconnect the device with a duplicate IP address from the network.

Example:

S2LP131: 192.168.0.50

Device 1: 192.168.0.51

Device 2: 192.168.0.99 (duplicate)

Device 3: 192.168.0.99 (duplicate)

- Case 1: Behavior when Device 2 is added first, and then Device 3 is added to the network
  - Communication between S2LP131 and Device 1 continues.
  - Communication between S2LP131 and Device 2 continues.
  - Communication between S2LP131 and Device 3 repeats a communication error SS-SCPATH Error Code=A3B0 and recovery.

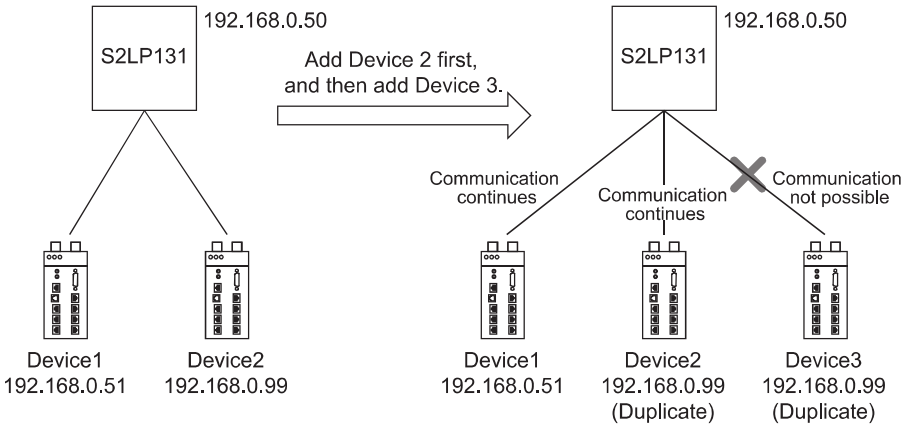


Figure E1.10-2 Behavior when Device 2 is added first, and then Device 3 is added to the network

- Case 2: Behavior when Device 2 and Device 3 are added to the network simultaneously
  - Communication between S2LP131 and Device 1 continues.
  - Communication between S2LP131 and Device 2 and between S2LP131 and Device 3 repeats a communication error SS-SCPATH Error Code=A3B0 and recovery. After a while, the communication between S2LP131 and one of the devices becomes normal, and the communication between S2LP131 and the other device results in a communication error SS-SCPATH Error Code=A3B0.

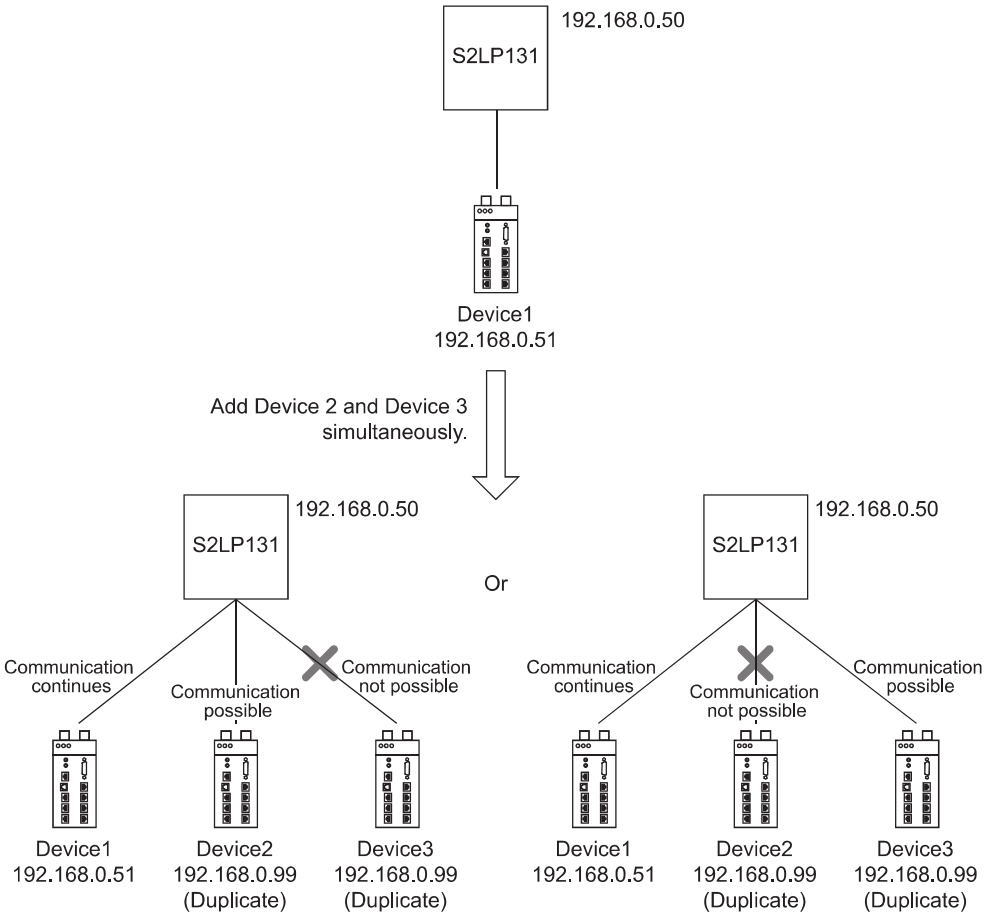


Figure E1.10-3 Behavior when Device 2 and Device 3 are added to the network simultaneously

F. Modbus slave communication

The Modbus slave communication function is one of the Modbus communication functions that are provided by ProSafe-RS. This function allows a safety control station (SCS) to act as a Modbus slave and communicate with other systems.

F1. Common items regarding the Modbus slave communication function

You can use the Modbus slave communication function to connect the ProSafe-RS SCS to other systems. The Modbus master (an external device) can reference or set data in SCS by using the communication function of the communication module. By accessing SCS data using the Modbus slave communication function, you can also display SCS status in other systems.

This section provides an overview and details of the SCS Modbus slave communication function and describes the setting method.

F1.1 Overview of Modbus slave communication

When the Modbus master (external device) sends data, the Modbus slave communication function of SCS receives the data through the communication function of the communication module. The SCS Modbus slave communication function sends a response message to the Modbus master (external device) in response to the request for data.

SEE ALSO For more information about precautions for engineering, refer to:

F4., “Precautions for engineering” on page F4-1

Relationship between SCS, SENG, and Modbus master

The following figure shows the relationship between the SCS, SENG, and Modbus master (external device).

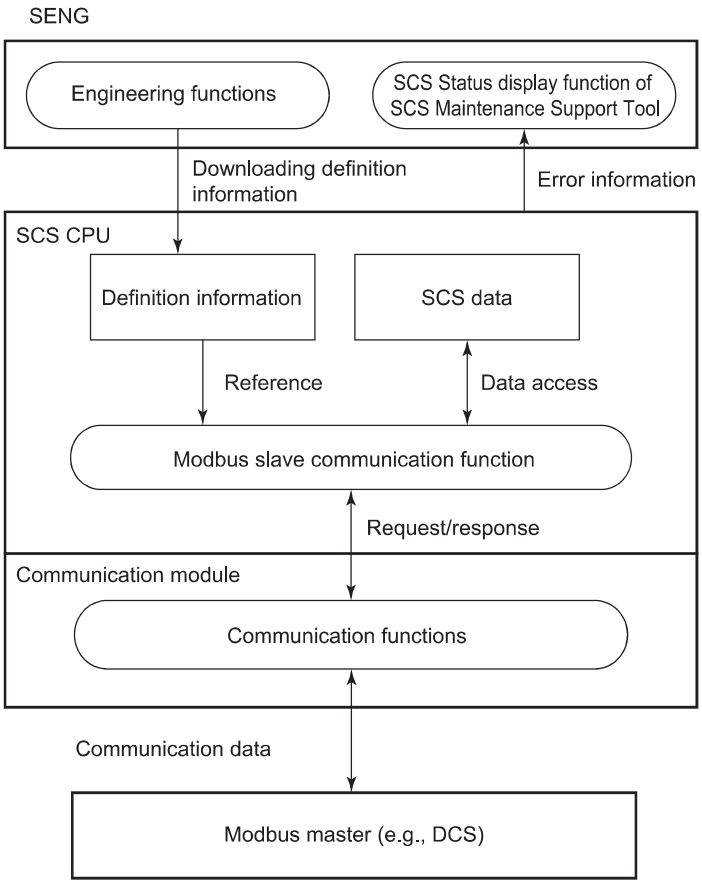


Figure F1.1-1 Relationship with an external device

The following describes the relationship between the SCS, SENG, and Modbus master (external device).

- SENG
  The engineering functions of the SENG download the definition information of the communication module and the definition of correspondence between Modbus device addresses and SCS data, etc. to SCS.
- SCS Maintenance Support Tool
  The SCS status display function of SCS Maintenance Support Tool receives error information and notifies the error status if there is any error in the communication module and communication content.

- Modbus master
  The Modbus master references and sets SCS data through the communication module.
- SCS
  The Modbus slave communication function of SCS accesses data in response to a request from the Modbus master and returns the result to the Modbus master through the communication module.

Interface with the Modbus master

SCS operates as a Modbus slave. An external device operates as the Modbus master and it can reference and set SCS data.

The external device and SCS are connected with a serial communication module or Ethernet communication module that is installed in the SCS node. Neither of these modules support dual-redundant configuration. These modules are interference-free modules that do not interfere with the safety loop.

- Serial communication module (RS-232C, 2-port)
- Serial communication module (RS-422/RS-485, 2-port)
- Ethernet communication module (10BASE-T, 1-port)

Data access by device speciation

The Modbus master requests data access to the SCS (Modbus slave) using the Modbus devices names in the following table as the interface.

SCS does not have actual Modbus devices. SCS assigns virtual Modbus device addresses to variables of the application logic and sends them responses accordingly.

Table F1.1-1 Modbus devices

Virtual Modbus device	Data	Access from master to slave (*1)	
		Read (reference)	Write (set)
Coil	Output device with 1 bit/channel	Yes	Yes (*2)
Input relay	Input device with 1 bit/channel	Yes	No
Input register	Input register with 16 bit/channel	Yes	No
Holding register	Output register with 16 bit/channel	Yes	Yes (*2)

*1: Yes: allowed
No: not allowed
*2: The Modbus master can only set data on SCS (Modbus slave) if virtual Modbus devices are assigned to external communication function blocks.

The correspondence between the addresses of the Modbus devices and variables of the application logic is defined using SCS Manager.

SEE ALSO

For more information about procedure for supporting addresses and application logic variables for Modbus devices, refer to:

F1.5.1, “Definitions in Modbus Address Builder” on page F1-12

Data settings from the Modbus master

Data can be set to variables of the application logic from the Modbus master through Modbus slave communication using external communication function blocks.

Modbus slave communication execution timing

As a Modbus slave, SCS performs Modbus slave communication at the idle time of each scan for the application logic. SCS checks whether any request has been sent from the Modbus master through the communication module. If SCS finds any request, SCS will respond to the request only when the scan has idle time.

SCS only responds to the request in this communication processing and will set the data to the variables of application logic in the scan by the safety functions after responding to the request.

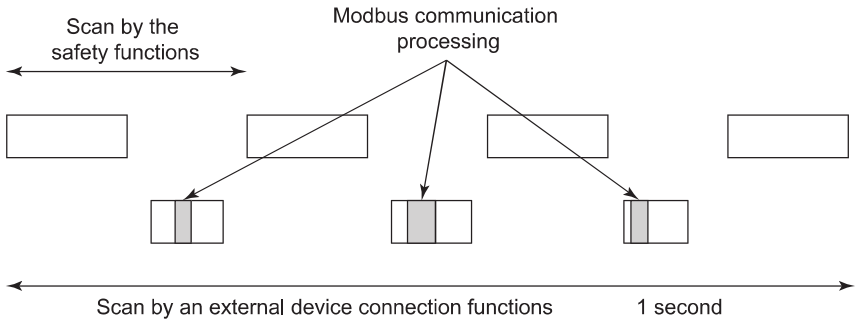


Figure F1.1-2 Modbus slave communication execution timing

Monitoring from HIS or SCS Maintenance Support Tool

The communication module status can be monitored from HIS or SCS Maintenance Support Tool.

Table F1.1-2 Monitoring of communication modules from HIS or SCS Maintenance Support Tool

Window	Monitoring operation
SCS State Management	Displays whether the communication module is normal or faulty. No communication errors are displayed.
System alarm	Errors in the communication module are notified by system alarms.

Operation when the communication module is added online

It is possible to make changes online to applications that involve addition or removal of serial communication modules. If you install an additional communication module in the SCS and execute an online change download, the communication module starts to run immediately. During downloading, the diagnostic information messages (IOM Fail, and then IOM Recover) are generated, but the operating mode of the SCS remains the same. You do not need to perform the Output enable operation or any other special operation.

F1.2 Data access using the Modbus communication functions

When the Modbus master sends a request for data access, SCS receives the data through the ALR111/ALR121 serial communication module or ALE111 Ethernet communication module. The SCS reads/writes data within itself using the Modbus communication commands and notifies the result to the Modbus master.

By using the Modbus communication functions, the SCS references or sets SCS data in response to requests from the Modbus master. To process the requests, it references the database that defines the correspondence between Modbus device addresses and application logic variables.

Referencing/setting SCS data

This function allows the Modbus master to reference internal variables (BOOL, DINT, REAL) or I/O variables of DI, DO and AI. It also allows the Modbus master to set (Modbus Word Order), variables data of external communication function blocks.

Word reversal

To reference SCS data, the order of 32-bit data can be changed.

The direct order is in the order of the upper word first and the lower word. The reverse order is in the order of the lower word first and the upper word if this option is specified.

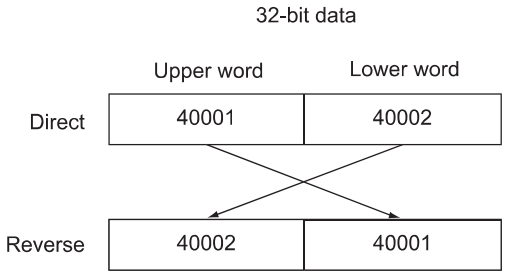


Figure F1.2-1 Execution example of word reversal

One shot write

When setting SCS data, a one shot write operation is performed on data that does not interfere with the safety loop. An error is returned if it is requested to set data that interfere with the safety loop.

16-bit Modbus master support mode

You can use 16-bit Modbus master support mode when connecting SCS to a Modbus master that handles only 16-bit data. If the Modbus master does not read or write data of SCS in 16-bit units, leave 16-bit Modbus master support mode disabled (default setting), and access data in 32-bit units. When this mode is enabled, the Modbus master can read and write data including 16-bit integer data, 32-bit signed integer data, and 32-bit floating point data. However, this requires very complicated ProSafe-RS application.

If the following types of data access is required, enable 16-bit Modbus master support mode by using SCS Constants Builder.

Table F1.2-1 Data accesses available in 16-bit Modbus master support mode

Access from the Modbus master to SCS	Data type	Function code (decimal)
Read one word from a holding register with an odd or even reference number	Signed integer data Floating-point data	Read Holding Registers (03)
Read one word from an input register with an odd or even reference number	Signed integer data Floating-point data	Read Input Registers (04)
Write one word to a holding register with an odd or even reference number	Signed integer data	Use the following function code whichever is available with the Modbus master: Preset Single Register (06) or Preset Multiple Registers (16)

SEE ALSO For more information about function codes supported on an SCS, refer to:

- "● Function code" on page F1-23
- "● Cautionary notes on function codes" on page F1-24

● Considerations on using the 16-bit Modbus master support mode in Modbus slave communication

When executing the following functions by using the function code from the Modbus master, set 16-bit Modbus master support mode for the definition of SCS Constants Builder to Enable.

- Writing to a single holding register by using the function code 06 from the Modbus master
- Reading one-word data or specifying even reference numbers by using the function codes 03 and 04 from the Modbus master
- Writing one-word data or specifying even reference numbers by using the function code 16 from the Modbus master

The function code 06 allows data to be written to the upper or lower word of 32-bit data. To use the written data as 16-bit data, create an application for extracting the upper or lower word of the 32-bit data.

When 16-bit Modbus master support mode is Enable in the SCS Constants Builder, the simultaneity of the upper and lower words is not assured because writing to the upper and lower words can be performed independently. If you intend to use the data as 32-bit data, write the data in units of 32 bits without using the function code 06 or 16.

■ Communication test

When testing for referencing a variable of SCS, change a value of the variable by using the Forcing function and confirm the value by the Modbus master. When testing for setting an external communication function block of SCS, connect a variable with the external function block and confirm the value of the variable by the Modbus master reading back.

SEE ALSO For more information about forcing function, refer to:

F8., "Forcing function" in Engineer's Reference Manual (IM 32P04B10-01EN)

F1.3 Setting items relating to Modbus slave communication

The following settings are required for the Modbus master to access application logic variables on an SCS through Modbus slave communication.

- Definition of communication modules
  To Modbus slave communication, define the serial communication module (ALR111/ALR121) or Ethernet communication module (ALE111) and set required I/O parameters. When performing I/O list engineering, you can use the IOM Definition Editor. When performing RS original engineering, you can use the I/O Wiring View and I/O Parameter Builder.
- Definition of addresses of Modbus devices
  You can define virtual Modbus devices on SCS and assign them to variables, using the Modbus Address Builder.
- Data setting using Modbus slave communication
  You can assign external communication function blocks to set SCS data from the Modbus master (external device).

F1.4 Definition of communication modules

You can define the communication module for SCS so that SCS can preform Modbus communication.

The editor to be used differs depending on engineering methods.

When performing I/O list engineering, you can define the serial communication module or Ethernet communication module and set parameters by using IOM Definition Editor.

When performing RS original engineering, you can define the serial communication module or Ethernet communication module by using the I/O Wiring View of the SCS Manager first. Then you can set parameters for each port of the module by using the I/O Parameter Builder.

This section mainly describes for the case when performing RS original engineering. The communication module definition items and the parameter setting items that are required in I/O list engineering are the same as those for RS original engineering.

SEE ALSO

For more information about I/O list engineering, refer to:

D., “Procedures to create applications using the I/O list engineering method” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about RS original engineering, refer to:

Appendix 2., “RS original engineering” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about I/O Wiring View and I/O Parameter Builder, refer to:

Appendix 2.2, “Definitions of inputs/outputs” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about parameter settings for communication modules, refer to:

Appendix 1.2, “Settings for modules” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

F1.4.1 Definitions in I/O Wiring View

When performing RS original engineering, you can define the serial communication module (ALR111/ALR121) or Ethernet communication module (ALE111) by using the I/O Wiring View in the SCS Manager as follows:

1. Open I/O Wiring View and select ALR111, ALR121, or ALE111. The number of channels should be set to 0.
2. Select parameters for the module and specify the node number and the slot number. The node number and the slot number must not overlap with those of other input/output modules and communication modules.

F1.4.2 Definitions in I/O Parameter Builder

When performing RS original engineering, you can specify parameters for the communication module by using I/O Parameter Builder. The parameters to specify differ depending on the type of the communication module.
Because a serial communication module (ALR111/ALR121) has two ports, two sets of parameters are required. You can specify the parameters in the Port1 and Port2 tabs of I/O Parameter Builder.

For an Ethernet communication module, you can set the parameters in the Ethernet communication module parameters tab of I/O Parameter Builder.

SEE ALSO

For more information about parameter settings for serial communication modules, refer to:

"■ Port 1, Port 2 tab" on page F2-6

For more information about parameter settings for Ethernet communication modules, refer to:

"■ Module tab of the Ethernet communication module" on page F3-5

F1.5 Definition of addresses of Modbus devices

To access variables of the application logic on SCS from the Modbus master through Modbus slave communication, it is necessary to define the correspondence between the variables and the addresses of Modbus devices. Define Modbus device addresses for the variables using Modbus Address Builder.

Modbus device addresses can be assigned to I/O variables and internal variables.

F1.5.1 Definitions in Modbus Address Builder

Use Modbus Address Builder to associate the variables of the application logic with the addresses of Modbus devices.

■ Assigning variables in Modbus Address Builder

Modbus devices can belong to the following four types: coils, input relays, input registers and holding registers. A reference number is assigned to each Modbus device type. The variable name to be accessed is assigned to a reference number in Modbus Address Builder. The type of variable to be assigned is selected according to the reference number. For example, a variable of BOOL type or IO_BOOL type can be assigned to an input relay.

SEE ALSO For more information about reference numbers, refer to:

"■ Modbus device tabs" on page F1-18

● Types of Modbus devices and variables

The type of variables that can be assigned to each reference number of Modbus devices is as follows:

Table F1.5.1-1 Variables to which Modbus device addresses can be assigned

Modbus device type	Variable type	Remark
Coil	ECW_B	Instance of external communication function block (BOOL type)
	BOOL	Read-only. Writing data to the SCS results in an error when the SCS runs.
	IO_BOOL	Read-only. Writing data to the SCS results in an error when the SCS runs.
	ECWR_B	Available only with SCSU1, which is dedicated to integration with CI Server
Input relay	BOOL	-
	IO_BOOL	Only the data value is included, and the data status is not included.
Input register	REAL	Requires two addresses per data.
	DINT	Requires two addresses per data.
	IO_REAL	Only the data value is included, and the data status is not included. Requires two addresses per data.

Continues on the next page

Table F1.5.1-1 Variables to which Modbus device addresses can be assigned (Table continued)

Modbus device type	Variable type	Remark
Holding register	ECW_R	Instance of external communication function block (REAL type) Requires two addresses per data
	ECW_I	Instance of external communication function block (DINT type) Requires two addresses per data
	REAL	Read-only. Writing data to the SCS results in an error when the SCS runs
	DINT	Read-only. Writing data to the SCS results in an error when the SCS runs
	IO_REAL	Read-only. Writing data to the SCS results in an error when the SCS runs
	ECWR_R	Available only with SCSU1, which is dedicated to integration with CI Server
	ECWR_I	Available only with SCSU1, which is dedicated to integration with CI Server

The BOOL, IO_BOOL, DINT, REAL, and IO_REAL-type variables are read-only. You can assign these variables to input relays and input registers. In Modbus Address Builder, variables of these types are not displayed in the data menu area for coils and holding registers. To assign these variables to coils or holding registers, you need to enter the variable names directly.

When the Modbus device is a coil or holding register, you can set data from the Modbus master only for the types that have correspondence with external communication function blocks such as ECW_B, ECW_R, and ECW_I types.

Variable names

A variable name can be up to 69 characters long. Both global and local variables can be accessed regardless of the scope. Describe a scope name after "@" to access local variables.

To access internal variables in a user-defined function block, you can use the SCS Manager Dictionary View to name instances of the user-defined function block itself. Specify the variable name in the following format. Up to two nesting levels can be specified for an instance name.

```
Instance name.internal variable name
```

Table F1.5.1-2 Example of variable names

Variable name	Scope	Description
VAR1	Global	Global variable
VAR2@PROG1	PROG1	A local variable of a function in PROG1
FB01.VAR3	Global	The internal variable VAR3 of an instance of the user-defined function block FB01
FB01.VAR3@PROG1	PROG1	The internal variable VAR3 of an instance of the user-defined function block FB01, which is locally defined in a function of PROG1
FB01.FB2.VAR3	Global	The internal variable VAR3 of an instance of the user-defined function block FB2 used inside an instance of the user-defined function block FB01 (The limit of nesting of a function block is two)

SEE ALSO For more information about SCS Manager Dictionary View, refer to:

Workbench User's Guide

How to define variable names

Variable names can be specified in the Variable name columns in the tabs for the four different types of Modbus devices.

A variable can be defined in one of the following ways:

- Direct entry from the keyboard
- Double-clicking a variable name in the data menu area
- Drag and drop a variable from Dictionary View

Direct entry from the keyboard

Enter a variable name in the Variable name column directly from the keyboard.

Double-clicking a variable name in the data menu area

The data menu area of Modbus Address Builder contains the Variable tab and the IOM tab. Double-click a variable name in the Variable tab to set the variable name in the Variable name column.

Double-click a node number or a slot number in the IOM tab to set variables wired for each Input/Output Module at once.

Drag and drop from Dictionary View

Drag and drop a variable name from Dictionary View to a variable name field of Modbus Address Builder to register the variable name in Modbus Address Builder. If you drag and drop multiple variable names, they are registered in order starting from the top of the Variable name column where they are dropped. If variable names have already been registered in the Variable name field, they are overwritten.

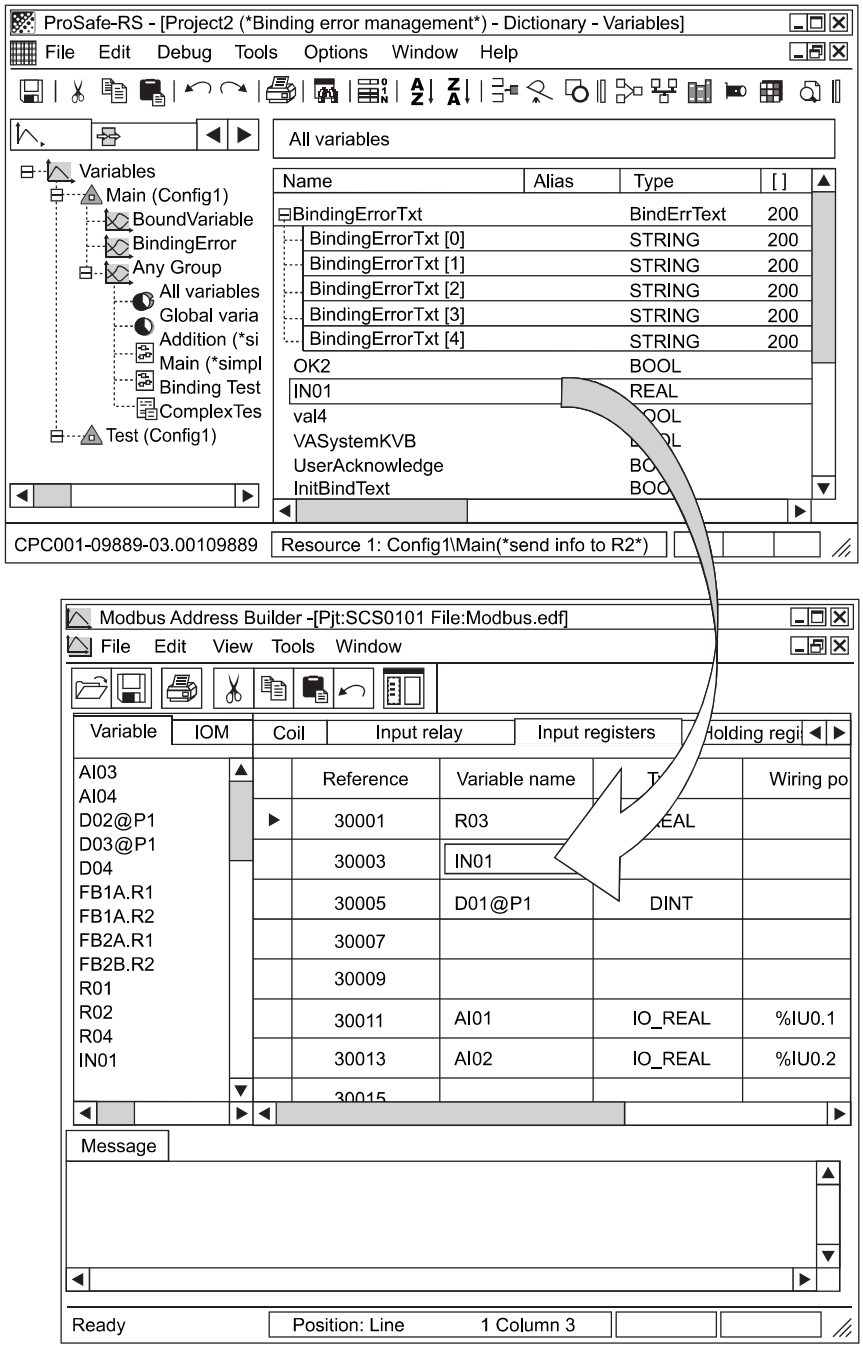


Figure F1.5.1-1 Drag and drop from Dictionary View

IMPORTANT

Changing a name and type of a variable in Dictionary View will not change the corresponding definition in Modbus Address Builder. Make the corresponding modifications in Modbus Address Builder according to changes.

- If a variable is added
  Use Modbus Address Builder and assign a reference number to the variable as necessary.
- If a variable name is changed
  Change the corresponding variable name in Modbus Address Builder as well.
- If a variable is deleted
  Delete the corresponding variable in Modbus Address Builder.

F1.5.2 Window configuration of Modbus Address Builder

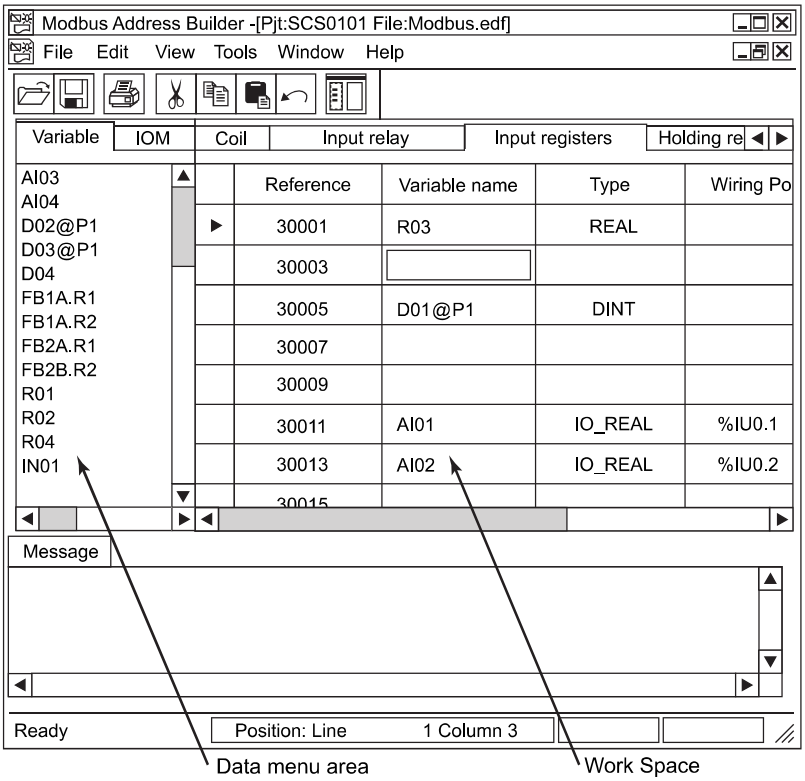


Figure F1.5.2-1 Window configuration of Modbus Address Builder

The Modbus Address Builder window mainly consists of the data menu area and work space.

Data menu area

The data menu area of Modbus Address Builder contains two tabs, the Variable tab and the IOM tab. Modbus Address Builder allows setting variable names only.

Variable tab

The Variable tab displays a list of variables that can be defined. The variable names displayed change depending on the type of Modbus devices displayed in the work space.

Variables that have been defined already at the time a variable was set or deleted are deleted from the list and not displayed.

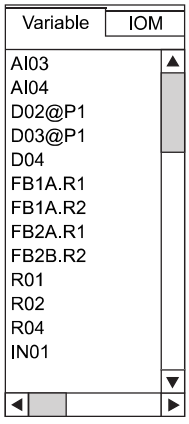


Figure F1.5.2-2 Data menu area - Variable tab

IOM tab

When the input relay tab or the input register tab is displayed, in the workspace the IOM tab becomes available.

For an Input Relay, a discrete input module will be displayed; while for an Input Register, an analog input module will be displayed.

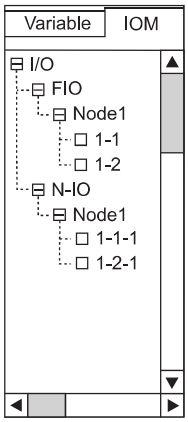


Figure F1.5.2-3 Data menu area - IOM tab

Modbus device tabs

The following tabs are provided in the Modbus Address Builder workspace:

- Coil tab
- Input relay tab
- Input registers tab
- Holding registers tab

Reference numbers in tabs

Each tab displays the reference numbers.

TIP

The range of reference numbers is expanded in the following manner for new SCS projects that are created in SENG in R4.08.00 or later. The applicable SCSs are SCSP1/SCSU1/SCSP3/SCSL2.

- Coil tab
  Range of reference numbers: 00001 to 09999

  Example:

  00001, 00002, 00003, ... , 09999

  Output devices of 1 bit per channel (allows both input and output)
- Input relay tab
  Range of reference numbers: 10001 to 19999

  Example:

  10001, 10002, 10003, ... , 19999

  Input devices of 1 bit per channel (allows input only)
- Input registers tab
  Range of reference numbers: Odd numbers between 30001 and 39999

  Example:

30001, 30003, 30005, ... , 39999

Input registers of 16 bits per channel (allows input only)

Each register is assigned to a 32-bit data, i.e. 2 words compose one data.

- Holding registers tab
  Range of reference numbers: Odd numbers between 40001 and 49999

  Example:

  40001, 40003, 40005, ... , 49999

  Output registers of 16 bits per channel (allows both input and output)

  Each register is assigned to a 32-bit data, i.e. 2 words compose one data.

Items displayed in tabs

Each tab displays the following items: Some items are not displayed depending on the tab. The user can set values only in the Variable name column.

- Reference
  Addresses of Modbus devices. These are displayed in advance in numerical order.

  This item is commonly displayed for all the tabs.

- Variable Name
  Variable names to be assigned.

  This item is commonly displayed for all the tabs.

- Type
  Types of variables. These are displayed once variable names are determined.

  This item is commonly displayed for all the tabs.

- Comment
  Comments attached to variables. These are displayed once variable names are determined.

  This item is commonly displayed for all the tabs.

- Wiring Position
  Installation positions of channels corresponding to variables. This item is displayed only for the Input relay and Input registers tabs. If the variable type is IO_BOOL in the case of the Input relay tab and IO_REAL in the case of the Input registers tab, the wiring positions are displayed when variables are determined.

  The format for FIO is %IUm.n(X-Y-Z).

  Example: %IU0.0(1-1-1)

  The format for N-IO is %IUm.n(X-A-Y-Z).

  Example: %IU1.0 (2-1-1-1)

F1.6 Data setting using Modbus slave communication

The SCS Modbus slave communication function allows setting data on SCS from the Modbus master. Use external communication function blocks to set SCS data from the Modbus master. Data setting through external communication function blocks does not interfere with the safety loop (interference-free). Make sure to read back and confirm the data set by external communication function blocks, when using the data for safety application.

Data setting using external communication function blocks

It is possible to read and write data of SCS from the Modbus master using the SCS Modbus slave communication function. The Modbus master device sends a data access request to SCS, using Modbus device address as interfaces. Although SCS is not equipped with any actual Modbus devices, it acts as if it has them and responds to the data access requests from the Modbus master.

Data can be set from the Modbus master to the SCS by combining the Modbus slave communication function and external communication function blocks. The Modbus device types that can be used for data setting are coil and holding register. Assign instance names of external communication function blocks to coils and holding registers using Modbus Address Builder.

- To set BOOL-type data, assign an ECW_B instance name to the reference number of a coil.
- To set DINT-type data, assign an ECW_I instance name to the reference number of a holding register.
- To set REAL-type data, assign an ECW_R instance name to the reference number of a holding register.

As a result, data set from the Modbus master are output from the output parameter OUT of the associated external communication function blocks.

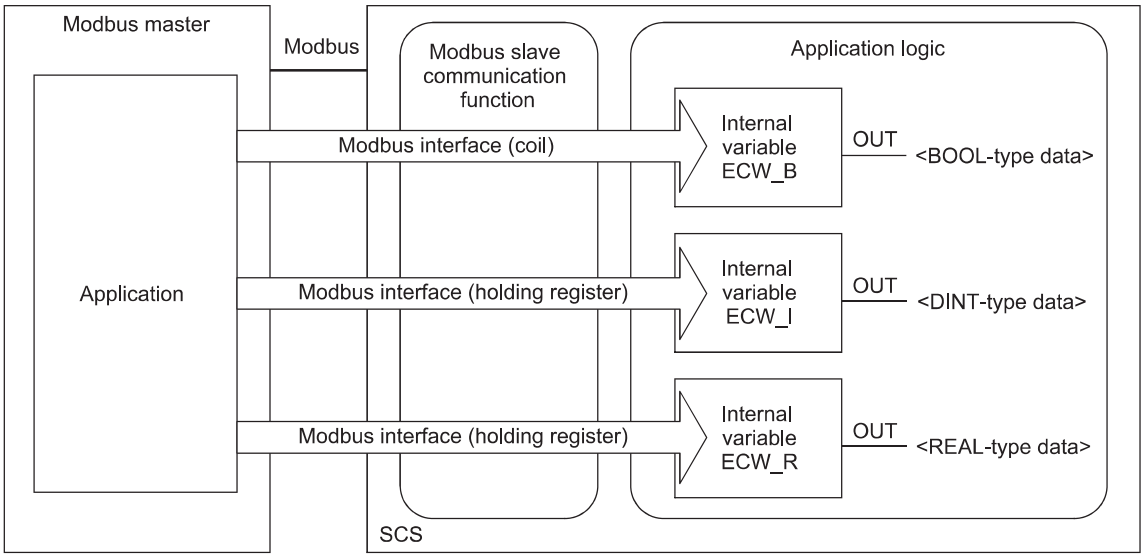


Figure F1.6-1 Data setting using the Modbus slave communication function and external communication function blocks

The user uses Modbus Address Builder to assign reference numbers of these Modbus devices to external communication function blocks and read-back variables.

Table F1.6-1 Modbus devices used for setting and read-back

Data type (*1)	Write register (*2)	Read register (*3)
BOOL	Coil	Input relay
DINT	Holding register	Input register
REAL	Holding register	Input register

*1: Assignation in Modbus Address Builder
*2: Assign registers to external communication function blocks
*3: Assign to readback variables (the READBACK variables in the following figure, "Figure Readback application")

BOOL-type data is set using the following procedure.

1. Use Modbus Address Builder to assign a reference number of a coil to ECW_B (BOOL-type external communication function block).
2. In Modbus Address Builder, assign a reference number of an input relay to a read-back variable.
3. The Modbus master (an external device) sets an address in a request message based on the reference number of the coil and writes data.
4. The Modbus master (an external device) sets an address in a request message based on the reference number of the input relay and reads back data.

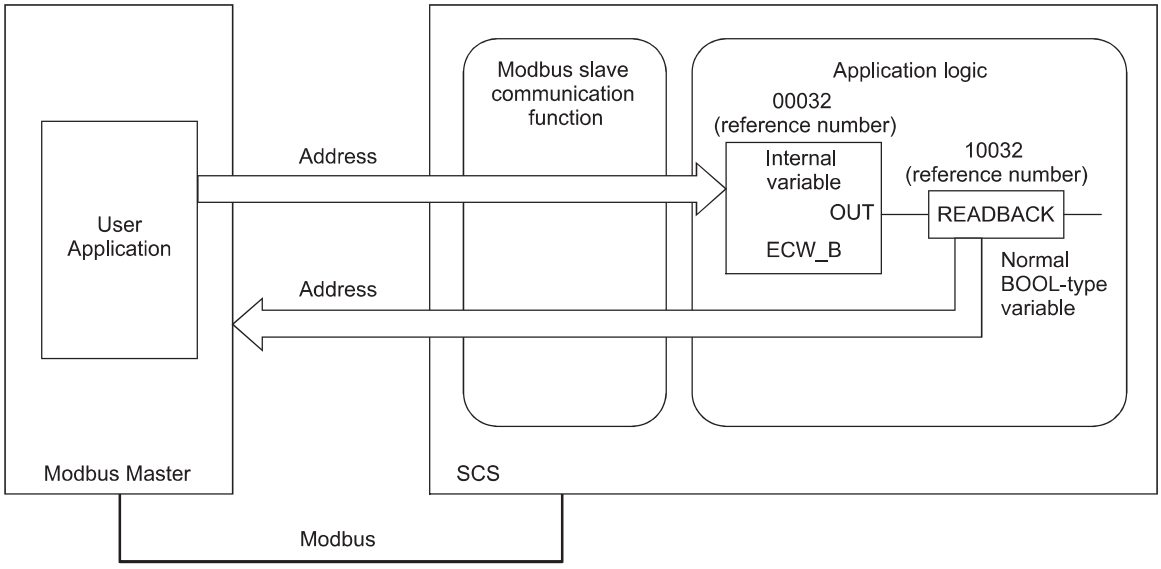


Figure F1.6-2 Readback application

SEE ALSO

For more information about Modbus Address Builder, refer to:

F1.5.1, “Definitions in Modbus Address Builder” on page F1-12

For more information about reference numbers, refer to:

“● Data” on page F1-25

For more information about external communication function blocks, refer to:

B6., “Data setting using external communication function blocks” on page B6-1

● Restrictions on the number of data setting communication operations using Modbus slave communication

On receiving a data setting request from the Modbus master, SCS returns a response and retains the request it accepted.

- A data setting request message from the Modbus master is referred to as a "request" here. Up to 32 data values can be specified in a request.
- Up to four requests can be retained across all Modbus slave communication at the same time.
- SCS will process the retained data setting requests from the Modbus master four requests per second at maximum when the scan period of the application logic is shorter than 250 ms. When the scan period is 250 ms or longer, SCS will process one request in one scan period. If SCS also retains any request from FCS and/or HIS for data setting via tag name interface in addition to requests from the Modbus master, the SCS will process only one request in one scan period in the order of acceptance.
- SCS responds with an error if the number of retained requests is four when SCS receives a request from the Modbus master.

IMPORTANT

Periodical data setting will result in a writing error. Do not set data periodically from the Modbus master.

Confirming data set using Modbus slave communication

When setting data from the Modbus master using Modbus slave communication, it is necessary to perform readback for checking the data. When performing a readback, the application logic should be designed as shown in the previously listed "Figure Readback application." Data is set to an external communication function block and the data is read back from a variable connected to an OUT (READBACK variable in the previous figure).

F1.7 Messages communication

In data communication between the Modbus master and SCS, SCS sends a response message in response to a request message from the Modbus master. When SCS detects an error relevant to the communication module, the SCS sends the diagnostic information message through the control bus.

Request message from the Modbus master

The request message from the Modbus master is composed of the following information according to the communication module used.

- For serial communication modules
  - Slave address
  - Function code
  - Data
  - Error check code
- For Ethernet communication modules
  - Transaction identifier
  - Protocol identifier
  - Field length
  - Unit identifier
  - Function code
  - Data

Slave address (specific to serial communication modules)

A slave address is a station number (1 to 247) that is set for a Modbus slave.

The Modbus master communicates only with the SCS with a matching slave address. A request message from the Modbus master is received by all the Modbus slaves. Of these, only the SCS whose slave address matches the one in the request message processes the request according to the received message.

Function code

The function codes supported on an SCS for request messages are as follows:

Table F1.7-1 Function codes supported on an SCS

Function code (decimal)	Description	Maximum size	Remark
01	Read Coil Status	512 bits	512 bits = 32 words
02	Read Input Status	512 bits	-
03	Read Holding Registers	124 words (62 or 124 data units)	When 16-bit Modbus master support mode is disabled, up to 62 data units (32 bits per unit) can be read. When enabled, up to 124 data units (16 bits per unit) can be read.

Continues on the next page

Table F1.7-1 Function codes supported on an SCS (Table continued)

Function code (decimal)	Description	Maximum size	Remark
04	Read Input Registers	124 words (62 or 124 data units)	When 16-bit Modbus master support mode is disabled, up to 62 data units (32 bits per unit) can be read. When enabled, up to 124 data units (16 bits per unit) can be read.
05	Force Single Coil	1 bit	Restriction from protocol
06	Preset Single Register	1 word (16 bits)	Can be used when 16-bit Modbus master support mode is enabled in SCS Constants Builder. Cannot be used by default.
08	Loopback Diagnostic Test	-	Can only be used for serial communication modules.
15	Force Multiple Coils	32 bits	-
16	Preset Multiple Registers	64 words (*1) (32 or 64 data units)	When 16-bit Modbus master support mode is disabled, up to 32 data units (32 bits per unit) can be set. When enabled, up to 64 data units (16 bits per unit) can be set.

*1: If an even number is specified for the reference number, the maximum size becomes 63 words (63 data units).

Cautionary notes on function codes

Normally, analog data used in SCS are 32-bit signed integer or 32-bit floating point data. Because an input register or holding register is assigned to 32-bit data, one data unit consists of two words. Note the following points when using these data:

IMPORTANT

- When the Modbus master writes 32-bit floating point data to SCS, writing a NaN (not a number) or an infinite value (+INF or -INF) by using Preset Multiple Registers (16) does not result in an error but the data is not written to the SCS.

- When 16-bit Modbus master support mode is disabled (default setting), specify an odd reference number for Read Holding Registers (03), Read Input Registers (04), or Preset Multiple Registers (16). For the number of registers, specify an even number.

IMPORTANT

- When 16-bit Modbus master support mode is enabled, the Modbus master can read and write data including 16-bit integer data, 32-bit signed integer data, and 32-bit floating point data. However, this requires very complicated ProSafe-RS application.
- You must note that simultaneity of the upper and lower words of 32-bit data is not assured if you read or write the upper word and the lower word separately in 16-bit Modbus master support mode.

- When 16-bit Modbus master support mode is enabled, you can specify an odd number or even number for the reference number and the number of registers for Read Holding

Registers (03), Read Input Registers (04), and Preset Multiple Registers (16). Therefore, error codes 10 and 11 (hexadecimal) do not occur in this mode.

- When 16-bit Modbus master support mode is enabled, the following operations will result in an error (error code 02).
  - Writing only to the upper or lower word of 32-bit floating point data by using Preset Single Register (06).
  - Writing only to the upper or lower word of 32-bit floating point data by using Preset Multiple Registers (16) specifying an odd number for the number of registers.
  - Writing only to the upper or lower word of 32-bit floating point data by using Preset Multiple Registers (16) specifying an even number for the reference number.

Data

This contains the detailed information for SCS to execute the requested function. The address information of Modbus devices (coil, input relay, input register and holding register) is the relative number from the first reference number of each device. Reference numbers of ProSafe-RS start from one. The following table shows the relationship between reference numbers and relative numbers.

Table F1.7-2 Relationship between reference numbers and relative numbers

Device	Reference number	Relative number
Coil	0xxxx	0xxxx - 1
Input relay	1xxxx	1xxxx - 10001
Input register	3xxxx	3xxxx - 30001
Holding register	4xxxx	4xxxx - 40001

TIP

The following table shows an example of the "Device & Address" setting that is specified in the Communication I/O Builder of CENTUM when communicating with CENTUM.

Table F1.7-3 Reference numbers and relative numbers when specifying a holding register from CENTUM

Communication module	Address specified by CENTUM	Relative number	Reference number
Serial communication module	A40001	0000	40001
Ethernet communication module	A40000	0000	40001

SEE ALSO

For more information about reference numbers, refer to:

"■ Modbus device tabs" on page F1-18

Error check code (specific to serial communication modules)

Error check information is used to detect errors in messages occurring during a signal transmission (bit errors). A request message sent to SCS contains CRC (Cyclic Redundancy Check) information. SCS verifies the CRC in a request message and discards the message if an error is detected.

Transaction identifier (specific to Ethernet communication modules)

The Modbus master assigns a unique identifier to each request message. SCS copies this value to the transaction identifier field of the response message.

Protocol identifier (specific to Ethernet communication modules)

The Modbus master sets this field to the fixed value of 0. SCS copies this value to the protocol identifier field of the response message.

Field length (specific to Ethernet communication modules)

Byte length of the fields (unit identifier + function code + data).

Unit identifier (specific to Ethernet communication modules)

This field identifies the Modbus slave and is set to the same value as the slave address that is used in the Modbus communication protocol (RTU mode). SCS copies this value to the unit identifier field of the response message.

SEE ALSO For more information about Modbus protocol (RTU mode), refer to:

"■ Supported Modbus protocol" on page F2-2

Response message from SCS

SCS sends a response message when it receives a request message from the Modbus master. The response message that SCS sends differs depending on whether the request message is sent normally or abnormally. In some cases, SCS does not send a response message in response to a request message.

Response message under abnormal conditions

When errors other than transmission errors are detected in a request message, or when the SCS is processing the request message, the SCS sends the response message with the following information. The format of the response message differs depending on the communication module used.

- For serial communication modules
  - Slave address
  - Function code: The function code in a request message plus 0x80
  - Error code
  - Error check code
- For Ethernet communication modules
  - Transaction identifier
  - Protocol identifier
  - Field length
  - Unit identifier
  - Function code: The function code in a request message plus 0x80
  - Error code

Details of error codes to indicate abnormal conditions are as follows.

Table F1.7-4 Error codes

Error code (hexadecimal)	Meaning of error
01	Function code error (non-existing function code)
02	Coil, input relay, register number error (out of range)

Continues on the next page

Table F1.7-4 Error codes (Table continued)

Error code (hexadecimal)	Meaning of error
03	Error of the number of coils, input relays, or registers (out of range)
04	CPU not started.
05	Another request message with the same transaction identifier is received while a request is being processed.(*1)
06	Another request message with a different transaction identifier is received while a request is being processed.(*1)
07	Unsupported diagnostic loop-back code(*2)
10	Even number specified as the register reference number.(*3)
11	Odd number specified as the number of registers (*3)
12	Data setting error • The number of simultaneously writing exceeds four. • Writing size exceeds limit. • Writing to an undefined variable or write-inhibited variable attempted.
13	Access error during online change download During online change download, it is not possible to read from/write to function block instances or variables whose types have been changed.

*1: Specific to Ethernet communication modules
*2: Specific to Modicon serial communication modules
*3: This error does not occur when 16-bit Modbus master support mode is enabled.

Response message in normal conditions

When the request message is sent normally, the following response message is sent. The response message differs depending on the content of the request message and the communication module used.

Table F1.7-5 Response messages depending on the content of the request message and the communication module used

Content of request message	Communication module	Response message
For functions of single coil status change, writing to a single holding register, or loop back	Serial communication module	The same message as the request message
	Ethernet communication module	The same message as the request message
For functions of multiple coil status changes or writing to multiple holding registers	Serial communication module	Slave address Function code Error check code Start number Number of coils or holding registers
	Ethernet communication module	Transaction identifier Protocol identifier Field length Unit identifier Function code Start number Number of coils or holding registers
In the case of read function	Serial communication module	Slave address Function code Error check code Read data
	Ethernet communication module	Transaction identifier Protocol identifier Field length Unit identifier Function code Read data

Cases where no response is made

SCS does not respond to a request in the following cases:

- A transmission error of a request message is detected (overrun, framing error, parity error or CRC error)
- Transmission specification setting values are invalid
- The slave address in a request message does not correspond to the slave address set on the communication module
- The time interval between receiving one character and the next character is longer than the setting value of the reception inter-character timer
- A protocol related error occurs (for example, a transmission is performed just when being responding to a request)
- Definitions of the serial communication module are being online change downloaded
- Definitions of Modbus communication are being changed

Response time

The response time refers to the time from when SCS receives a request message to when it starts to transmit the response message. The transmission time is not included.

Response time = (Message receiving and sending processing time) +
(Modbus message reading and writing processing time)

Set the message receiving and sending processing time to 20 ms.

The time taken by Modbus message reading and writing processing varies as shown in the following table, according to the scan period of application logic and the number of communication ports. The Modbus message reading and writing are processed during the idle time after the processing of application logic is completed.

Table F1.7-6 Modbus message processing time and the combination of scan period of application logic and the number of communication ports

Scan period	Number of communication ports per SCS	Processing time of Modbus message reading and writing
200 ms or longer	-	0 to the scan period of application logic
Shorter than 200 ms	2 ports or less	0 to the scan period of application logic
	3 ports or more	0 to (The scan period of application logic x 2)

TIP

- For the Ethernet communication module, take the number of ports that appear in the above description for the number of connections.
- If you install two serial communication modules or Ethernet communication modules or mix of both in an SCS and use two ports per module, the number of communication ports per SCS is regarded as three or more.

IMPORTANT

- The longest time it takes for data to be read by the Modbus master is as follows:

  Maximum data update time = transmission time + scan period of external connection function

- If a writing request from the CENTUM integration function coincides with those from a Modbus master on another port, notification of the writing request to the application logic will be delayed for the number of writing requests. Therefore, the longest time it takes for notification of a write operation from the Modbus master to reach the SCS application logic is as follows:

  Maximum data update time = transmission time + scan period of the application logic x number of writing requests from the external connection function

Diagnostic information messages

If a communication module is faulty, the SCS send a diagnostic Information message to SENG and/or HIS through the control bus. This section describes the SCS diagnostic Information messages.

Error occurrence/recovery to normal state on communication module

When an error occurs in the communication module, or when the module recovers from an error, an IOM Fail diagnostic information message, or an IOM Recover diagnostic information message, respectively, is sent through the control bus.

The configuration error occurs if the communication driver cannot operate due to configuration mismatch. For example, this error occurs if the communication driver has not been downloaded to the communication module or if an application program different from the defined communication driver has been downloaded.

TIP

Communication modules ALR111, ALR121, and ALE111 must be loaded with a driver for Modbus communication.
After you replace these communication modules, perform IOM download to the new modules.

However, if the communication driver of SCS is already downloaded to the replaced module, the module starts normally. In this case, you do not need to perform IOM download.

SEE ALSO

For more information about diagnostic information messages for communication module error occurrence and recovery to normal state, refer to:

3.1, “Safety Control Station Error Occurrence and Recovery Messages (Message Numbers 0001 through 0094)” in Messages Reference Manual (IM 32P02B10-01EN)

When a communication error occurs

When a communication error occurs, no system alarm message is sent because the Modbus master is assumed to handle the error.

When downloading the communication driver

When downloading the communication driver to the communication module, system alarm messages indicating the start of the download, and the completion or abnormal termination of the download, are sent through the control bus.

SEE ALSO For more information about system alarm messages for communication driver downloads, refer to:

3.2, “Safety Control Station Status Change Related Messages (Message Numbers 0425 through 0480)” in Messages Reference Manual (IM 32P02B10-01EN)

When a communication module is added online

Communication modules can be added or removed online. When a communication module is added, diagnostic information messages (IOM Fail, and then IOM Recover) are sent through the control bus.

SEE ALSO For more information about diagnostic information messages for communication module error occurrence and recovery to normal state, refer to:

3.1, “Safety Control Station Error Occurrence and Recovery Messages (Message Numbers 0001 through 0094)” in Messages Reference Manual (IM 32P02B10-01EN)

F1.8 Troubleshooting

If a communication module error occurs, you can use the SCS Maintenance Support Tool to acquire information on the communication module and communication error information. This section describes typical troubleshooting cases.

The status display window shows the status of ALR111/121 or ALE111 in red

If the status of the communication module appears in red in the status display window of the SCS Maintenance Support Tool, check the error code that is related to the input/output module in the diagnostic information message.

There is no response and communication fails

- Check if the transmission specifications are consistent with those of the master.
- Check if the cable wiring complies with the specifications.
- Analyze the communication log for the cause of the communication error by using the SCS Maintenance Support Tool.
- Check if there is enough CPU time available. Response may be delayed when the CPU load is high.

A response message under abnormal conditions is received

- Check if the function code that is included in the message is correct.
- Check if the Modbus master sent another request message to the SCS before receiving a response message through a given connection. (Specific to Modbus TCP)

Connection cannot be established and communication fails (specific to Modbus TCP)

- Check if the destination IP address and port number are correct.
- If the Modbus master fails without a notification of the communication termination (socket close) to the Modbus slave while they are communicating through an Ethernet communication module, the slave becomes ready for reconnection in up to 34 seconds.

F2. Serial communication modules

SCS uses a serial communication module to send and receive data to and from the Modbus master (external device).

This section describes the connection between the Modbus master and SCS through the serial communication module and the required I/O Parameter Builder settings when performing RS original engineering.

The parameter setting items that are required in I/O list engineering are the same as those for RS original engineering.

F2.1 Connection between the Modbus master and SCS

This section describes the connection configuration between the Modbus master and SCS, the Modbus protocol, serial communication modules, and cable connections.

Connection configuration of the serial communication module

The following is an example of connection using YOKOGAWA STARDOM autonomous controller FCN (Field Control Node) as the Modbus master.

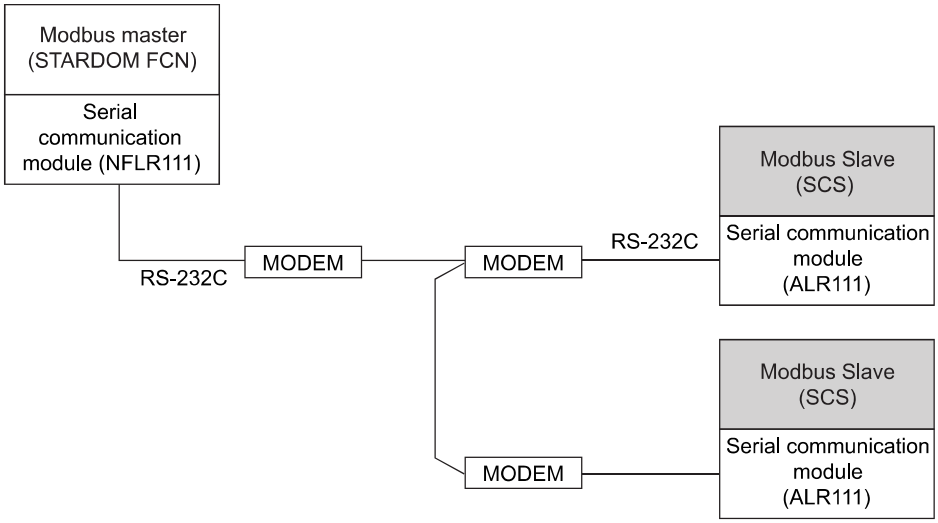


Figure F2.1-1 Example of connection between the Modbus master and SCS (ALR111) (using a STARDOM FCN as the Modbus master)

An SCS communicates with the STARDOM FCN, the Modbus master, via a serial communication module (NFLR111 and ALR111 in the previous example).

Supported Modbus protocol

The Modbus protocol defines communication procedures and message formats between one master and multiple slaves when performing serial communication.

The Modbus protocol for the SCS Modbus slave communication has the following features:

- Only the master can initiate communication via the Modbus protocol. The master requests data reference or setting, and the slave responds to the request.
- The signal transmission between the master and slaves can be performed in either the RTU (Remote Terminal Unit) mode or the ASCII mode. SCS supports the RTU mode only.

Transmission specifications of serial communication modules

The SCS transmission specifications when using a serial communication module are as follows:

Table F2.1-1 Transmission specifications when using a serial communication module

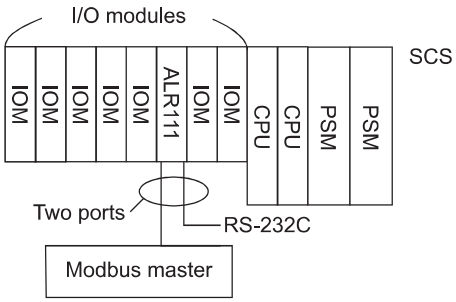
Item		Description(*1)	Builder specification(*2)	Remark
Interface		RS-232C	Yes	ALR111
		RS-422/RS-485 (4-wire system)		ALR121
Synchronization method		Start-stop synchronization	-	
Baud rate		1200, 2400, 4800, 9600, [19200], 38400 bps	Yes	
Start bits		Fixed to 1	-	
Data bits		7 to [8]	-	Fixed to 8 in Modbus RTU mode
Stop bits		[1], 2	Yes	
Parity		None, Odd, [Even]	Yes	
Control Line	RS control	Yes, [No]	Yes	Valid only for ALR111
	DR check	[Yes], No	Yes	Valid only for ALR111
	CD check	Yes, [No]	Yes	Valid only for ALR111
Time monitoring	Transmission enable monitoring time	0 to 99990 (ms) [1000] Specify in units of 10 ms	-	Fixed to 1000 ms for Modbus
	Reception character interval timer	0 to 99999 (ms) [10] Specify in units of 1 ms	Yes	
	Character internal monitoring timeout	[Do not set], Set	-	Fixed to Do not set for errors in Modbus RTU mode
Text frame	Reception start character	1 character, [None]	-	Fixed to None for Modbus
	EOT character	1 character, 2 characters, [None]	-	Fixed to None for Modbus
	Maximum number of transmit characters	Up to 512 bytes	-	
	Maximum number of receive characters	Up to 512 bytes	-	
Station number		1 to 247	Yes	
Option 1 to 4		Fixed to 0	-	
MODBUS RTU/ASCII		RTU(*3)	-	

*1: [ ] indicates a default value (recommended value).
*2: Yes: Can be specified.
-: Cannot be specified.
*3: Only the RTU mode is supported. The ASCII mode is not supported.

Mounting of a serial communication module

SCS uses ALR111/ALR121, as a serial communication module. ALR111/ALR121 is used by mounting in SCS and connecting a serial communication cable.

If ALR111 is mounted, use an RS-232C cable. If ALR121 is mounted, use an RS-422/RS-485 cable.



• ALR111: Serial communication module (RS-232C)
• ALR121: Serial communication module (RS-422/RS-485)

Figure F2.1-2 Example of mounting a serial communication module to SCS

The following table shows the communication capacity of ALR111/ALR121.

Table F2.1-2 Communication capacity of ALR111/ALR121

Item	Maximum number
Number of communication modules that can be mounted	2 modules/SCS (*1) (*2)
Number of ports used per communication module	2 ports

*1: Total number of ALR111/ALR121/ALE111 for the Modbus slave communication that is mounted to the same SCS
*2: Communication modules for the subsystem communication and DNP3 communication are not included in the count.

IMPORTANT

ALR111/ALR121 cannot be installed in any I/O node that is 5 km or further away from the CPU node.

● Status display

The operation status of serial communication modules can be checked by observing the status display LEDs on the module or a system status display view on HIS.

SEE ALSO For more information about the types and functions of status display LEDs of communication modules, refer to:

"■ Inspection by checking status lamps" in E2., "Routine maintenance" in Hardware User's Guide (IM 32P06C10-01EN)

■ Cable connection when using ALR111

You can connect the Modbus master and ALR111 by using a modem.

SEE ALSO For more information about connections and connectors of ALR111, refer to:

D1.4.1, "Connection of the serial communication module (RS-232C)" in Hardware User's Guide (IM 32P06C10-01EN)

For more information about modem connection, refer to:

"■ Connecting external devices to ALR111" in D1.4.1, "Connection of the serial communication module (RS-232C)" in Hardware User's Guide (IM 32P06C10-01EN)

■ Precautions when wiring signal lines

This section describes the precautions when wiring the ALR111 signal lines.

SEE ALSO For more information about ALR111 connector signals, refer to:

D1.4.1, “Connection of the serial communication module (RS-232C)” in Hardware User's Guide (IM 32P06C10-01EN)

CD signal line

When the CD signal is ON, data is being transmitted to the receiver. Wire a signal line that turns ON when the connection destination sends data to the CD signal. In general, wire the RS signal of the connection destination to the CD signal.

If a signal line that turns ON when the connection destination sends data is not available, wire a signal that is always ON, for example the ER signal line of the ALR111 itself, to the CD signal pin.

When the CD check is enabled, transmission is not allowed when the CD signal is ON (because data is being transmitted from the other end of the line). Turn OFF the CD check if the CD signal line is always in the ON status. The check is turned OFF by default.

ER (DTR) signal line

The ER signal turns ON after the serial communication module has completed the startup processing and is ready to receive and send data. Use this signal to judge whether or not the serial communication module can receive data at the connection destination.

DR (DSR) signal line

The DR signal line is used to judge whether the device to which the ALR 111 is wired can receive data.

When the DR check is enabled, data can be sent while the DR signal is ON. Wire a signal line that turns ON when the connected device can receive data to the DR signal pin.

To disable this check, specify [No] for the DR check, or wire a signal line that is always ON to the DR signal pin.

RS (RTS)/CS (CTS) signal lines

For RS signal setting, either [No] (always ON) or [Yes] (ON at transmission) can be specified for the RS control. If the RS signal connected to the device should be ON while transmitting and stay OFF otherwise, specify [Yes] for the RS control.

Data is transmitted when the CS signal is ON. Wire the line in such a way that the CS signal line turns ON at transmission.

F2.2 Definitions in I/O Parameter Builder

This section explains the settings of communication module to perform Modbus slave communication through RS original engineering. Settings for the serial communication modules can be configured in the Port 1 tab and Port 2 tab of I/O Parameter Builder.

SEE ALSO For more information about display method and window configuration for the I/O Parameter Builder, refer to:

Appendix 2.2.2, “I/O Parameter Builder” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about parameter tabs in the serial communication module, refer to:

Appendix 1.2, “Settings for modules” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Port 1, Port 2 tab

The following items can be set in the [Port 1], [Port 2] tab.

The settings of each item can be changed online download, but the corresponding module will restart after download.

Table F2.2-1 Port 1, Port 2 tab

Title		Description	Remark
Baud Rate		Set the baud rate	-
Stop Bits		Set the stop bit	-
Parity		Specify the type of parity	-
Control Line	RS Control	Specify whether or not to perform RS control during ALR111 transmission	Valid only for ALR111
	DR Check	Specify whether or not to perform DR signal check during ALR111 transmission	Valid only for ALR111
	CD Check	Specify whether or not to perform CD signal check during ALR111 transmission	Valid only for ALR111
	Reception Inter-Character timer	Specify the monitoring time of reception character interval during reception by the ALR111/ALR121	-
Station Number		Specify the slave address of the Modbus slave	-
Option 1 to 4		Option items	Fixed to 0.

Baud Rate

Specify the baud rate of communication. Select from 1200, 2400, 4800, 9600, 19200 and 38400 bps. The default is 19200 bps.

Stop Bits

Specify the stop bits of communication. Select 1 bit or 2 bits. The default is 1 bit.

Parity

Specify the parity. Select None, Odd or Even. The default is Even.

RS Control

Specify whether or not to perform RS control during ALR111 transmission. The setting is only valid for the ALR111. The default is not to perform the RS control function.

- Without RS control
  Always set the RS signal cable to ON regardless of the data transmission from the ALR111.
- With RS control
  Turn the RS signal cable ON when data is transmitted from the ALR111 and OFF at the completion of transmission.

DR Check

Specify whether or not to perform DR signal line check during ALR111 transmission. The setting is only valid for the ALR111. The default is to perform the DR check function.

- Without DR check
  ALR111 transmission data regardless of the status of the DR signal cable.
- With DR check
  ALR111 transmission data only if the DR signal cable is ON. A no-response error occurs if the DR signal does not turn ON after the transmission enable monitoring time has elapsed (the response data is discarded).

The DR signal is used to connect to the ER (data terminal ready) signal line to communicate with and to determine whether or not the ER signal line at the connection destination is able to receive character data (normal operation). If the ER signal line cannot be used, set "without DR check" or wire the line in such a way that the DR signal line is switched ON at all times (*1) .

*1: For example, connect the RS signal line to the DR signal pin of its own.

CD Check

Specify whether or not to perform CD signal check during ALR111 transmission. The default is not to perform the CD check function.

- Without CD check
  ALR111 transmission data regardless of the status of the CD signal cable.
- With CD check
  ALR111 transmission data if the CD signal is OFF. A no-response error occurs if the CD signal does not turn OFF after the transmission enable monitoring time has elapsed.

Reception Inter-Character timer

The reception Inter-Character timer (reception Inter-Character timeout setting value) is a function that monitors the time between characters are received when the ALR111/ALR121 module receives data. In the Modbus (RTU mode) binary communication, the communication is regarded as completed if this duration of time or longer elapses between two character receptions.

If the communication is performed through a modem with data buffering or similar functionality, specify this value taking into account the communication delay (inter-character delay) due to buffering by the modem. However, this affects the communication time because the communication is regarded as completed based on this time.

Default: 10 ms

Setting range: 0 to 99999 ms

IMPORTANT

If multiple slave devices are connected on the same line, set the time so that it corresponds to the transmission of approximately 20 characters in the serial communication (20 ms for 9600 bps, 10 ms for 19200 bps). If there is any slave device with a Reception Inter-Character Timer value larger than those of other slave devices, reception is not performed properly on that device and a non-response error occurs.

Station Number

Specify the slave address of the Modbus slave.

Default: 1

Setting range: 1 to 247

Option 1 to 4

Always set 0 for these options.
Default: 0 (for all)

F3. Ethernet communication modules

SCS uses an Ethernet communication module to send and receive data to and from the Modbus master (external device).

This section describes the connection between the Modbus master and SCS through the Ethernet communication module and the required I/O Parameter Builder settings when performing RS original engineering.

The parameter setting items that are required in I/O list engineering are the same as those for RS original engineering.

F3.1 Connection between the Modbus master and SCS

This section describes the connection configuration between the Modbus master and SCS, the Modbus protocol, and the Ethernet communication module.

Connection configuration of the Ethernet communication module

The following figure shows an example of a connection using the YOKOGAWA STARDOM autonomous controller FCN (Field Control Node) as the Modbus master.

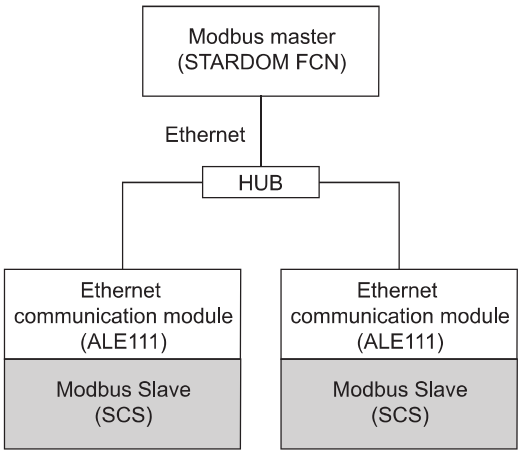


Figure F3.1-1 Example of a connection between the Modbus master and SCS (ALE111) (using a STARDOM FCN as the Modbus master)

An SCS communicates with the STARDOM FCN, the Modbus master, through an Ethernet communication module (ALE111 in the previous example).

Supported Modbus protocol

The Modbus protocol that is supported on Ethernet communication modules is the Modbus TCP protocol. The Modbus TCP protocol uses TCP/IP (Ethernet) for Modbus slave communication.

- The Modbus TCP protocol can be used to communicate with multiple Modbus slaves at almost the same time.
- The Modbus master can send a request message to multiple Modbus slaves at the same time and wait for response messages.

Transmission specifications of Ethernet communication modules

The SCS transmission specifications when using an Ethernet communication module are as follows:

Table F3.1-1 Transmission specifications when using an Ethernet communication module

Item	Description	Builder specification(*1)	Remark
Interface	Ethernet (IEEE802.3)	-	-
	10BASE-T	-	-
Baud rate	10 Mbps	-	Fixed to 10 Mbps(*2)

Continues on the next page

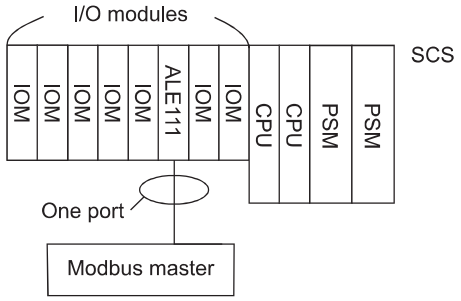
Table F3.1-1 Transmission specifications when using an Ethernet communication module (Table continued)

Item	Description	Builder specification(*1)	Remark
Transmission method	Half-duplex	-	Fixed to half-duplex
Port number	502	Yes	Modbus TCP port number. The default value is 502. (*3)
Number of connections	2	-	-
Number of transactions per connection (*4)	1	-	When two connections are used, the number of transactions per SCS is 2.
Data format	Binary	-	Fixed to binary
Option 1 to 4	0 to 0xFFFFFFFF or -2147483648 to 2147483647	Yes	Reserved for extensions

*1: Yes: Specification required
-: Specification not required
*2: Network auto-negotiation cannot be specified in hub settings.
*3: The default value is recommended.
*4: This is the number of request messages that SCS can process per connection. The Modbus master should not send more request messages to an SCS than this value, regardless of the transaction identifier of the request message. If sent, the SCS sends a response message with an error code set.

Mounting of an Ethernet communication module

SCS uses the ALE111 as an Ethernet communication module. Install the ALE111 in the SCS and connect it to the Modbus master by using an Ethernet cable.



• ALE111: Ethernet communication module

Figure F3.1-2 Example of mounting an Ethernet communication module to SCS

IMPORTANT

When using ALE111, use the style S1 module with unit revision U:2 or later. The unit revision is indicated on the top of the module. However, the unit revision is not indicated if it is U:0.

The following table shows the communication capacity of ALE111.

Table F3.1-2 Communication capacity of ALE111

Item	Maximum number
Number of communication modules that can be mounted	2 modules/SCS (*1) (*2)
Number of ports used per communication module	1 ports

*1: Total number of ALR111/ALR121/ALE111 for the Modbus slave communication that is mounted to the same SCS
*2: Communication modules for the subsystem communication and DNP3 communication are not included in the count.

IMPORTANT

ALE111 cannot be installed in any I/O node that is 5 km or further away from the CPU node.

Status display

The operation status of Ethernet communication modules can be checked by observing the status display LEDs on the module or a system status display view on HIS.

SEE ALSO For more information about the types and functions of status display LEDs of communication modules, refer to:

"■ Inspection by checking status lamps" in E2., "Routine maintenance" in Hardware User's Guide (IM 32P06C10-01EN)

F3.2 Definitions in the I/O Parameter Builder

This section explains the settings of Ethernet communication module to perform Modbus communication through RS original engineering. Settings for the Ethernet communication modules can be configured in the Module tab of I/O Parameter Builder.

SEE ALSO For more information about display method and window configuration for the I/O Parameter Builder, refer to:

Appendix 2.2.2, "I/O Parameter Builder" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Module tab of the Ethernet communication module

The following tables show the display-only items and settable items on the Module tab of the Ethernet communication module.

The setting of each item can be changed by online change download, but the target module restarts after online change download.

Table F3.2-1 Display-only items on the Module tab of the Ethernet communication module

Title	Description	Remarks
Node Number	The node number of the node in which the module is mounted	Defined in I/O Wiring View
Slot Number	The slot number of the slot in which the module is mounted	Defined in I/O Wiring View
Device	The model name of the module	Defined in I/O Wiring View
Dual-Redundant	Whether the module is used in a single or dual-redundant configuration	The module cannot be dual-redundant
Device Number	The device number that is assigned to the module	Defined in I/O Wiring View

Table F3.2-2 Setting items on the Module tab of the Ethernet communication module

Title	Description	Remarks
Connection Device	Types of connection devices	-
Comment	A comment regarding the module	-
IP Address	The IP address of the module	-
Subnet Mask	The subnet mask of the module	-
Default Gateway	The default gateway address of the module	-
Port Number	The TCP/IP port number	-
Option 1 to 4	Option items	Fixed to 0.

Connection Device

Set the type of connection device.

Select SCSMDTCP when the Modbus slave communication function should be used.

Default value: SCSMDTCP

SCSMDTCP: Modbus TCP master

SCSDPTCP: DNP3 master (Selectable only when the version of SCSU1 is R3.02.20 or later.)

TIP

If an attempt is made to change the connection device and the selected port number is not the default, the following dialog box appears:

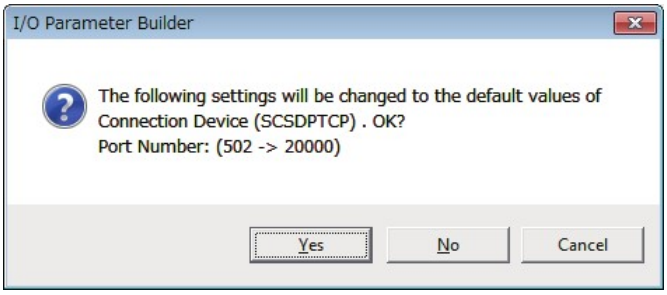


Figure F3.2-1 Connection Device dialog box

Yes: The connection device is changed and the port number is changed to the default.

No: The connection device is changed but the port number is not changed.

Cancel: Neither the connection device nor port number is changed.

Comment

A comment regarding the Ethernet communication module can be entered. This comment can be entered using up to 24 single-byte characters or 12 double-byte characters.

IP Address

Set the IP address of the Ethernet communication module. Enter a desired IP address.

Default:	This field is empty by default; be sure to enter an IP address. If no value is entered, an error occurs when you try to save the settings in the builder.
Format:	nnn.nnn.nnn.nnn
Setting range:	0.0.0.1 to 255.255.255.254 However, do not set the following IP addresses: • Host address digits are all zeros or all ones in binary form. (Examples: 192.168.1.0 and 192.168.1.255 when the subnet mask is 255.255.255.0) • Any of the numbers delimited with a period has leading zeros. (Examples: 192.168.08.09 and 192.168.008.009)

Subnet Mask

Set the subnet mask of the Ethernet communication module. Enter a desired subnet mask.

Default:	This field is empty by default; be sure to enter a subnet mask. If no value is entered, an error occurs when you try to save the settings in the builder.
Format:	nnn.nnn.nnn.nnn
Setting range:	0.0.0.1 to 255.255.255.254 However, do not set the following subnet masks: • Values less than 255.0.0.0 for a class A IP address (Example: 128.0.0.0) • Values less than 255.255.0.0 for a class B IP address (Example: 255.128.0.0) • Values less than 255.255.255.0 for a class C IP address (Example: 255.255.128.0)

Default Gateway

Set the gateway address of the Ethernet communication module. Enter a desired gateway address.

Default: Blank

Format: nnn.nnn.nnn.nnn

Setting range: 0.0.0.1 to 255.255.255.254
However, do not set the following gateway addresses:

- Host address digits are all zeros or all ones in binary form.
(Examples: 192.168.1.0 and 192.168.1.255 when subnet mask is 255.255.255.0)
- Network address digits do not match the IP address.
(IP address is 192.168.1.1 and default gateway address is 192.168.2.2 when the subnet mask is 255.255.255.0.)
- Any of the numbers delimited with a period has leading zeros.
(Examples: 192.168.08.09 and 192.168.008.009)

Port Number

Set the port number for Modbus TCP.

Default: 502

Setting range: 0 to 65535

Option 1 to 4

You must set 0 for these options.

Default: 0 (for all)

F4. Precautions for engineering

The Modbus slave communication function of SCS is for a Modbus master (external device) reading and setting SCS data via Modbus protocols. DCSs supplied by other manufacturers can function as a Modbus master to be connected with SCS. The Modbus slave communication function of an SCS does not affect the safety functions of it.

For Modbus connection, the following communication modules need to be installed in SCS nodes to be connected to other systems.

- RS-232C serial communication module (ALR111)
- RS-422/RS-485 serial communication module (ALR121)
- Ethernet communication module (ALE111)
  When the CPU node of SCS is SSC10D or SSC10S, do not define ALE111.

To set data in SCS from an external device, the External Communication Function Block is used. The External Communication FB allows setting data of a variable of application logic from a Modbus master. In this case, the SCS data must be confirmed by Modbus master by reading back the data.

SEE ALSO For more information about Modbus connection function, refer to:

F1., “Common items regarding the Modbus slave communication function” on page F1-1

For more information about engineering of Modbus slave communication, refer to:

F., “Modbus slave communication” on page F-1

■ Redundancy of Modbus communication

To implement redundant Modbus slave communication, you need to create a user application for that purpose on the Modbus master side.

For serial communication, it is possible to duplex the path of Modbus communication in the following ways.

- Using two serial communication modules
  The communication modules and communication paths are both duplexed. When one module fails, communication can be continued with the other module.
- Using two ports on one module
  When Ports 1 and 2 on the same communication module are used, only the communication paths are duplexed.

For Ethernet communication, it is possible to duplex the path of Modbus communication by using two Ethernet communication modules. The communication modules and communication paths are both duplexed. When one module fails, communication can be continued with the other module.

■ Data setting and reading from Modbus master

The Modbus slave communication function of SCS allows an external device to read the internal variables of SCS (BOOL, DINT, and REAL) and its I/O variables (DI/DO, AI, etc). The External Communication Function Block is used for setting data of these variables. Attentions are needed for data handling when accessing to SCS from the Modbus master. In addition, SCS data is 32-bit, however, access from the Modbus master that handles 16-bit data only is available depending on the settings.

SEE ALSO For more information about data access from the Modbus master that handles 16-bit data only, refer to:

“■ 16-bit Modbus master support mode” on page F1-5

Retry for a communication error

The application in Modbus master must be implemented so as to make retry when an error occurs in Modbus communication.

Response timeout period setting on the Modbus master when communicating with SCSP2/SCSP3/SCSL2

When performing Modbus slave communication with an SCSP2/SCSP3/SCSL2 installed with dual-redundant CPU modules and an Ethernet communication module, you must set five seconds or longer response timeout period on the Modbus master device.

If the control right is switched to the standby-side CPU module while the control-side CPU module is processing for Modbus slave communication, the SCSP2/SCSP3/SCSL2 processes the Modbus communication data again. As a result, it will take a maximum of 5 seconds for the Modbus master to send a request and receive a response.

G. DNP3 slave function

The DNP3 slave function uses DNP3, which is an open protocol, to let the SCS operate as the DNP3 slave and communicate with the DNP3 master, such as SCADA.

This section provides an overview of the DNP3 slave function and explanation of this function, engineering and maintenance on the SENG, and DNP3 communication function block (hereinafter referred to as DNP3 communication FB).

The DNP3 slave function is supported only by SCSU1 of R3.02.20 or later.

SEE ALSO For more information about DNP3 Field Device Profile of the SCS, refer to:

Appendix 2., “DNP3 field device Profile” on page App.2-1

G1. Overview of the DNP3 slave function

The DNP3 slave function of SCS allows the DNP3 master to refer data from SCS or set data to SCS through DNP3 communication. The DNP3 slave function does not affect the safety functions of SCS.

You must install the Ethernet communication module (model: ALE111) to an SCS node for the SCS to communicate with the DNP3 master.

To use the DNP3 slave function, use DNP3 communication FBs. By assigning instances of DNP3 communication FBs to DNP3 data, SCS data can be referred or set from the DNP3 master.

When a variable of the application logic changes, the SCS generates and buffers an event that includes a time stamp and data. This prevents data loss when a communication failure occurs because the DNP3 master can read the relevant event from the SCS's event buffer after the recovery.

Precautions for using the DNP3 slave function

The precautions when using the DNP3 slave function are as follows:

- The DNP3 slave function is supported only by SCSU1 of R3.02.20 or later.
- To use the DNP3 slave function, the CI Server Integration Package is required.
- The DNP3 event buffering function cannot be used simultaneously with the data buffering function that is used when the system is integrated with CI Server.
- The duplexed interface for DNP3 communication can be used on new SCS projects that are created in R4.02 or a later version.

G1.1 DNP3 communication system configuration and components

The DNP3 communication system is configured in such a way that the DNP3 master is connected to the DNP3 slave, such as the SCS or any third-party controller, through Ethernet. The SENG and SCS are connected through the Vnet/IP-Upstream network. The DNP3 communication interface can also be used in a duplexed configuration on SCSU1 of R4.02 or later.

The following figure shows an example of the configuration of a DNP3 communication system where the SENG and SCS are connected through the Vnet/IP-Upstream network.

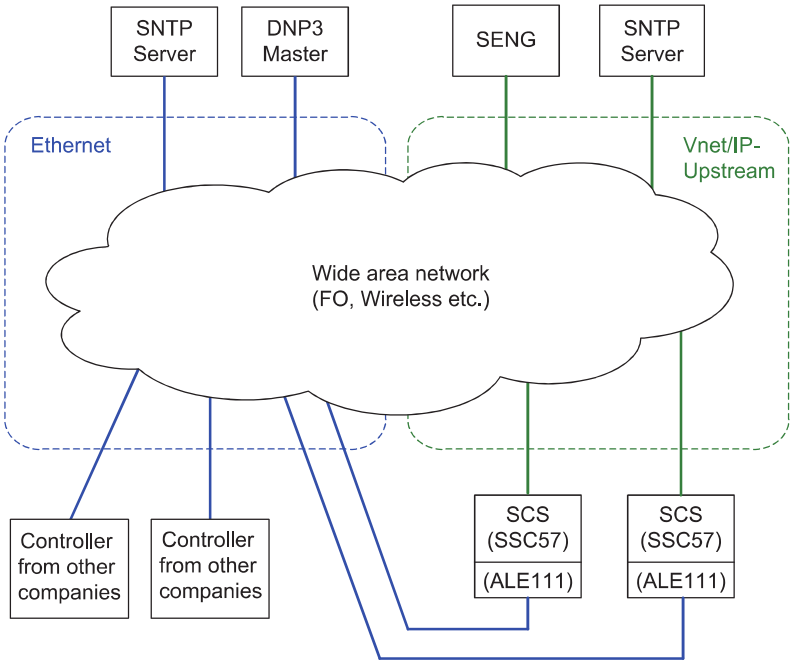


Figure G1.1-1 Example of configuration of a DNP3 communication system where the SENG and SCS are connected through the Vnet/IP-Upstream network

The following figure shows an example of the configuration of a DNP3 communication system where the SENG is connected to the SCS only when required for engineering purposes.

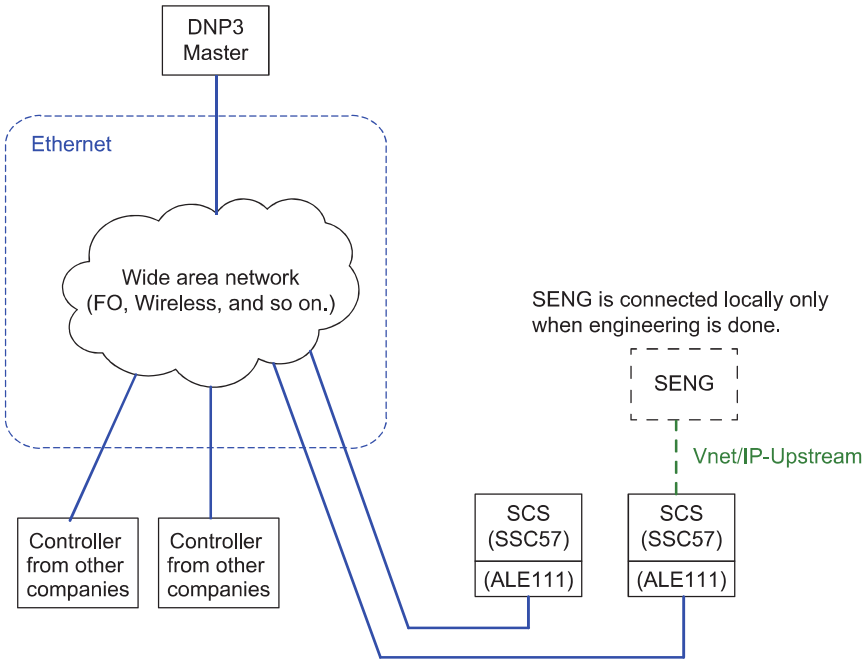


Figure G1.1-2 Example of configuration of a DNP3 communication system where the SENG is connected to the SCS only when required for engineering purposes

The following figure shows an example of the configuration of a DNP3 communication system where the communication interface has a duplexed configuration.

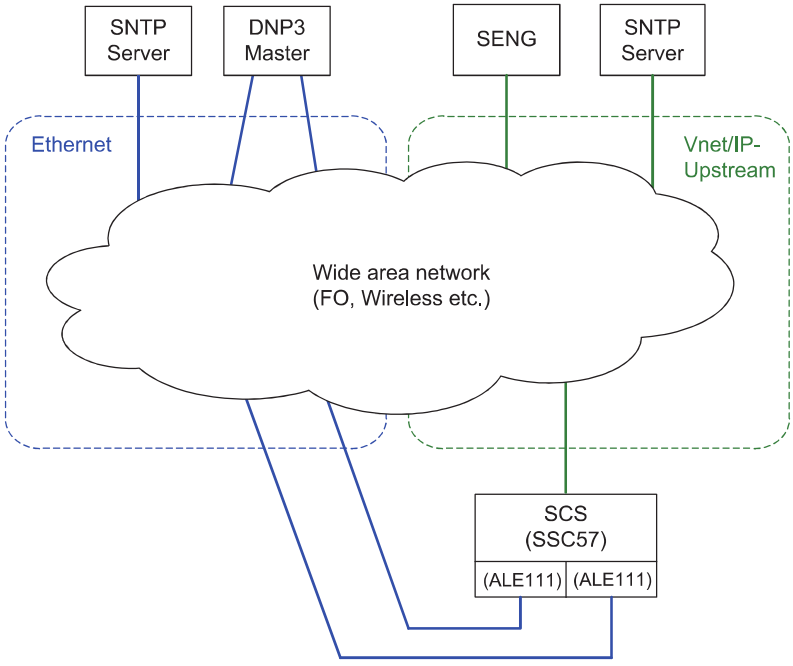


Figure G1.1-3 Example of the configuration of a DNP3 communication system where the communication interface has a duplexed configuration

Any system used in DNP3 communication requires the following components:

- DNP3 master
  It uses the DNP3 protocol to communicate with the DNP3 slave, such as the SCS or any third-party controller.
- SCS
  It uses the DNP3 protocol to communicate with the DNP3 master. One SCS can be connected to one DNP3 master.

The SCS performs DNP3 communication through the Ethernet communication module (model: ALE111). Up to two ALE111 modules per SCS can be used for DNP3 communication.

- SENG
  For the SCS to be able to use the DNP3 slave function, engineering must be performed on the SENG. The SENG supports remote engineering in the Central Control Room, or engineering based on local connection to the SCS. The SENG and SCS are connected through the Vnet/IP-Upstream network.
- Controller from other companies
  It uses the DNP3 protocol to communicate with the DNP3 master.
- SNTP server
  In an environment where SNTP servers can be installed, use SNTP servers to synchronize the time of the DNP3 master and that of the SCS. Connect UTC-synchronized SNTP servers to the Ethernet network to which the DNP3 master is connected, and also to the Vnet/IP-Upstream network to which the SCS is connected, to synchronize the time of the DNP3 master and that of the SCS.

Duplexed communication interface

In a duplexed configuration of DNP3 communication interface, two ALE111 modules are mounted to the SCS and the path between the DNP3 master and ALE111 is duplexed.

If there is an error on one of the paths between the DNP3 master and ALE111, the SCS can still use the other ALE111 to communicate with the DNP3 master. In the DNP3 master, set which of the two ALE111 modules for the DNP3 communication to use normally. This configuration cannot be set in the SCS.

The duplexed interface for DNP3 communication can only be used on SCSU1 of R4.02 or later. A database that is created by using SENG of R4.02 or later is also required.

IMPORTANT

You can mount two ALE111 modules for a duplexed communication interface, but only one DNP3 master can be connected to SCS as before. The two ALE111 modules cannot be connected to different DNP3 masters.

Behavior of SCS with a duplexed communication interface

With a duplexed communication interface, SCS behaves as follows:

- The SCS communicates with the DNP3 master through two ALE111 modules.
- The SCS returns the response from the ALE111 that was requested by the DNP3 master. Even if an error is found in the path between the ALE111 and the DNP3 master before SCS can return the response, the SCS still attempts to return the response from the ALE111 that was requested. In such a case, even if the path between the other ALE111 and the DNP3 master is functioning properly, the SCS will not return the response from the ALE111 from which it did not receive the request. In the event of an error in the communication path, switch the path from the DNP3 master. SENG cannot be used to confirm which ALE111 is being used to communicate with the DNP3 master.

G2. DNP3 slave function of SCS

The DNP3 slave function of the SCS comprises the following:

- Referencing and setting data
- Event buffering
- Time synchronization

The DNP3 slave function accesses data during idle time when no safety function is active, so it does not affect any of the safety functions.

G2.1 Data access using the DNP3 slave function

To reference and set any variable of application logic of the SCS from the DNP3 master through DNP3 communication, assign an instance of DNP3 communication FB that is connected to the variable of the application logic, to DNP3 data.

DNP3 data is the virtual data of SCS that consists of the data type and Index.

The following six data types are available:

- Binary Input
- Binary Output
- Binary Counter
- Frozen Counter
- Analog Input
- Analog Output

For the Index, a sequential value of 0 to 499 is appended for each data type.

Once an instance of DNP3 communication FB is assigned to the Index for each data type, the DNP3 master can access the variable of the application logic as DNP3 data. An instance of DNP3 communication FB can be assigned to any Index. Note, however, that the total number of assignable instances of DNP3 communication FBs is limited to 1000 for all data types combined. For the Frozen Counter, it is not necessary to assign an instance to the Index, because there is one Frozen Counter corresponding to one Binary Counter.

The following figure shows the correspondence of DNP3 data and DNP3 communication FBs.

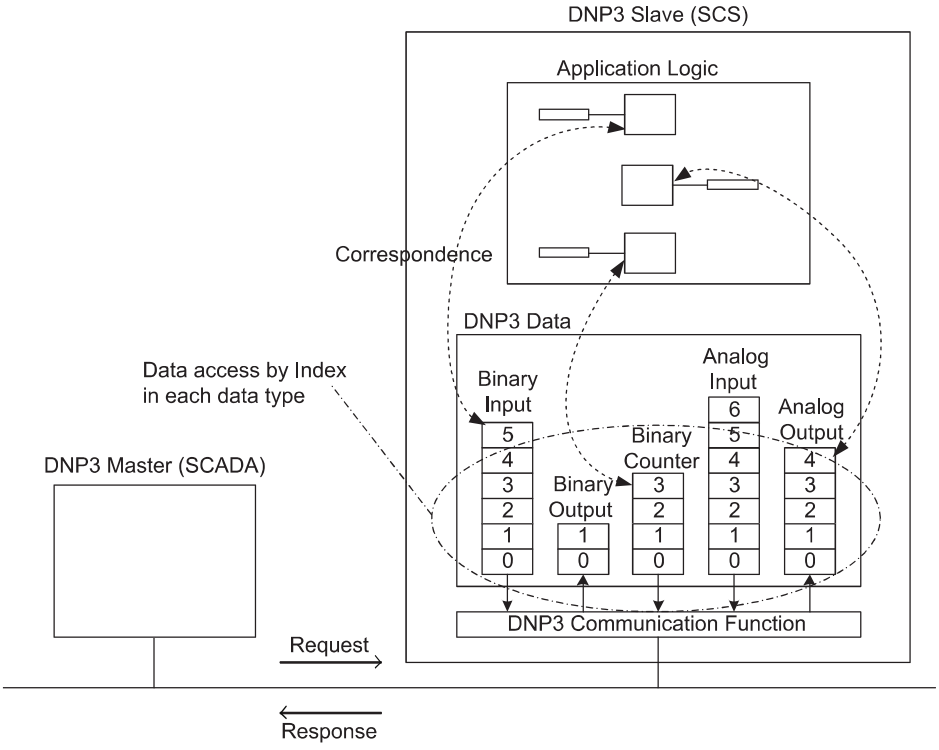


Figure G2.1-1 Correspondence of DNP3 data and DNP3 communication FBs

The DNP3 communication function executes processes relating to the DNP3 slave, such as referencing, setting and freezing DNP3 data, and responding to and deleting events.

Data referencing and data setting from the DNP3 master

Use DNP3 communication FBs to reference data from or set data to the SCS from the DNP3 master. The following table shows the relationship between the DNP3 communication FBs and DNP3 data that can be referenced and set from the DNP3 master.

Table G2.1-1 Relationship between the DNP3 communication FBs and DNP3 data that can be referenced and set from the DNP3 master

DNP3 communication FB	DNP3 data	Referencing/setting from DNP3 master
DNP3_BI	Binary Input	Referencing
DNP3_BO	Binary Output	Referencing and setting
DNP3_CT_16, DNP3_CT_32	Binary Counter, Frozen Counter	Referencing (*1)
DNP3_AI_16, DNP3_AI_32, DNP3_AI_SF	Analog Input	Referencing
DNP3_AO_16, DNP3_AO_32, DNP3_AO_SF	Analog Output	Referencing and setting

*1: Binary Counter can only be referenced, whereas the Frozen Counter can be referenced and cleared.

SEE ALSO For more information about engineering method of DNP3 data, refer to:

G3.5, “Definition of DNP3 data” on page G3-12

G2.1.1 Referencing DNP3 data

The following describes how to reference the DNP3 data of the SCS from the DNP3 master.

- Index specification
  The DNP3 master obtains the DNP3 data of the specified Index or Index range from SCS. If no instance of DNP3 communication FB is assigned to the specified Index, or an out-of-range Index (other than 0 to 499) is specified, the SCS returns the following error:

  `IIN2.2 PARAMETER_ERROR`

  Moreover, when there is a reference request for Analog Input, Analog Output and Binary Counter, if a data type different from the data types (16-bit, 32-bit, float) is specified in the SCS, the SCS returns the following error:

  `IIN2.2 PARAMETER_ERROR`

- Batch specification (Class 0 specification)
  The DNP3 master obtains from the SCS all DNP3 data to whose Index an instance of DNP3 communication FB is assigned.

  You can specify whether to include the Frozen Counter in the response for batch specifications.

SEE ALSO

For more information about setting of whether to include or not include the Frozen Counter in the response in the case of batch specification, refer to:

G3.3, “DNP3 slave setting” on page G3-8

For more information about precautions when assigning DNP3 data, refer to:

“■ Precautions when assigning DNP3 data” on page G3-22

■ Referencing DNP3 data

The DNP3 communication function of SCS is responsible for referencing of DNP3 data. The DNP3 communication function is processed during the idle time after the processing of application logic is completed. Accordingly, DNP3 data is referenced with a delay up to the scan period of application logic. When a variable of the application logic is updated, it takes time up to the scan period of the external connection function before the value can be referenced.

The following figure shows the execution timing of the DNP3 communication function.

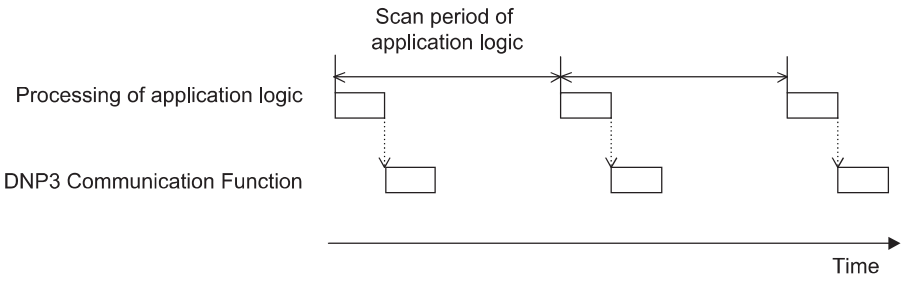


Figure G2.1.1-1 Execution timing of DNP3 communication function

G2.1.2 Setting DNP3 data

The following describes how to set DNP3 data to the SCS from the DNP3 master.

- Direct Operate - With Acknowledgment
  DNP3 data is set to the SCS according to the Operate command from the DNP3 master. The SCS returns the setting result (Success/Error) to the DNP3 master as an Acknowledgment.
- Direct Operate - No Acknowledgment
  DNP3 data is set to the SCS according to the Operate command from the DNP3 master. The SCS does not return the setting result (Success/Error) to the DNP3 master. Use the DNP3 master to acknowledge the setting result based on a change event or readback.
- Select Before Operate
  DNP3 data is set by using the Operate command after the Select command with Operate Parameter is sent to the SCS from the DNP3 master. The SCS accepts only the Operate command for the request reserved by the Select command. If no Operate command is received within a specified period, or the received Operate command is not for the reserved request, the SCS cancels the Select command and no longer executes the Operate process for any subsequently received Operate command.

  Only one Select command can be accepted. If multiple Select commands are received, the last Select command is accepted.

IMPORTANT

- When setting data from the DNP3 master, use the Direct Operate - With Acknowledgment command unless there is a specific reason.
- If the specified Index has no instance of DNP3 communication FB assigned to it, or an out-of-range Index (other than 0 to 499) is specified, the SCS returns the following error:

  `IIN2.2 PARAMETER_ERROR`

The following figure shows the sequence for each DNP3 data setting method.

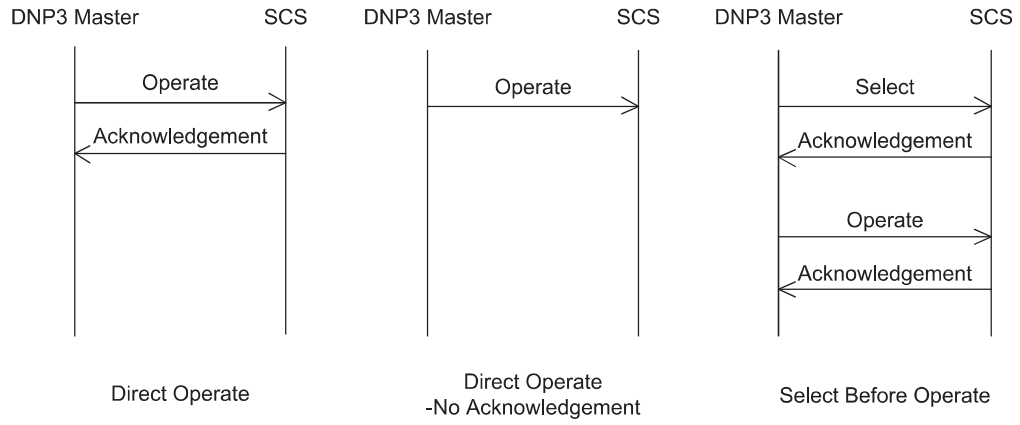


Figure G2.1.2-1 Sequence for each DNP3 data setting method

SEE ALSO For more information about precautions when setting data from the DNP3 master, refer to:

"■ Data setting from the DNP3 master" on page G3-19

Setting DNP3 data

DNP3 data is set by the DNP3 communication function.

The following figure shows how a DNP3 data setting request is processed.

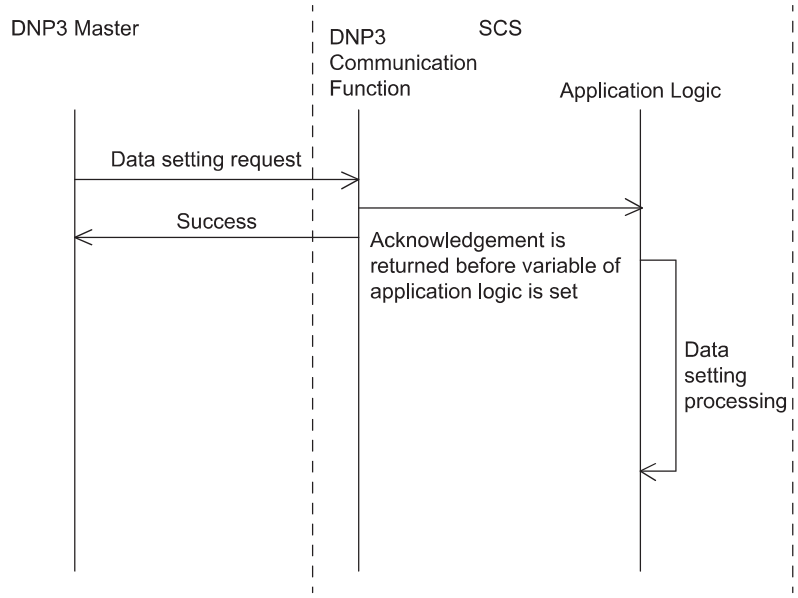


Figure G2.1.2-2 How a DNP3 data setting request is processed

When SCS accepts a data setting request from the DNP3 master, the DNP3 communication function of SCS issues a data setting request to the application logic of the SCS. The DNP3 communication function of SCS returns an acknowledgment to the DNP3 master before the application logic of SCS sets the data.

The time that is taken for the variable of the application logic to be updated after the DNP3 communication function receives the setting request, depends on the number of data setting requests from the Modbus and other external connection functions.

SEE ALSO For more information about execution timing of DNP3 communication function, refer to:

"■ Referencing DNP3 data" on page G2-4

For more information about maximum time before the set value can be referenced, refer to:

"● Maximum time before the set value can be referenced" on page G3-21

Precautions when setting DNP3 data

This section describes the precautions when setting the DNP3 data.

● Limitations on data setting using DNP3 communication

When SCS receives a data setting request from the DNP3 master, it returns a response and retains the request it accepted.

- Up to four data setting requests that uses DNP3 communication can be retained. A Freeze & Clear request is also considered a data setting request.
- SCS processes the maximum of four retained data setting requests per second from the DNP3 master when the scan period of the application logic is 250 ms or less. If the scan period exceeds 250 ms, SCS processes one request in one scan period.

- If SCS also retains any data setting request from the Modbus master or other external connection devices, the SCS processes data setting requests from the external connection device and the DNP3 master in the order of acceptance.
- If SCS retains four unprocessed requests when it receives a data setting request from the DNP3 master, the SCS returns the following status code:

  PROCESSING_LIMITED

  The SCS just discards the data setting request if the request requires no acknowledgement.

SEE ALSO For more information about freeze & Clear request, refer to:

"■ Freeze & Clear command" on page G2-8

Binary Output limit

The SCS's Binary Output supports latch output type operation only. Pulse output operation cannot be used.

G2.1.3 Freeze command, Freeze & Clear command

The SCS supports the DNP3 Freeze command and Freeze & Clear command.

Freeze command

The Freeze command is used to save the current value of the Binary Counter. After accepting a Freeze request from the DNP3 master, the SCS copies the current values of all Binary Counters to the Frozen Counter. The Frozen Counter will store the values of all Binary Counters effective when the Freeze command was executed.

The following figure shows how the SCS operates upon accepting a Freeze command from the DNP3 master.

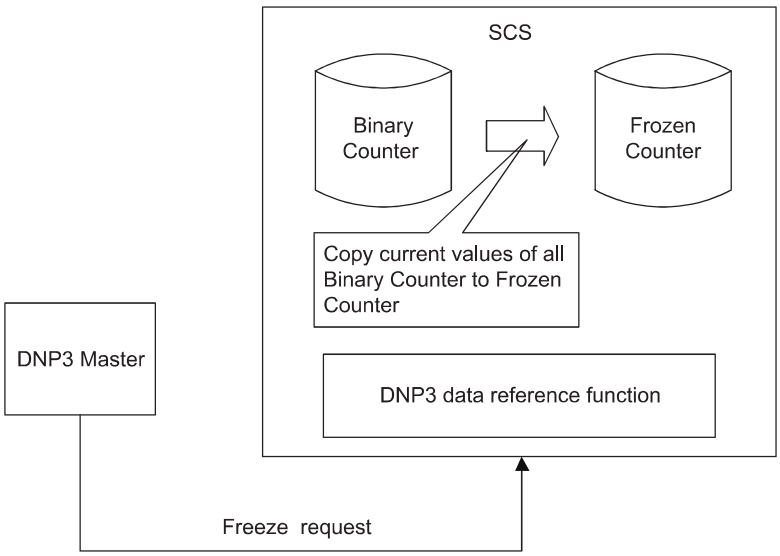


Figure G2.1.3-1 How the SCS operates upon accepting a Freeze command

Freeze & Clear command

If no more than 32 Binary Counters are defined, the Freeze & Clear command can be used.

The Freeze & Clear command is used to save the current value of the Binary Counter in the Frozen Counter and then clear the value of the Binary Counter to 0. After accepting a Freeze & Clear command from the DNP3 master, the SCS copies the current values of all Binary Counters to the Frozen Counter and then clears the values of all Binary Counters to 0.

The following figure shows how the SCS operates upon accepting a Freeze & Clear command from the DNP3 master.

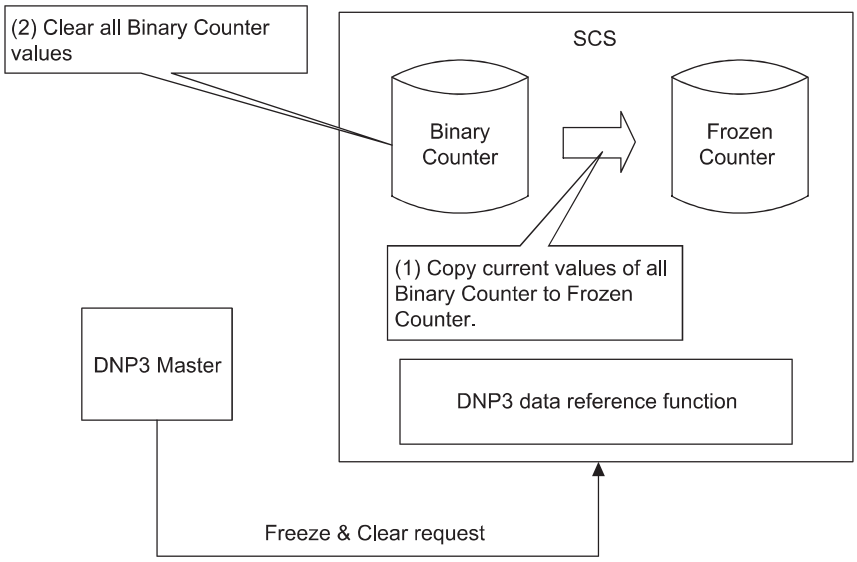


Figure G2.1.3-2 How the SCS operates upon accepting a Freeze & Clear command

The DNP3 master can calculate the rate of change in Binary Counter values by periodically executing a Freeze & Clear command.

IMPORTANT

- If SCS receives a Freeze & Clear request when 33 or more Binary Counters are defined, SCS returns the following error:

  `IIN2.0 NO_FUNC_CODE_SUPPORT`

- If SCS receives a Freeze & Clear request from the DNP3 master when it retains four un-processed requests, the SCS returns the following error:

  `IIN2.0 NO_FUNC_CODE_SUPPORT`

- If SCS returns an error in response to the Freeze & Clear request, no Freeze process is executed.

G2.1.4 Response time

The response time it takes for the SCS to response to the request for data referencing and data setting from the DNP3 master refers to the time from when SCS receives a request message to when it starts to transmit the response message. The Ethernet transmission time is not included.

```
Response time = (Message receiving processing time and message sending processing
 time) + (Data referencing processing time or data setting processing time)
```

The message receiving processing time and message sending processing time should be within 20 ms.

The data referencing processing time or data setting processing time may be as long as the scan period of the application logic.

G2.2 Event buffering

The SCS generates an event the moment a variable of the application logic assigned to DNP3 data changes. This event contains the applicable DNP3 data and a time stamp indicating when the DNP3 data changes. The SCS can retain events while a communication failure is present, by buffering the generated events. Once communication is restored, the DNP3 master reads the buffered events to prevent missing data.

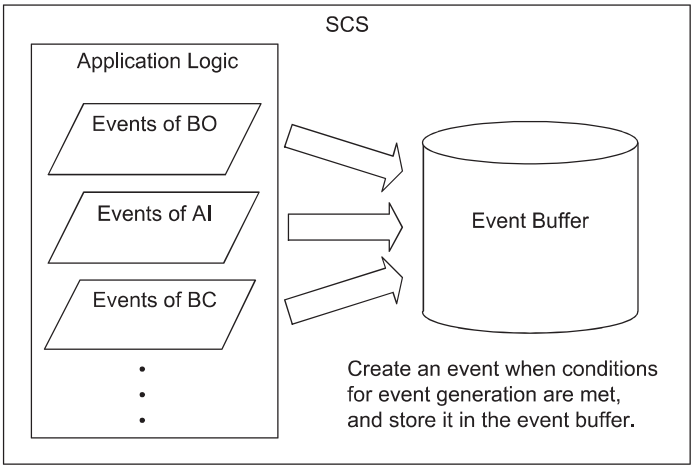


Figure G2.2-1 Event buffering operation

IMPORTANT

The DNP3 event buffering function cannot be used simultaneously with the data buffering function that is used when the system is integrated with CI Server.

G2.2.1 Event generation

To generate events in SCS, set an event class for each DNP3 data and event buffer size for each DNP3 data type.

Event class

For events, set an event class of 0, 1, 2, or 3 for each DNP3 data. Event classes are used to organize generated events into groups. The DNP3 master can specify an event class to obtain events that are set under the event class.

No event is generated for DNP3 data of event class 0. Set event class 0 for those data that do not require an event.

Set event classes using input parameters of DNP3 communication FBs. Event classes cannot be set by using DNP3 communication commands from the DNP3 master.

Event buffer size

Set the number of events that can be stored in the event buffer, for each DNP3 data type. An event buffer size can be set separately for each DNP3 data type. The total of all event buffer sizes must be less than or equal to 135000.

Set event buffer sizes by using the DNP3 Communication Builder of the SENG.

Event generation condition

The SCS generates an event when the following conditions are met:

- Event class 1, 2, or 3 is set for each DNP3 data.
- A value other than 0 is set for the event buffer size.
- The value of DNP3 data is changed.

Determine whether or not the value of DNP3 data is changed, as follows:

- In the case of Analog Input, the value changes when the absolute difference between the previous change event value and this value exceeds the set Deadband.
- In the case of DNP3 data other than Analog Input, the value changes when there is a difference between the previous value and this value.

The Deadband is a threshold that is used to generate an event. Set the Deadband by using an input parameter of a DNP3 communication FB.

IMPORTANT

- No event is generated for DNP3 data that has an event class that is set to 0.
- No event is generated for DNP3-type data that has an event buffer size that is set to 0.

Event time stamp

An event has a time stamp that indicates the time that the application logic scan started. All of the events that are generated during the same scan period have an identical time stamp. However, the events are stored in the event buffer in the order that they are generated.

G2.2.2 Event response

Upon receiving an event acquisition request from the DNP3 master, the SCS responds with the specified event, if available.

The following methods are used to acquire SCS event data from the DNP3 master:

- Data type specification: Acquire events of the specified data type.
- Class specification: Acquire events of the specified class.

IMPORTANT

The event response of the SCS supports the Pulled Report by Exception type only. The Unsolicited Response type is not supported.

G2.2.3 Event deletion

The SCS deletes an event after receiving a confirmation from the DNP3 master.

When the SCS receives an event acquisition request, the SCS sets an event responding flag. Upon receiving a confirmation of completed event acquisition from the DNP3 master, the SCS deletes the event for which the flag is set.

If the SCS receives no confirmation from the DNP3 master 10 seconds after the event response, the SCS clears the responding flag and retains the event.

The following figure shows the event deletion sequence.

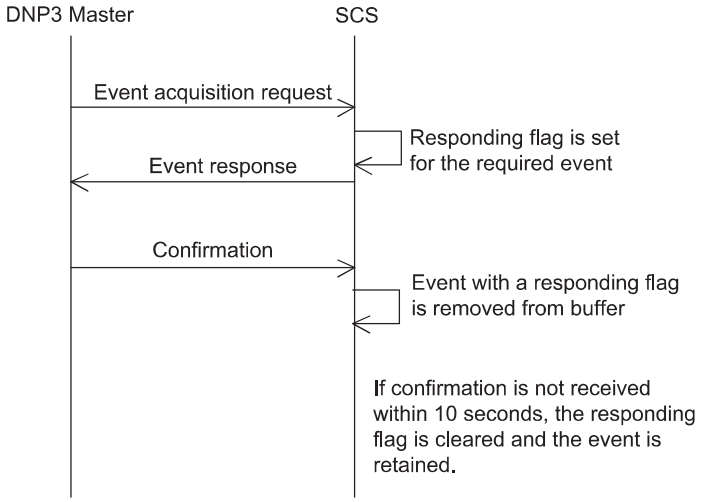


Figure G2.2.3-1 Event deletion sequence

G2.3 DNP3 function support for each data type

The following table shows DNP3 data type, Index range and DNP3 function supported by the SCS.

Table G2.3-1 SCS support Data type for DNP3 function

Data type	IEC data type	Index range	DNP3 function (*1)							
			Read Static	Read Event	Write	Select and Operate	Direct Operate	Freeze	Assign Class	Set Analog Deadband
Binary Input	BOOL	0 to 499 (*2)	Yes	Yes	-	-	-	-	Yes (*3)	-
Binary Output	BOOL	0 to 499 (*2)	Yes	Yes	-	Yes (*4)	Yes (*4)	-	Yes (*3)	-
16-Bit Binary Counter	DINT (*5)	0 to 499 (*2)	Yes	Yes	-	-	-	Yes	Yes (*3)	-
32-Bit Binary Counter	DINT (*5)		Yes	Yes	-	-	-	Yes	Yes (*3)	-
16-Bit Frozen Counter	DINT (*5)		Yes	Yes	-	-	-	-	Yes (*3)	-
32-Bit Frozen Counter	DINT (*5)		Yes	Yes	-	-	-	-	Yes (*3)	-
16-Bit Analog Input	DINT (*5)	0 to 499 (*2)	Yes	Yes	-	-	-	No	Yes (*3)	Yes (*3)
32-Bit Analog Input	DINT		Yes	Yes	-	-	-	No	Yes (*3)	Yes (*3)
Single-Precision Floating Point Analog Input	REAL		Yes	Yes	-	-	-	No	Yes (*3)	Yes (*3)
16-Bit Analog Output	DINT (*5)	0 to 499 (*2)	Yes	Yes	-	Yes	Yes	-	Yes (*3)	No
32-Bit Analog Output	DINT		Yes	Yes	-	Yes	Yes	-	Yes (*3)	No
Single-Precision Floating Point Analog Output	REAL		Yes	Yes	-	Yes	Yes	-	Yes (*3)	No

*1: Yes: Supported, No: Not supported, -: Function not available under DNP3
*2: The total number of data is 1000 for all data types combined.
*3: Set by a DNP3 communication FB. Command setting from the DNP3 master is not supported.
*4: Only latch type output operation is supported. Pulse type output operation is not supported.
*5: The UNIT, UDINT and INT data types under DNP3 are handled as DINT on the SCS.

SEE ALSO For more information about definition of DNP3 data, refer to:

G3.5, “Definition of DNP3 data” on page G3-12

For more information about DNP3 communication FB, refer to:

15., “Function blocks for DNP3 communication (Interference-free FB)” in POU Reference Manual (IM 32P03B20-01EN)

G2.4 Time synchronization

Methods to synchronize the time of the DNP3 master and that of the SCS include time synchronization by using SNTP servers and time synchronization by using DNP3 communication. However, the accuracy of time synchronization using DNP3 communication is no more than 1 second plus the scan period of the application logic.

In an environment where SNTP servers can be connected to the Ethernet network to which the DNP3 master is connected, and also to the Vnet/IP-Upstream network to which the SCS is connected, use time synchronization using SNTP servers for greater time synchronization accuracy.

IMPORTANT

The DNP3 communication contains IIN (internal indications) information, which indicates the status of the DNP3 slave. The IIN is added to the DNP3 response frame and transmitted from the DNP3 slave to the DNP3 master. The IIN includes the time synchronization request status (IIN 1.4 NEED_TIME), which is used to determine the timing for the DNP3 master to synchronize its time.

The SCS sets a flag for the time synchronization request status when it is launched. Once the SCS has received the time synchronization request from the DNP3 master, it will clear the flag and set it again 30 minutes later.

When performing time synchronization by using SNTP servers, the SCS will clear the flag for the time synchronization request status once it has established connection with an SNTP server and will not set the flag again. As such, even if the SCS is disconnected from the SNTP server, time synchronization is not performed by using DNP3 communication.

Time synchronization using SNTP servers

Connect time-synchronized SNTP servers to the Ethernet and Vnet/IP-Upstream, respectively. Synchronize the DNP3 master with the time of the SNTP server on the Ethernet, and synchronize the SCS with the time of the SNTP server on the Vnet-/IP-Upstream. As a result, the time of the DNP3 master will synchronize with the time of the SCS.

The following figure shows the time synchronization by using SNTP servers.

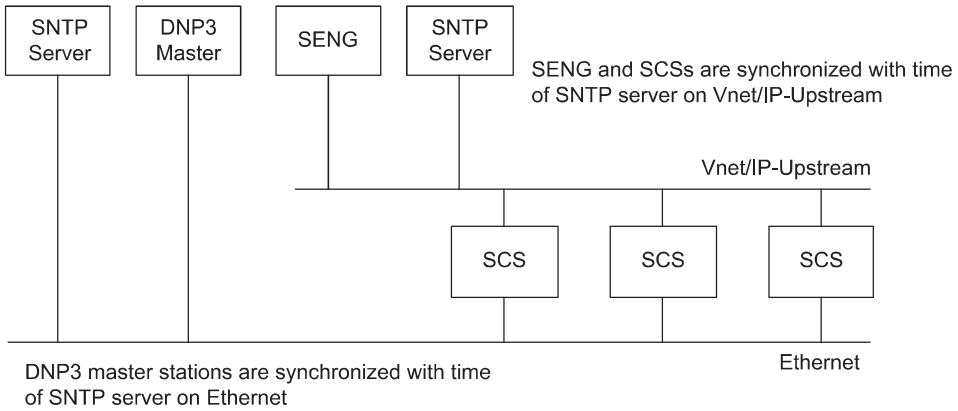


Figure G2.4-1 Time synchronization using SNTP servers

IMPORTANT

Once the SCS has established connection with an SNTP server, it will return the following error when it receives a time synchronization request from the DNP3 master.

```
IIN2.0 NO_FUNC_CODE_SUPPORT
```

Time synchronization using DNP3 communication (The SCS is not connected to the Vnet/IP-Upstream network)

If the SCS is not connected to the Vnet/IP-Upstream network, set the times of all SCSs from the DNP3 master by using DNP3 communication.

The following figure shows time synchronization by using DNP3 communication when the SCS is not connected to the Vnet/IP-Upstream network.

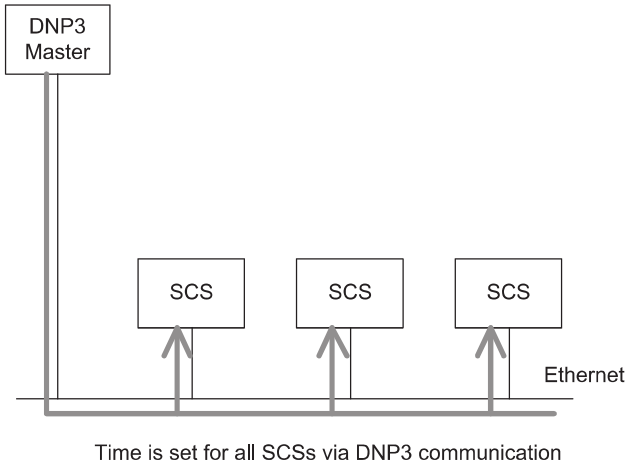


Figure G2.4-2 Time synchronization by using DNP3 communication when the SCS is not connected to the Vnet/IP-Upstream network

Time synchronization using DNP3 communication (The SCS is connected to the Vnet/IP-Upstream network)

If the SCS is connected to the Vnet/IP-Upstream network, set the time of one SCS from the DNP3 master by using DNP3 communication.

The times of other SCSs connected to the Vnet/IP-Upstream network will be synchronized by the time synchronization function of the Vnet/IP-Upstream.

The following figure shows time synchronization by using DNP3 communication when the SCS is connected to the Vnet/IP-Upstream network.

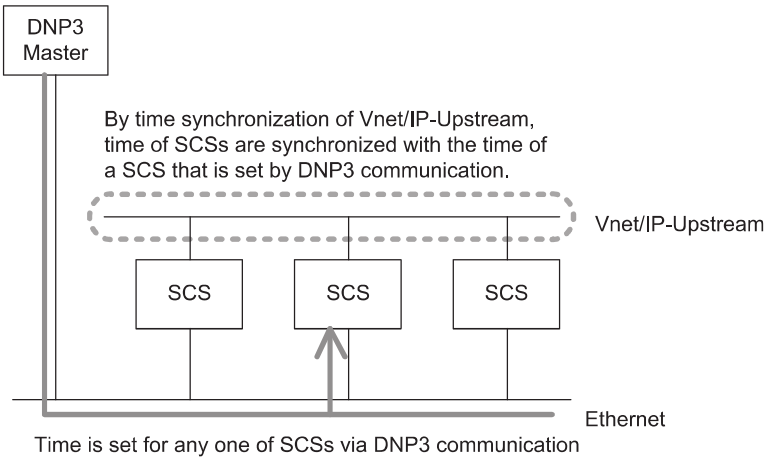


Figure G2.4-3 Time synchronization by using DNP3 communication when the SCS is connected to the Vnet/IP-Upstream network

TIP

- Even when the Vnet/IP-Upstream network consists of multiple domains, setting the time of any one SCS synchronizes the times of all SCSs.
- If some SCSs are connected to the Vnet/IP-Upstream network and others are not, set the time of one SCS that is connected to the Vnet/IP-Upstream network and the times of all SCSs that are not connected to the Vnet/IP-Upstream network.

SEE ALSO

For more information about precautions when setting the time through DNP3 communication, refer to:

"■ Precautions when setting the time through DNP3 communication" on page G3-21

G3. Engineering and maintenance with SENG

The following settings are required for the DNP3 master to access application logic variables of the SCS by using the DNP3 communication function.

- Enabled DNP3 slave function
- Definition of communication modules
- DNP3 slave setting
- Definition of instances for DNP3 communication FBs
- Definition of DNP3 data
- Creating an application logic

Engineering flow

Use the following flow to set the DNP3 slave function engineering on the SENG.

The communication module can be defined in the following engineering methods: I/O list engineering and RS original engineering.

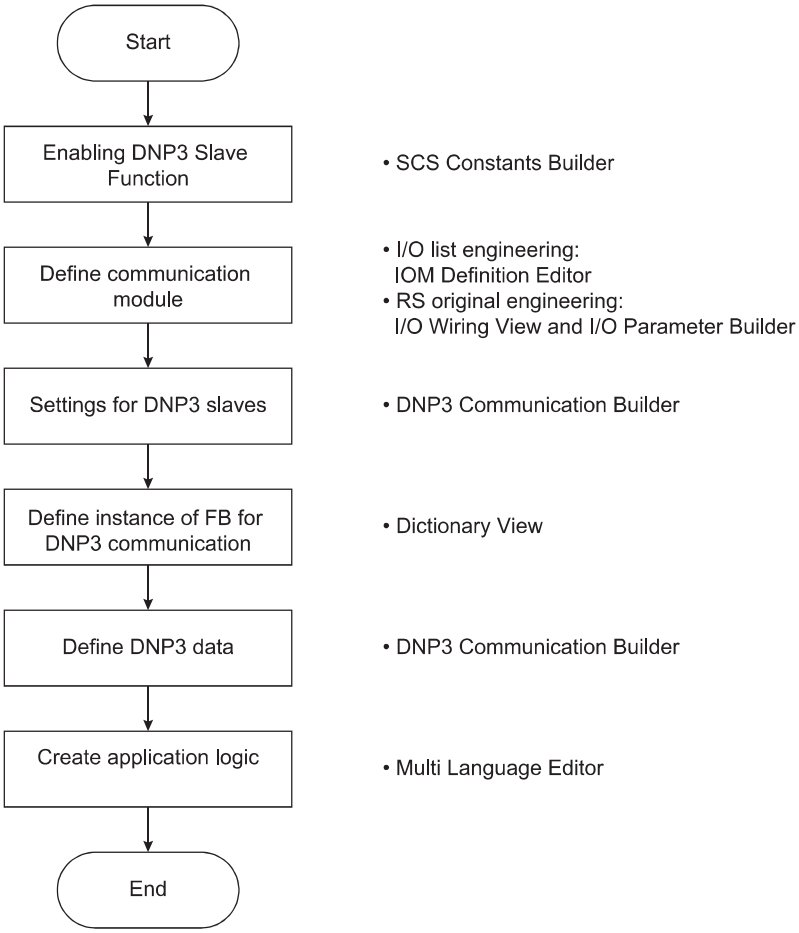


Figure G3-1 Engineering flow of DNP3 slave function

G3.1 Enabled DNP3 slave function

Use the SCS Constants Builder to enable the DNP3 slave function so that the SCS can perform DNP3 communication. Enable the DNP3 slave function on the Communication tab of the SCS Constants Builder.

IMPORTANT

- The DNP3 slave function cannot be enabled online. Changing this setting requires offline download to the SCS.
- Once the DNP3 slave function is enabled, the data buffering function in Integration with CI Server can no longer be used. The event buffer function of the DNP3 slave function can be used.

SEE ALSO For more information about SCS Constants Builder, refer to:

C1.2.6, “SCS Constants Builder” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

G3.2 Definition of communication modules

You must define an Ethernet communication module so that the SCS can perform DNP3 communication.

The editor to be used differs depending on engineering methods.

When performing I/O list engineering, you can define the Ethernet communication module and set parameters by using IOM Definition Editor.

When performing RS original engineering, you can use the I/O Wiring View in the SCS Manager and define the Ethernet communication module. Then, you can set the parameters in the Ethernet communication module by using the I/O Parameter Builder.

This section mainly describes for the case when performing RS original engineering. The communication module definition items and the parameter setting items that are required in I/O list engineering are the same as those for RS original engineering.

SEE ALSO

For more information about I/O list engineering, refer to:

D., “Procedures to create applications using the I/O list engineering method” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about RS original engineering, refer to:

Appendix 2., “RS original engineering” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about I/O Wiring View and I/O Parameter Builder, refer to:

Appendix 2.2, “Definitions of inputs/outputs” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about parameter settings for communication modules, refer to:

Appendix 1.2, “Settings for modules” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

G3.2.1 Definitions in I/O Wiring View

When performing RS original engineering, you can use the I/O Wiring View in the SCS Manager, and define the Ethernet communication module (model: ALE111) as follows:

1. Open I/O Wiring View and select ALE111.
2. Select parameters for the module and specify the node number and the slot number. The node number and the slot number must not overlap with those of other I/O modules and communication modules.

IMPORTANT

When implementing a duplexed communication interface, you must define two ALE111 modules in a non-redundant configuration. There is no restriction on the installation location.

SEE ALSO For more information about display method and window configuration for the I/O Wiring View, refer to:

Appendix 2.2.1, “I/O Wiring View” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

G3.2.2 Definitions in I/O Parameter Builder

When performing RS original engineering, you can specify parameters for the communication module by using I/O Parameter Builder.

For an Ethernet communication module, you can specify the parameters in the Module tab of I/O Parameter Builder.

SEE ALSO For more information about display method and window configuration for the I/O Parameter Builder, refer to:

Appendix 2.2.2, "I/O Parameter Builder" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Module tab of Ethernet communication module

The following tables show the display-only items and settable items on the Module tab of the Ethernet communication module.

The setting of each item can be changed by online change download, but the target module restarts after online change download.

Table G3.2.2-1 Display-only items on the Module tab of the Ethernet communication module

Title	Description	Remarks
Node Number	The node number of the node in which the module is mounted	Defined in I/O Wiring View
Slot Number	The slot number of the slot in which the module is mounted	Defined in I/O Wiring View
Device	The model name of the module	Defined in I/O Wiring View
Dual-Redundant	Whether the module is used in a single or dual-redundant configuration	The module cannot be dual-redundant
Device Number	The device number that is assigned to the module	Defined in I/O Wiring View

Table G3.2.2-2 Setting items on the Module tab of the Ethernet communication module

Title	Description	Remarks
Connection Device	Types of connection devices	-
Comment	A comment regarding the module	-
IP Address	The IP address of the module	-
Subnet Mask	The subnet mask of the module	-
Default Gateway	The default gateway address of the module	-
Port Number	The TCP/IP port number	-
Option 1 to 4	Option items	Fixed to 0.

IMPORTANT

When implementing a duplexed communication interface, you must configure the settings for each of the Ethernet communication modules to be duplexed. However, set the different IP address for the Ethernet communication module for each of modules.

Connection Device

Set the type of connection device.

Select SCSDPTCP when the DNP3 slave function should be used.

Default value: SCSMDTCP

SCSMDTCP: Modbus TCP master

SCSDPTCP: DNP3 master (Selectable only when the version of SCSU1 is R3.02.20 or later.)

TIP

If an attempt is made to change the connection device and the selected port number is not the default, the following dialog box appears:

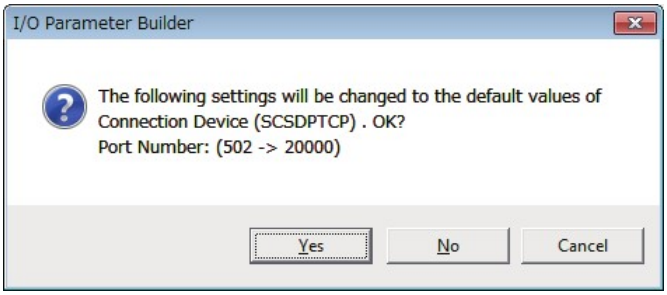


Figure G3.2.2-1 Connection Device dialog box

Yes: The connection device is changed and the port number is changed to the default.

No: The connection device is changed but the port number is not changed.

Cancel: Neither the connection device nor port number is changed.

Comment

A comment regarding the Ethernet communication module can be entered. This comment can be entered using up to 24 single-byte characters or 12 double-byte characters.

IP Address

Set the IP address of the Ethernet communication module. Enter any IP address that you want. When implementing a duplexed communication interface, you must set different IP addresses for the two modules.

Default: This field is empty by default; be sure to enter an IP address. If no value is entered, an error occurs when you try to save the settings in the builder.

Format: nnn.nnn.nnn.nnn

Setting range: 0.0.0.1 to 255.255.255.254
However, do not set the following IP addresses:

- Host address digits are all zeros or all ones in binary form. (Example: When subnet mask is 255.255.255.0, 192.168.1.0, 192.168.1.255, etc.)
- Any of the numbers delimited with a period has leading zeros. (Example: 192.168.08.09, 192.168.008.009, etc.)

Subnet Mask

Set the subnet mask of the Ethernet communication module. Enter a subnet mask that you want.

Default: This field is empty by default; be sure to enter a subnet mask. If no value is entered, an error occurs when you try to save the settings in the builder.

Format: nnn.nnn.nnn.nnn

Setting range: 0.0.0.1 to 255.255.255.254
However, do not set the following subnet masks:

- Values less than 255.0.0.0 for a class A IP address
  (Example: 128.0.0.0)
- Values less than 255.255.0.0 for a class B IP address
  (Example: 255.128.0.0)
- Values less than 255.255.255.0 for a class C IP address
  (Example: 255.255.128.0)

Default Gateway

Set the gateway address of the Ethernet communication module. Enter a desired gateway address.

Default: Blank

Format: nnn.nnn.nnn.nnn

Setting range: 0.0.0.1 to 255.255.255.254
However, do not set the following gateway addresses:

- Host address digits are all zeros or all ones in binary form.
  (Example: When subnet mask is 255.255.255.0, 192.168.1.0, 192.168.1.255, etc.)
- Network address digits do not match the IP address.
  (IP address is 192.168.1.1 and default gateway address is 192.168.2.2 when the subnet mask is 255.255.255.0.)
- Any of the numbers delimited with a period has leading zeros.
  (Example: 192.168.08.09, 192.168.008.009, etc.)

Port Number

Set the port number for DNP3 communication.

Default: 20000

Setting range: 0 to 65535

Option 1 to 4

Always set 0 for these options.

Default: 0 (for all)

G3.3 DNP3 slave setting

Use the DNP3 Communication Builder of SENG to set the following parameters so as to make the SCS operate as the DNP3 slave:

Set it as the DNP3 slave on the Parameters tab of the DNP3 Communication Builder.

- DNP3 slave station address
- DNP3 master station address
- Timeout value for Select Before Operate
- Binary Input event buffer size
- Binary Output event buffer size
- Binary Counter event buffer size
- Frozen Counter event buffer size
- Analog Input event buffer size
- Event to be removed when event buffer overflows
- Generate an event when Freeze and Clear command changes the data values
- Include Frozen Counters in Class 0 response
- Type of response message fragmentation

IMPORTANT

- All DNP3 slave settings, except for the event buffer size, can be changed online without stopping the SCS.
- If the DNP3 slave station address or DNP3 master station address is changed, the TCP/IP connection is cut off.
- If the station address is changed, reconnect from the DNP3 master.
- Changing any DNP3 slave setting does not affect the events that are already buffered.
- Changing the event buffer size requires offline download to the SCS.

SEE ALSO For more information about display method and window configuration for the DNP3 Communication Builder, refer to:

G3.5, “Definition of DNP3 data” on page G3-12

DNP3 slave station address

Set the station address of the SCS.

Setting range: 0 to 65519

Default: 0

DNP3 master station address

Set the station address of the DNP3 master.

Setting range: 0 to 65519

Default: 1

Timeout value for Select Before Operate

Set the timeout value in seconds for the Select Before Operate function.

Setting range: 1 to 600
Default: 5

Binary Input event buffer size

Set the number of events that can be stored in the Binary Input event buffer.

Setting range: 0 to 135000
Default: 500

Binary Output event buffer size

Set the number of events that can be stored in the Binary Output event buffer.

Setting range: 0 to 135000
Default: 0

Binary Counter event buffer size

Set the number of events that can be stored in the Binary Counter event buffer.

Setting range: 0 to 135000
Default: 500

Frozen Counter event buffer size

Set the number of events that can be stored in the Frozen Counter event buffer.

Setting range: 0 to 135000
Default: 0

Analog Input event buffer size

Set the number of events that can be stored in the Analog Input event buffer.

Setting range: 0 to 135000
Default: 500

Analog Output event buffer size

Set the number of events that can be stored in the Analog Output event buffer.

Setting range: 0 to 135000
Default: 0

Event to be removed when event buffer overflows

Set how events will be stored when the event buffer overflows.

Oldest: The oldest event stored in the event buffer is deleted and a new event is stored.

Newest: The newest event stored in the event buffer is deleted and a new event is stored.

Default: Oldest

Generate an event when Freeze and Clear command changes data values

Set whether or not to send an event notification when values are cleared to 0 by the Freeze & Clear command.

No: Do not send an event notification.

Yes: Send an event notification.

Default: No

Include Frozen Counters in Class 0 response

Set whether or not to include the Frozen Counter in the Class 0 response.

Yes: Including Frozen Counter

No: Not including Frozen Counter

Default: Yes

Type of response message fragmentation

Set how a response is sent to one acquisition request when the size of the response DNP3 frame exceeds the maximum frame size that SCS can handle.

Single: Single fragment
The DNP3 frame is divided into frames with the maximum frame size and only one frame is sent for one acquisition request.

Multi: Multi fragments
The DNP3 frame is divided into frames with the maximum frame size and multiple frames are sent consecutively for one acquisition request.

Default: Single

To acquire events from the SCS that receives data setting requests, change the event response method of the SCS to "Single fragment."

SEE ALSO For more information about precautions on event acquisition methods, refer to:

"■ Method of response upon event acquisition" on page G3-21

G3.4 Definition of instances for DNP3 communication FBs

Use the Dictionary View to define an instance of DNP3 communication FB.

SEE ALSO For more information about how to define variables using the Dictionary View, refer to:

"Dictionary View" in "Workbench" in the Workbench User's Guide

G3.5 Definition of DNP3 data

To access any variable of the application logic of the SCS from the DNP3 master through DNP3 communication, associate an instance of DNP3 communication FB, to DNP3 data. Use the DNP3 Communication Builder to define an instance of DNP3 communication FB to DNP3 data.

Launching DNP3 Communication Builder

1. Select [Engineering] from the [Tools] menu of SCS Manager.
   The Engineering Launcher menu appears.
2. Select [DNP3 Communication Builder].
   The DNP3 Communication Builder appears.

G3.5.1 Window configuration of the DNP3 Communication Builder

The window of the DNP3 Communication Builder is primarily composed of the data menu area and work space.

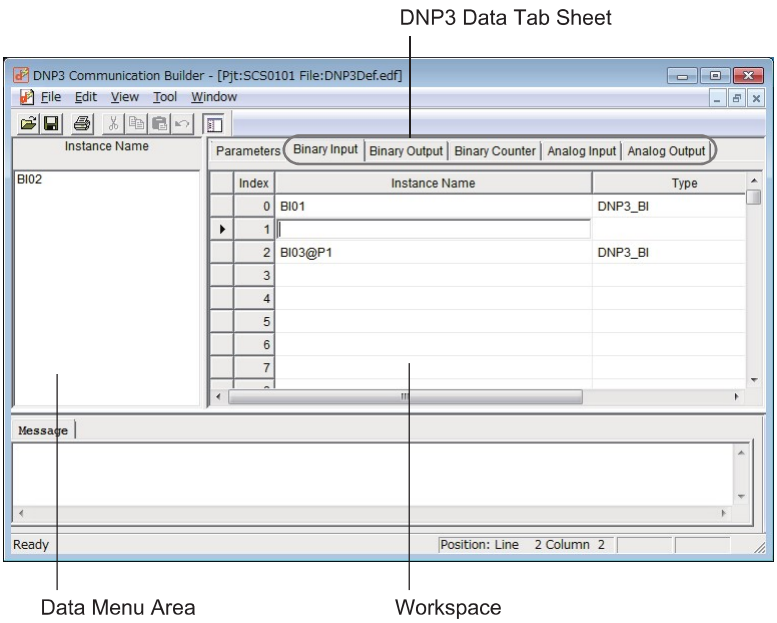


Figure G3.5.1-1 Window configuration of the DNP3 Communication Builder

The data menu area of the DNP3 Communication Builder is composed of the Instance tab.

The work space of the DNP3 Communication Builder is composed of the Parameters tab and DNP3 data tab.

Instance tab of the Data menu area

A list of available instances is displayed on the Instance tab. The displayed names of instances vary depending on the type of DNP3 data displayed in the work space.

The following figure shows an example of the Instance tab for Binary Input.

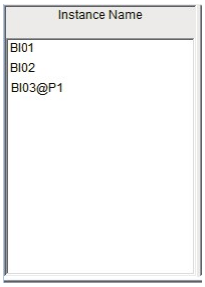


Figure G3.5.1-2 Example of Instance tab in Binary Input

Instances that are already set or deleted are removed from this list and not displayed.

Parameters tab of the work space

The Parameters tab is used to define the parameters of the DNP3 slave function.

SEE ALSO For more information about parameter defined by the DNP3 slave function, refer to:

G3.3, “DNP3 slave setting” on page G3-8

DNP3 data tabs in the work space

The DNP3 data tabs include the following tabs that are used to define a DNP3 communication FB for each DNP3 data type:

- Binary Input
- Binary Output
- Binary Counter
- Analog Input
- Analog Output

Items displayed in tabs

The following items are displayed on each DNP3 data tab:

- Index
  This is the index number of the DNP3 data. The index is displayed in advance in numerical order. 0 to 499.
- Instance name
  This is the instance name of the FB that is assigned to the DNP3 data. You can change the instance name online.
- Type
  This is the type of the FB that is assigned to the DNP3 data.
- Comment
  This is the comment string that represents the instance name of the FB that is assigned to the DNP3 data.

G3.5.2 Definition in the DNP3 Communication Builder

Use the DNP3 Communication Builder to assign an instance of DNP3 communication FB to a DNP3 Index.

Assigning an instance name in the DNP3 Communication Builder

The DNP3 data types that you can set in the DNP3 Communication Builder include Binary Input, Binary Output, Binary Counter, Analog Input and Analog Output, and an Index is assigned to DNP3 data of each DNP3 data type. The DNP3 Communication Builder assigns an instance name for the DNP3 communication FB to be accessed, to one of Indexes 0 to 499. An instance name for the DNP3 communication FB to be assigned is selected according to the Index.

If the DNP3 data type is Binary Input, for example, an instance name for DNP3 communication FB of DNP3_BI type can be assigned. If the DNP3 data type is Binary Counter, an instance name for DNP3 communication FB of DNP3_CT_16 type or DNP3_CT_32 type can be assigned.

DNP3 data types and assignable FBs

The following table describes the DNP3 data types and the types of FBs that can be assigned to these data types in the DNP3 Communication Builder.

Table G3.5.2-1 DNP3 data types and types of FBs that can be assigned in the DNP3 Communication Builder

DNP3 data type	Type of DNP3 communication FB	Description of FB
Binary Input	DNP3_BI	FB that corresponds to the DNP3 data of the DNP3 data type Binary Input
Binary Output	DNP3_BO	FB that corresponds to the DNP3 data of the DNP3 data type Binary Output
Binary Counter	DNP3_CT_16	FB that corresponds to the DNP3 data of the DNP3 data type 16-bit Binary Counter
	DNP3_CT_32	FB that corresponds to the DNP3 data of the DNP3 data type 32-bit Binary Counter
Analog Input	DNP3_AI_16	FB that corresponds to the DNP3 data of the DNP3 data type 16-bit Analog Input
	DNP3_AI_32	FB that corresponds to the DNP3 data of the DNP3 data type 32-bit Analog Input
	DNP3_AI_SF	FB that corresponds to the DNP3 data of the DNP3 data type Single-Precision Floating Point Analog Input
Analog Output	DNP3_AO_16	FB that corresponds to the DNP3 data of the DNP3 data type 16-bit Analog Output
	DNP3_AO_32	FB that corresponds to the DNP3 data of the DNP3 data type 32-bit Analog Output
	DNP3_AO_SF	FB that corresponds to the DNP3 data of the DNP3 data type Single-Precision Floating Point Analog Output

Instance name

Set an instance name of DNP3 communication FB to be assigned to the DNP3 data.

An instance name of DNP3 communication FB consists of up to 69 single-byte characters. In terms of accessibility to instance names, both global instances and local instances can be set regardless of the scope. In the case of a local instance, the scope name must be added after "@."

To access an instance of internal parameter in a user-defined function block, you can use the SCS Manager Dictionary View to name instances of the user-defined function block itself. Specify an instance name of DNP3 communication FB in the following format. Up to two nesting levels can be specified for an instance name.

```
instance name.internal parameter name
```

Table G3.5.2-2 Examples of instance name

Instance name	Scope	Description
VAR1	Global	Global instance
VAR2@PROG1	PROG1	Local instance of PROG1 function
FB01.VAR3	Global	The internal parameter VAR3 of an instance of the user-defined function block FB01
FB01.VAR3@PROG1	PROG1	The internal parameter VAR3 of an instance of the user-defined function block FB01, which is locally defined in a function of PROG1
FB01.FB2.VAR3	Global	The internal parameter VAR3 of an instance of the user-defined function block FB2 used inside an instance of the user-defined function block FB01 (The limit of nesting of a function block is two)

SEE ALSO For more information about SCS Manager Dictionary View, refer to:

"Dictionary View" in "Workbench" in the Workbench User's Guide

Definition method of instance name

An instance name can be set in the Instance Name field of the tab corresponding to one of five DNP3 data types.

Direct entry from the keyboard

Enter an instance name in the Instance name field directly from the keyboard.

Double-clicking an instance name in the Data menu area

Double-click an instance that is set in the Instance Name field on the Instance tab in the data menu area, and you can set an instance name in the Instance Name field of the line selected in the work space.

Drag and drop an instance name from Dictionary View

By dragging and dropping an instance name from Dictionary View to an Instance Name field of DNP3 Communication Builder, you can register the instance name in the DNP3 Communication Builder. If you drag and drop multiple instance names, they are registered in order starting from the top of the Instance Name field where they are dropped. If instance names are already registered in the Instance Name field, they are overwritten.

SEE ALSO For more information about screen image of drag & drop, refer to:

"● Drag and drop from Dictionary View" on page F1-14

Precaution when setting definitions in the DNP3 Communication Builder

Take note of the following when setting definitions in the DNP3 Communication Builder.

- An instance of DNP3 connection FB should be assigned to one of the indexes, 0 to 499, of a given DNP3 data type.
- The total number of assignable instances of DNP3 communication FBs is limited to 1,000 for all data types combined.
- The Frozen Counter need not have any instance assigned, because Frozen Counters are associated with Binary Counters in a one-to-one correspondence.
- DNP3 data assignments can be changed online without stopping the SCS. When online change is executed, changing the definitions of the DNP3 master is also required.

The actions of SCS during online change are as follows:

- Assume that the type name of a function block instance is being changed. If a data referencing request or setting request for the function block instance of the new type name is received before the change is completed, the SCS returns the following error:

  ```
  IIN2.1 OBJECT_UNKNOWN
  ```

- When a response message for batch specification (Class 0 is specified) is divided into several messages, if online change is executed before the SCS finishes sending all response messages, the SCS stops sending the response messages and returns the following error:

  ```
  IIN2.1 OBJECT_UNKNOWN
  ```

- Any event of the data for which online change is performed is not created during online change.
- If the data types (16 bit, 32 bit, float) of Analog Input, Analog Output, Binary Counter, and Frozen Counter are changed, the event data before the change may be incorrect.
- If a request is received for an Index whose definition was lost after the assignment change, the SCS returns the following error:

  ```
  IIN2.2 PARAMETER_ERROR
  ```

  The same applies to Frozen Counters.
- When Binary Counter is changed online, all values of all Frozen Counters are cleared to 0. However, the events of Frozen Counter which are cleared to 0 due to online change of Binary Counter are not created.

SEE ALSO For more information about precautions when assigning DNP3 data, refer to:

"■ Precautions when assigning DNP3 data" on page G3-22

G3.6 Creating an application logic

Use the Multi-language Editor to create an application logic.

G3.7 Precautions for engineering

The DNP3 slave function of SCS allows the DNP3 master to refer data from SCS or set data to SCS through DNP3 communication. The DNP3 slave function does not affect the safety functions of SCS.

You must install the Ethernet communication module (model: ALE111) to an SCS node for the SCS to communicate with the DNP3 master.

To use the DNP3 slave function, use DNP3 communication FBs. By assigning instances of DNP3 communication FBs to DNP3 data, SCS data can be referred or set from the DNP3 master.

When a variable of the application logic changes, the SCS generates and buffers an event that includes a time stamp and data. This prevents data loss when a communication failure occurs because the DNP3 master can read the relevant event from the SCS's event buffer after the recovery.

Transmission specifications of ALE111

The following table describes the transmission specifications of the Ethernet communication module (model: ALE111) that is required to use the DNP3 slave function.

Table G3.7-1 Transmission specifications of ALE111

Item	Specification
Interface	Ethernet (IEEE 802.3)
	10 BASE-T
Baud rate	10 Mbps

IMPORTANT

- Up to two ALE111 modules per SCS can be used for DNP3 communication. Communication modules for the subsystem communication and Modbus slave communication are not included in the count.
- The ALE111 cannot be installed in any I/O node that is 5 km or further away from the CPU node.
- For the Ethernet network that is used in DNP3 communication, use a network of line quality equivalent to or better than that of the Vnet/IP-Upstream network, which requires bandwidth of 2 Mbps or more and transmission delay of 500 ms or less.

Data setting from the DNP3 master

When setting data in SCS from the DNP3 master, use the Operate - With Acknowledgment command unless you are required not to use it.

Precautions for using Operate - With Acknowledgment command

When setting data by using the Operate - With Acknowledgment command, wait for an acknowledgment before issuing the next data setting request. If the next data setting request is issued consecutively without waiting for an acknowledgment, the following status code will be returned:

```
PROCESSING_LIMITED
```

If PROCESSING_LIMITED is returned, issue the data setting request again because the target data may not have been set.

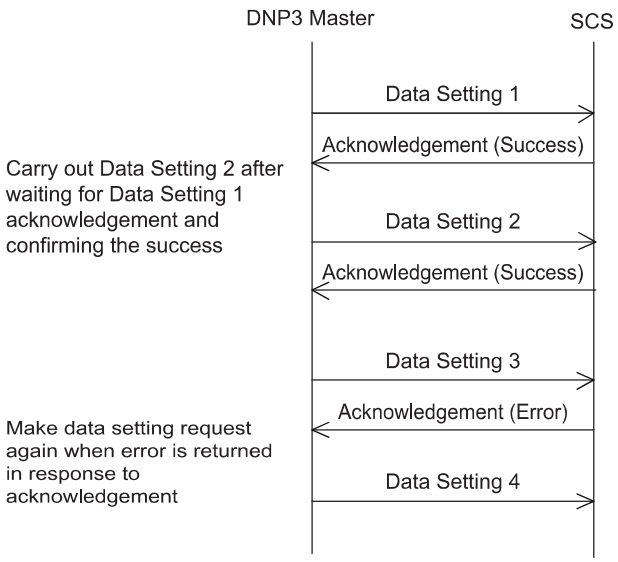


Figure G3.7-1 Data setting request with acknowledgment

Precautions for using Operate - Without Acknowledgment command

When setting data by using the Operate - Without Acknowledgment command, read back the event or current value to confirm that the target value has been set, before issuing the next data setting request.

IMPORTANT

It takes time before the set value can be read, so ensure a sufficiently long wait time before the read-back. If the value is not yet set when checked after waiting for sufficiently long time, issue the data setting request again.

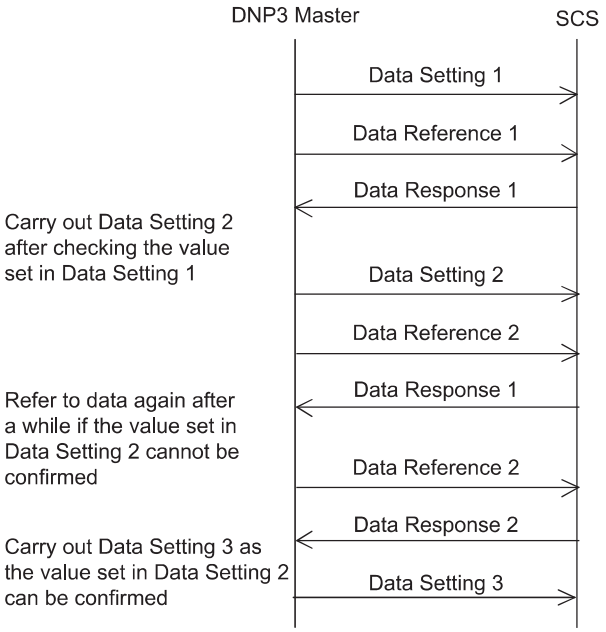


Figure G3.7-2 Data setting request without acknowledgment

Maximum time before the set value can be referenced

After setting data, the event or current value can be read back to confirm that the target value has been set. The following time must elapse before the set value can be read.

The maximum time that must elapse before the set value can be referenced is the sum of the maximum time that is required for the set data to be set to the variable of the application logic, and the maximum time required for the value to be referenced using DNP3 communication after the variable of the application logic is set.

- Maximum time required for the set data to be set to the variable of the application logic

  ```
  Scan period of application logic x Number of data setting requests from exter
  nal connection function
  ```

- Maximum time required for the value to be referenced using DNP3 communication after the variable of the application logic is set

  ```
  Scan period of the external communication function
  ```

- Maximum time before the set value can be referenced

  ```
  Maximum time before the set value can be referenced = Scan period of applicat
  ion logic x Number of data setting requests from external connection function
   + Scan period of external connection function
  ```

Method of response upon event acquisition

To acquire events from the SCS, you must set the event response method of the SCS to "Single fragment."

Setting "Multiple fragments" as the event response method of the SCS allows the DNP3 master to acquire events efficiently, but it may disable data setting request and other processes.

TIP "Data setting" includes setting data using Modbus or other communication.

Precautions when setting the time through DNP3 communication

If multiple SCSs are connected to the Vnet/IP-Upstream network and the time of the SCSs is set by using the DNP3 communication, you must set the time of only one SCS from each Vnet/IP-Upstream domain. When you set the time for multiple SCSs by using DNP3 communication, it may take 10 seconds for the stations that are connected to the Vnet/IP-Upstream network to synchronize.

Engineering for DNP3_CT_16/DNP3_CT_32

To use the DNP3_CT_16/DNP3_CT_32 as a counter, create a calculation application by using the output value of the DNP3_CT_16/DNP3_CT_32 from the previous scan and input value of an external device, and so on.

Create a calculation application as follows:

- Define a variable.
- Use the defined variable and the input value from an external device for the calculation, and connect the result to the input of DNP3_CT_16/DNP3_CT_32.
- Write the output of DNP3_CT_16/DNP3_CT_32 to the defined variable.

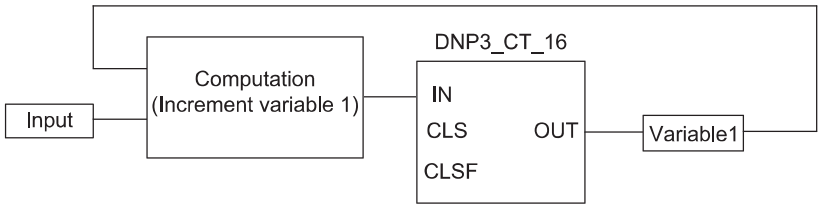


Figure G3.7-3 Engineering example for DNP3_CT_16

Create an application that sets the value of DNP3_CT_16/DNP3_CT_32 to zero by using the DNP3 communication function when the value exceeds the maximum limit it can handle.

TIP

The range of data that DNP3_CT_16/DNP3_CT_32 can handle is as follows:

- DNP3_CT_16: 0 to 65535 of the DINT type
- DNP3_CT_32: 0 to 2147483647 of the DINT type

In the scan period during which a reset request from the DNP3 communication function is received, set the value of DNP3_CT_16/DNP3_CT_32 and the defined variable to zero.

Precautions when assigning DNP3 data

It is recommended for efficient DNP3 communication that when DNP3 data is assigned, the Indexes must be defined consecutively from 0 without missing number.

Precautions for the duplexed communication interface

When implementing a duplexed communication interface, ensure that the DNP3 master communicates with either one of the two ALE111 modules. If the DNP3 communication is used on both ALE111 at the same time, the SCS will take the following action.

The SCS will process the request received from both ALE111. The SCS receives data setting and freeze & clear requests from both ALE111 and processes the requests twice, but the SCS can only process one request for each scan period, so there is a time lag between the two data setting actions.

SEE ALSO

For more information about restrictions when configuring the DNP3 communication data, refer to:

"● Limitations on data setting using DNP3 communication" on page G2-6

Precautions when reconnecting

ALE111 maintains its TCP/IP connection for a maximum of 34 seconds after it loses its DNP3 connection with the DNP3 master. During this time, the DNP3 master cannot connect with ALE111 via TCP/IP because the connection is being used. To reconnect in the event of an error, wait 34 seconds before trying again.

G3.8 Troubleshooting

If a communication module error occurs, you can use the SCS Maintenance Support Tool to acquire information on the communication module and communication error information. This section describes typical troubleshooting cases.

There is no response and communication fails

If there is no response and communication fails, check the following points:

- Check if the TCP/IP settings of the communication module match those on the master side.
- Use the SCS Maintenance Support Tool to check the status of the communication module.
- Use Network Monitor or other tools to analyze the protocol managing the send/receive frames.
- Check if there is enough CPU time available. Response may be delayed when the CPU load is high.

Connection cannot be established and communication fails

If connection cannot be established and communication fails, check the following points:

- Check if the destination IP address and port number are correct.
- If the DNP3 protocol communication between the DNP3 master and SCS is cut off without the DNP3 master notifying the end of communication to the SCS, connection to the SCS becomes possible again after up to 34 seconds.

The SCS time is not synchronized with the DNP3 master time

If the SCS time is not synchronized with the DNP3 master time, check the following procedures.

SNTP servers are used

- Check if the time of the SNTP server on the Ethernet side is synchronized with that of the SNTP server on the Vnet/IP-Upstream side.
- Check if the DNP3 master and SCS are synchronized with their respective SNTP servers.

SNTP servers are not used

Check if an application that issues time setting requests to the SCS exists on the DNP3 master.

Appendix 1. Information regarding engineering for subsystems

Appendix 1.1 Differences between safety subsystem communication I/O, subsystem communication I/O, and AIO/DIO modules I/O

The following table shows the differences between safety subsystem communication I/O, subsystem communication I/O, and AIO/DIO modules I/O.

Table Appendix 1.1-1 Differences between safety subsystem communication I/O, subsystem communication I/O, and AIO/DIO modules I/O

Classification	Item	Safety subsystem communication I/O	Subsystem communication I/O	AIO/DIO modules I/O
General	Number of channels	Variable	Variable	Fixed
	Safety	Safety (*1)	interference-free	Safety
Communication data, AIO/DIO data	Variable	FB instance	FB instance	Structure variable
	Data type	DINT, REAL	BOOL, DINT, REAL	BOOL, REAL
	Data status	Safety: Status of devices to the safety communication function	Status of subsystems to communication modules Errors in subsystems are not applicable	Status of I/O terminals to I/O modules
		interference-free: Status of devices to the safety communication module Only communication errors within the ISA100 wireless communication system are applicable		
Forcing	Lock	Individual communication definitions, all communication module inputs	All communication module inputs, all outputs, all inputs/outputs	Individual channels, all module inputs, all outputs, all inputs/outputs
	Value set	Individual data	Individual data	Individual channels
	Lock management	SYS_FORCE_SF Communication related system alarms Communication I/O Lock Window	SYS_FORCE_SC Communication related system alarms Communication I/O Lock Window	SYS_FORCE System alarms I/O Lock Window
Error handling action	Output enable start	Not required. Output enable operation allowed even when there is a module error	Output enable operation from SENG, or operation by SYS_STAT_SC Output enable allowed even when there is a module error	Output enable operation from SENG, or operation by SYS_STAT Output will not be enabled for modules with errors
	Input module error	Specification of behavior at fault allowed (specified input value at fault, specified to hold value)		
CENTUM Integration	CENTUM Integration	Available (%XB)	Available (%WB)	Available (%Z, %Y, %WB)
Online change	Online change download	Available (*2)	Available	Available
Test function	Virtual test	Available		
	Target test	Available		

*1: Non-safety data of PROFINET can also be handled.
*2: PROFINET communication between S2LP131 and YFGW410 and PROFIsafe communication between the SCS and GS01 are both disconnected and S2LP131 restarts. After restarting, PROFINET communication and PROFIsafe communication will

resumed. During this process, PROFIsafe communication between S2LP131 and GS01 will be in a state of error and the input value will be the input value at fault.

Appendix 1.2 Items of I/O Parameter Builder

You can set the I/O parameters of the fire and gas communication module with IOM Definition Editor of AD Suite. By executing RS Generation, you can reflect the setting items onto the fire and gas communication module parameter tab in I/O Parameter Builder. Reflected items become read-only in I/O Parameter Builder.

The following table shows the displayed I/O parameter items for the fire and gas communication module.

Table Appendix 1.2-1 Displayed I/O parameter items for the fire and gas communication module

Title	Description	Remarks
Node Number	The node number corresponding to the mounting position of the module is displayed.	
Slot Number	The slot number corresponding to the mounting position of the module is displayed.	
Device	The type of module is displayed.	
Dual-Redundant	Whether the module is used in a single or dual-redundant configuration is displayed.	Single only
Device Number	The device number assigned to the module is displayed.	
Connection Device	The type of connection device (safety subsystem) is displayed.	Fixed as S_FGCOM
Comment	A comment regarding the module is displayed.	
Host Name	The host name of the module is displayed.	
IP Address	The IP address of the module is displayed.	
Subnet Mask	The subnet mask of the module is displayed.	
Default Gateway	The gateway address of the module is displayed.	
Dual-Redundant YFGW Switching Time	The time during which a communication error accompanying a switchover is not notified when an error occurs with a dual-redundant YFGW410 is displayed.	

Appendix 1.3 Items of Communication I/O Builder

You can set the communication definition of the fire and gas communication module with Safety Communication I/O Editor of AD Suite. By executing RS Generation, you can reflect the setting items onto each tab in Communication I/O Builder. Communication I/O Builder is configured of the following four tabs. For fire and gas communication, you will be using the Safety Subsystem Comm. I/O Definition tab and the Safety Subsystem Comm. I/O Wiring tab.

- Comm. I/O Definition tab
- Comm. I/O Wiring tab
- Safety Subsystem Comm. I/O Definition tab
- Safety Subsystem Comm. I/O Wiring tab

Reflected items become read only in Communication I/O Builder.

Safety Subsystem Comm. I/O Definition tab

The Safety Subsystem Comm. I/O Definition tab is displayed when the SCS is using I/O list engineering with SCSP3.

Element

The address of the data storage area used for safety subsystem communication I/O is displayed.

Format: %XWnnnn

%XW: Fixed

nnnn: 0001 to 4000

Buffer

The storage area address size of the safety subsystem communication I/O data used by fire and gas communication programs is displayed. This is assigned to only the odd numbers of %XW.

Program Name

A program name combining the node number of S2LP131, slot number, and communication program name is displayed.

Format: n-s Fixed character string

n: Node number

s: Slot number

Fixed character string: S_FGCOM

Size

The assigned size (data length) from the beginning address set in "Device Address" is displayed.

Station Name

The host name of any device connected with PROFINET is displayed.

- **IP Address**

  The IP address of any device connected with PROFINET is displayed.

- **Subnet Mask**

  The subnet mask of any device connected with PROFINET is displayed.

- **Default Gateway**

  The default gateway of any device connected with PROFINET is displayed.

- **PN-Updating Time**

  The interval for updating the PROFINET communication I/O data is displayed.

- **PN-Watchdog Time**

  The interval at which communication of PROFINET is checked for whether it is running correctly is displayed.

- **PN-Slot**

  The slot number used by PROFINET is displayed.

- **PN-Module**

  The name of the PROFINET module is displayed.

- **PN-Sub Slot**

  The subslot number used by PROFINET is displayed.

- **PN-Submodule**

  The name of the PROFINET submodule is displayed.

- **PN-Alarm Group**

  A string sequence for every communication definition added to an alarm message.

  Display example of SS-SCPATH Error:

  ```
  SCS0101 SS-SCPATH Error FIO NODE 01 SLOT 01 PORT 01 GS01-001-PV Code=A3B0
  ```

  GS01-001-PV is the string sequence for PN-Alarm Group.

- **PN-Data**

  The data name defined in the PROFINET GSDML file is displayed.

- **Data Type**

  The type of data when exchanging data with PROFINET is displayed.

- **Comment**

  A comment is displayed.

- **F Parameter**

  The F parameter used when performing safety communication with PROFIsafe is displayed.

  The following table shows a list of F parameters.

Table Appendix 1.3-1 List of F parameters

Parameter name	Setting value	Remarks
F_Check_iPar	No check, Check	
F_SIL	SIL1, SIL2, SIL3, NonSIL	
F_CRC_Length	3Byte CRC, 4Byte CRC	
F_CRC_Seed	0, 1	
F_Passivation	0, 1	
F_Block_ID	1	
F_Par_Version	V2-Mode	
F_Source_Addr	Numerical value	Controller identification address
F_Dest_Addr	Numerical value	Device identification address
F_WD_Time	Numerical value	Monitors whether a signal arrives within this time
F_WD_Time_2	Numerical value	
F_iPar_CRC	Numerical value	
F_Par_CRC	Numerical value	

Safety Subsystem Comm. I/O Wiring tab

The Safety Subsystem Comm. I/O Wiring tab shows a list of elements corresponding to the areas assigned in the Safety Subsystem Comm. I/O Definition tab.

Element

The element number (%XB) automatically assigned according to the element number (%XW) set with PN-data and the data type on the Safety Subsystem Comm. I/O Definition tab is displayed.

Example:

When the element is %XW2001
%XB200101

PN-Data

The PN-data assigned to the Safety Subsystem Comm. I/O Definition tab is displayed.

Variable Name

The instance name of the FB used for fire and gas communication I/O set to the variable name with Safety Communication I/O Editor is displayed.

The following table shows the data types and specifiable variable types.

Table Appendix 1.3-2 Data types and specifiable variable types

Object	Data type	Type
PROFINET	Analog input (8-bit signed integer) Analog input (16-bit signed integer) Analog input (32-bit signed integer) Analog input (8-bit unsigned integer) Analog input (16-bit unsigned integer) Analog input (32-bit unsigned integer)	PNI_I
	Analog input (32-bit floating)	PNI_R

Continues on the next page

Table Appendix 1.3-2 Data types and specifiable variable types (Table continued)

Object	Data type	Type
Fire and gas communication	Analog input (8-bit signed integer) Analog input (16-bit signed integer) Analog input (32-bit signed integer) Analog input (8-bit unsigned integer) Analog input (16-bit unsigned integer) Analog input (32-bit unsigned integer)	PSI_I
	Analog input (32-bit floating)	PSI_R

Type

The selected variable type is displayed.

Comment

The comment of the variable is displayed.

Input processing at Fault

This is the setting item you can use to specify the value to pass to the logic in place of the actual input when a communication error is detected.

You can specify this item using AD Suite only when the data type is analog input.

Table Appendix 1.3-3 Input processing at fault

Option	Description
Hold	Holds the value from right before the error when an error is detected.
Fixed value	Uses the input value specified in "Input Value at Fault" when an error is detected.

Input Value at Fault

This is the value to be used as the input value instead of the process value when "Fixed Value" is specified in "Input Processing at Fault."

Appendix 2. DNP3 field device Profile

This section describes the DNP3 specifications of the SCS. Refer to the information listed here to confirm that slave devices meeting these specifications can connect to the DNP3 master that communicates with the SCS.

Appendix 2.1 Device properties

Table Appendix 2.1-1 Device properties

DEVICE IDENTIFICATION	
Device Function:	[ ] Master [v] Outstation
Vendor Name:	Yokogawa Electric Corporation
Device Name:	ProSafe-RS SCS
Device manufacturer's hardware version string:	
Device manufacturer's software version string:	
Device Profile Document Version Number:	2013
DNP Levels Supported for:	Outstations Only Requests and Responses [v] None - partially supported [v] Level 1 - except Unsolicited Response; [v] Level 2 - except Device Attributes; [v] Level 3 - except Device Attributes [v] Level 4 - partially supported
Supported Function Blocks:	[ ] Self-Address Support [ ] Data Sets [ ] File Transfer [ ] Virtual Terminal [ ] Mapping to IEC 61850 Object Models defined in a DNP3 XML file. [ ] Function code 31, activate configuration [ ] Authentication
Methods to set Configurable Parameters:	[ ] XML - Loaded via DNP3 File Transfer [ ] XML - Loaded via other transport mechanism [ ] Terminal - ASCII Terminal Command Line [v] Software - Vender software named "Multi Language Editor", "I/O Parameter Builder", "DNP3 Communication Builder" and "IOM Definition Editor" [ ] Proprietary file loaded via DNP3 File Transfer [ ] Proprietary file loaded via other transport mechanism [ ] Direct - Keypad on device front panel [ ] Factory - Specified when device is ordered [ ] Protocol - Set via DNP3 (e.g. assign class, write deadband) [ ] Other - explain:
DNP3 XML files available On-line:	Rd Wr [ ] dnpDP.xml - Complete Device Profile [ ] dnpDPcap.xml - Device Profile Capabilities [ ] dnpDPcfg.xml - Device Profile config. values [ ] [ ] *.xml
External DNP3 XML files available Off-line:	Rd Wr [ ] [ ] dnpDP.xml - Complete Device Profile [ ] [ ] dnpDPcap.xml - Device Profile Capabilities [ ] [ ] dnpDPcfg.xml - Device Profile config. values [ ] [ ] *.xml
Connections Supported:	[ ] Serial (complete section "SERIAL CONNECTIONS") [v] IP Networking (complete section "IP NETWORKING") [ ] Other, explain
Conformance Testing	[v] Self-tested [ ] Independently tested, version Test organization name

Continues on the next page

Table Appendix 2.1-1 Device properties (Table continued)

IP NETWORKING	
Port Name:	
Type of End Point:	[ ] TCP Initiating (Master Only) [v] TCP Listening (Outstation Only) [ ] TCP Dual (required for Master) [ ] UDP Datagram (required)
IP Address of this Device:	
Subnet Mask:	
Gateway IP Address:	
Accepts TCP Connections or UDP Datagrams from:	[v] Allows all [ ] Limits based on IP address [ ] Limits based on list of IP address [ ] Limits based on a wildcard IP address [ ] Limits based on list of wildcard IP address [ ] Other, explain:
IP Address(es) from which TCP Connections or UDP Datagrams are accepted.	
TCP Listen Port Number:	[ ] Not Applicable (Master w/o dual end point) [ ] Fixed at 20000 [v] Configurable, range 0 to 65535 - by I/O Parameter Builder, or IOM Definition Editor - default = 20000 - The number must NOT be duplicated with other TCP Listen Port Numbers on the controller. [ ] Configurable, selectable from [ ] Configurable, other, describe:
TCP Listen Port Number of remote device:	[v] Not Applicable (Outstation w/o dual end point) [ ] Fixed at 20000 [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe:
TCP Keep-alive timer:	[v] Fixed at 30000 ms [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe:
Local UDP Port:	[ ] Fixed at 20000 [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe:
Destination UDP port for initial unsolicited null responses:	[ ] None [ ] Fixed at 20000 [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe:
Destination UDP port for responses:	[ ] None [ ] Fixed at 20000 [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe: [ ] Use source port number
Multiple Master Connections:	[ ] Supports multiple masters (Outstations only) If supported, the following methods may be used: [ ] Method 1 (based on IP address) [ ] Method 2 (based on IP port number) [ ] Method 3 (browsing for static data)

Continues on the next page

Table Appendix 2.1-1 Device properties (Table continued)

Time Synchronization Support:	[v] DNP3 LAN procedure (function code 24) [v] DNP3 Write Time (not recommended over LAN) [ ] Other, explain [ ] Not Supported
LINK LAYER	
Data Link Address: (DNP3 Outstation Address)	[ ] Fixed at [v] Configurable, range 0 to 0xffff - Configurable by DNP3 Communication Builder [ ] Configurable, selectable from [ ] Configurable, other, describe:
DNP3 Source Address Validation:	[ ] Never [v] Always, one address allowed [ ] Always any one of multiple addresses allowed [ ] Sometimes, explain:
DNP3 Source Address(es) expected when Validation is Enables: (DNP3 Master Address)	[v] Configurable to any 16 bit DNP Data Link Address value - Configurable by DNP3 Communication Builder [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe:
Self Address Support using address 0xFFFC:	[ ] Yes (only allowed if configurable) [v] No
Sends Confirmed User Data Frames:	[v] Never [ ] Sometimes, explain: [ ] Always
Data Link Layer Confirmation Timeout:	[v] None [ ] Fixed at [ ] Configurable, range to ms [ ] Configurable, selectable from ms [ ] Configurable, other, describe: [ ] Variable, explain:
Maximum Data Link Retries:	[v] Never Retries [ ] Fixed at [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe:
Maximum number of octets Transmitted in a Data Link Frame:	[v] Fixed at 292 [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe:
Maximum number of octets Received in a Data Link Frame:	[v] Fixed at 292 [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe:
APPLICATION LAYER	
Maximum number of octets Transmitted in an Application Layer Fragment other than File Transfer:	[v] Fixed at 1600 [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe:
Maximum number of octets Transmitted in an Application Layer Fragment containing File Transfer:	[ ] Fixed at [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe:
Maximum number of octets that can be Received in an Application Layer Fragment :	[v] Fixed at 1600 [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe:

Continues on the next page

Table Appendix 2.1-1 Device properties (Table continued)

Timeout waiting for Complete Application Layer Fragment:	[ ] None [v] Fixed at 15 seconds [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe: [ ] Variable, explain:
Maximum number of objects allowed in a single control request for CROB (group 12):	[v] Fixed at 1 [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe: [ ] Variable, explain:
Maximum number of objects allowed in a single control request for Analog Outputs (group 41):	[v] Fixed at 1 [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe: [ ] Variable, explain:
Maximum number of objects allowed in a single control request for Data Sets (groups 85, 86, 87):	[ ] Fixed at [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe: [ ] Variable, explain:
Supports mixing object groups (AOBs, CROBs and Data Sets) in the same control request:	[ ] Not applicable - controls are not supported [ ] Yes [v] No
Control Status Codes Supported	[v] 1 - Timeout [v] 2 - NO_SELECT [v] 3 - FORMAT_ERROR [v] 4 - NOT_SUPPORTED [v] 5 - ALREADY_ACTIVE [ ] 6 - HARDWARE_ERROR [ ] 7 - LOCAL [v] 8 - TOO_MANY_OBJS [ ] 9 – NOT_AUTHORIZED [ ] 10 – AUTOMATION_INHIBIT [v] 11 – PROCESSING_LIMITED [ ] 12 – OUT_OF_RANGE [ ] 13 – DOWNSTREAM_LOCAL [ ] 14 – ALREADY_COMPLETE [ ] 15 – BLOCKED [ ] 16 – CANCELLED [ ] 17 – BLOOCKED_OTHER_MASTER [ ] 18 – DOWNSTREAM_FAIL [ ] 126 – RESERVED [ ] 127 - UNDEFINED
ITEMS FOR OUTSTATIONS	
Timeout waiting for Application Confirm of solicited response message:	[ ] None [v] Fixed at 10000 ms [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other, describe: [ ] Variable, explain:
How often is time synchronization required from the master:	[v] Never needs time [ ] Within seconds after IIN1.4 is set [v] Periodically, fixed at 1800 seconds - IIN1.4 will be set at startup and every 30 minutes (1800 seconds) after the last "Time Synchronization" [ ] Periodically, between and seconds
Device Trouble Bit IIN1.6:	[v] Never used [ ] Reason for setting:

Continues on the next page

Table Appendix 2.1-1 Device properties (Table continued)

File Handle Timeout:	[v] Not Applicable, Files Not Supported [ ] Fixed at ms [ ] Configurable, range to ms [ ] Configurable, selectable from ms [ ] Configurable, other, describe: [ ] Variable, explain:
Event Buffer Overflow Behavior:	[v] Discard the oldest event [v] Discard the newest event - Configurable by DNP3 Communication Builder [ ] Other, explain
Event Buffer Organization:	[v] Per Object Group [ ] Per Class Class 1: [ ] Fixed at_____ [ ] Configurable, range _____ to _____ [ ] Configurable, selectable from ___,___,___ [ ] Configurable, other, describe_____ Class 2: [ ] Fixed at_____ [ ] Configurable, range _____ to _____ [ ] Configurable, selectable from ___,___,___ [ ] Configurable, other, describe_____ Class 3: [ ] Fixed at_____ [ ] Configurable, range _____ to _____ [ ] Configurable, selectable from ___,___,___ [ ] Configurable, other, describe_____ [ ] Single Buffer [ ] Fixed at_____ [ ] Configurable, range _____ to _____ [ ] Configurable, selectable from ___,___,___ [ ] Configurable, other, describe_____ [ ] Other, describe _____
Sends Multi-Fragment Responses:	[v] Yes [v] No - Configurable by DNP3 Communication Builder
Last Fragment Confirmation:	[v] Always [ ] Sometimes, explain [ ] Never
DNP Command Settings preserved through a device reset:	[ ] Assign Class [ ] Analog Deadbands [ ] Data Set Prototypes [ ] Data Set Descriptors. [ ] Function Code 31 Activate Configuration.
Supports configuration signature	[ ] Configuration signature supported If configuration signature is supported, then the following algorithm(s) are available for calculating the signature: Algorithm Name:
Requests Application Confirmation	For event response [v]Yes [ ]No [ ]Configurable For non-final fragments [v]Yes [ ] No [ ] Configurable
OUTSTATION UNSOLICITED RESPONSE SUPPORT	
Supports Unsolicited Reporting:	[v] Not Supported [ ] Configurable, selectable from On or Off
INDIVIDUAL FIELD OUTSTATION PARAMETERS	

Continues on the next page

Table Appendix 2.1-1 Device properties (Table continued)

Analog Input Deadbands:	[ ] Configurable - Per Point - by Master [v] Configurable - Per Point - by Outstation - Configurable by Multi Language Editor	
Class Assign:	[ ] Configurable - Per Point - by Master [v] Configurable - Per Point - by Outstation - Configurable by Multi Language Editor	
Time Value for all DNP3 protocol time stamps reported and time synchronization messages:	[v] Fixed at UTC [ ] Configurable, selectable from "Local Time" or "UTC"	
File Handling:	[v] Not Supported	
Control Relay Output Block (CROB) Latch Operation:	[v] Yes - "CROB Operation" is available for Binary Outputs. - Output Block Operation (CROB and AOB) cannot run without error more than four times a second.	
Control Relay Output Block (CROB) Pulse, Trip and Close Operation:	[v] Not Supported	
Analog Output Block (AOB) Operation:	[v] Yes - Output Block Operation (CROB and AOB) cannot run without error more than four times a second.	
Freeze & Clear Operation	Freeze & Clear Operation is available only when the number of Binary Counter is defined as 32 or less.	
Time Synchronization Accuracy	If you use Time Synchronization using DNP3 communication, time synchronization accuracy between DNP3 master and SCS is up to the scan cycle of application logic plus 1000 ms.	
Delay of data setting	There is delay after SCS receives the setting request of DNP3 data until the actual data is updated. This delay is dependent on the scanning cycle and the number of requests from external connection devices.	
Support Data Types	DNP3 Data type	IEC data type treated by SCS
	Binary Input	BOOL
	Binary Output	BOOL
	16-Bit Binary Counter	DINT
	32-Bit Binary Counter	DINT
	16-Bit Frozen Counter	DINT
	32-Bit Frozen Counter	DINT
	16-Bit Analog Input	DINT
	32-Bit Analog Input	DINT
	Single-Precision Floating Point Analog Input	REAL
	16-Bit Analog Output	DINT
	32-Bit Analog Output	DINT
	Single-Precision Floating Point Analog Output	REAL

Continues on the next page

Table Appendix 2.1-1 Device properties (Table continued)

Online maintenance	DNP3 data can be modified by using online change without stopping SCS. The following list shows how SCS behaves when online change is performed: - If the SCS receives a write request or a read request while the data in the SCS is being updated by the online change, the SCS returns the error IIN2.1 OBJECT_UNKNOWN. - If the Class 0 response is divided into multiple messages, running the online change before the SCS finishes sending response messages causes the SCS to stop sending messages and return the error IIN2.1 OBJECT_UNKNOWN. - While the online change is running, events for the data in the SCS are not generated. - If you change the detailed data type of Analog Input, Analog Output, Binary Counter, or Frozen Counter, the event data before the change may be converted into an invalid data. - If a write request or a read request to the data that has been deleted by the online change is received, the SCS returns the error IIN2.2 PARAMETER_ERROR. - If you perform online change on Binary Counter, the SCS clears all Frozen Counters to 0.

This Device Properties is referred to "DNP3 SPECIFICATION, Version 2013, November-2013".

Appendix 2.2 Capabilities for device database

Table Appendix 2.2-1 Capabilities for device database

SINGLE-BIT BINARY INPUT POINTS Static (Steady-State) Object Number: 1 Event Object Number: 2	
Static Variation reported when variation 0 requested or in response to Class polls :	[ ] Variation 1 - packed format [v] Variation 2 - with flag [ ] Based on point index
Event Variation reported when variation 0 requested or in response to Class polls:	[ ] Variation 1 - without time [v] Variation 2 - with absolute time [ ] Variation 3 - with relative time [ ] Based on point index
Event reporting mode:	[ ] Only most recent [v] All events
Binary Inputs included in Class 0 response:	[v] Always [ ] Never [ ] Only if the point is assigned to a class [ ] Based on point index
Binary Inputs Event Buffer Organization	[ ] Fixed at [v] Configurable, range 0 to 135000 - Configurable by DNP3 Communication Builder [ ] Configurable, selectable from , , [ ] Configurable, other, describe
BINARY OUTPUT STATUS AND CONTROL RELAY OUTPUT BLOCK Binary Output Status Object Number: 10 Binary Output Event Object Number 11 CROB Object Number 12	
Binary Output Status included in Class 0 response:	[v] Always [ ] Never [ ] Only if point is assigned to a class [ ] Based on point index
Static Variation reported when variation 0 requested or in response to Class polls:	[ ] Variation 1 - packed format [v] Variation 2 – output status with flag [ ] Based on point index
Event Variation reported when variation 0 requested or in response to Class polls:	[ ] Variation 1 – status without time [v] Variation 2 – status with time [ ] Based on point index
Event reporting mode:	[ ] Only most recent [v] All events
Maximum Time between Select and Operate:	[ ] Not Applicable [ ] Fixed at seconds [v] Configurable, range from 1 to 600 seconds - by DNP3 Communication Builder ; (default=5) [ ] Configurable, selectable from seconds [ ] Configurable, other, describe: [ ] Variable, explain: [ ] Based on point index
Binary Outputs Event Buffer Organization	[ ] Fixed at _____ [v] Configurable, range 0 to 135000 - Configurable by DNP3 Communication Builder [ ] Configurable, selectable from ____,____,____ [ ] Configurable, other, describe_____
COUNTERS/FROZEN COUNTERS Static Counter Object Number: 20 Static Frozen Counter Object Number: 21 Counter Event Object Number: 22 Frozen Counter Event Object Number: 23	

Continues on the next page

Table Appendix 2.2-1 Capabilities for device database (Table continued)

Static Counter Variation reported when variation 0 requested or in response to Class 0 polls:	[ ] Variation 1 - 32-bit with flag [ ] Variation 2 - 16-bit with flag [ ] Variation 5 - 32-bit without flag [ ] Variation 6 - 16-bit without flag [v] Based on point index (Variation 1 or 2)
Counter Event Variation reported when variation 0 requested or in response to Class 0 polls:	[ ] Variation 1 - 32-bit with flag [ ] Variation 2 - 16-bit with flag [ ] Variation 5 - 32-bit with flag and time [ ] Variation 6 - 16-bit with flag and time [v] Based on point index (Variation 5 or 6)
Counter included in Class 0 response:	[v] Always [ ] Never [ ] Only if point is assigned to a class [ ] Based on point index
Counter Event reporting mode:	[ ] A: Only most recent (value at time of event) [ ] B: Only most recent (value at time of response) [v] C: All events [ ] Based on point index
Static Frozen Counter Variation reported when variation 0 requested or in response to Class polls:	[ ] Variation 1 - 32-bit with flag [ ] Variation 2 - 16-bit with flag [ ] Variation 5 - 32-bit with flag and time [ ] Variation 6 - 16-bit with flag and tie [ ] Variation 9 – 32-bit without flag [ ] Variation 10 – 16-bit without flag [v] Based on point index (Variation 1 or 2)
Frozen Counter Event Variation reported when variation 0 requested or in response to Class polls:	[ ] Variation 1 - 32-bit with flag [ ] Variation 2 - 16-bit with flag [ ] Variation 5 - 32-bit with flag and time [ ] Variation 6 - 16-bit with flag and time [v] Based on point index (Variation 1 or 2)
Frozen Counters included in Class 0 response:	[v] Always (default) [v] Never (can be selected by DNP3 Communication Builder) [ ] Only if point is assigned to a class [ ] Based on point index
Frozen Counter Event reporting mode:	[ ] A: Only most recent frozen value [v] B: All frozen values [ ] Based on point index
Counter Roll Over at:	[ ] 16 Bits (65,535) [ ] 32 Bits (4,294,967,295) [ ] Other Fixed Value [ ] Configurable, range to [ ] Configurable, selectable from [ ] Configurable, other describe: [v] Based on point index (16 Bits (65,535) or 32 Bits (2,147,483,647))
Counter frozen by means of:	[v] Master Request [ ] Freezes itself without concern for time of day [ ] Freezes itself and requires time of day [ ] Other, explain:
Counters Event Buffer Organization	[ ] Fixed at _____ [v] Configurable, range 0 to 135000 - Configurable by DNP3 Communication Builder [ ] Configurable, selectable from _____,_____,_____ [ ] Configurable, other, describe_____
Frozen Counters Event Buffer Organization	[ ] Fixed at _____ [v] Configurable, range 0 to 135000 - Configurable by DNP3 Communication Builder [ ] Configurable, selectable from _____,_____,_____ [ ] Configurable, other, describe_____

Continues on the next page

Table Appendix 2.2-1 Capabilities for device database (Table continued)

ANALOG INPUT POINTS Static (Steady-State) Object Number: 30 Event Object Number: 32 Analog Input Deadband Object Number: 34	
Static Variation reported when variation 0 requested or in response to Class 0 polls:	[ ] Variation 1 - 32-bit with flag [ ] Variation 2 - 16-bit with flag [ ] Variation 3 - 32-bit without flag [ ] Variation 4 - 16-bit without flag [ ] Variation 5 - single-precision floating point with flag [ ] Variation 6 - double-precision floating point with flag [v] Based on point index (variation 1, 2 or 5)
Event Variation reported when variation 0 requested or in response to Class 0 polls:	[ ] Variation 1 - 32-bit without time [ ] Variation 2 - 16-bit without time [ ] Variation 3 - 32-bit with time [ ] Variation 4 - 16-bit with time [ ] Variation 5 - single-precision floating point w/o time [ ] Variation 6 - double-precision floating point w/o time [ ] Variation 7 - single-precision floating point with time [v] Variation 8 - double-precision floating point with time [v] Based on point index (Variation 2, 4 or 7)
Event reporting mode:	[ ] A: Only most recent (value at time of event) [ ] B: Only most recent (value at time of response) [v] C: All events [ ] Based on point index
Analog Inputs included in Class 0 response:	[v] Always [ ] Never [ ] Only if point is assigned to a class [ ] Based on point index
How Deadbands are set:	[ ] A. Global Fixed [ ] B. Configurable through DNP [v] C. Configurable via other means - by Multi Language Editor [ ] D. Other, explain [ ] Based on point index
Analog Input Deadband Algorithm:	[v] Simple [ ] Integrating [ ] Other, explain [ ] Based on point index
Analog Inputs Event Buffer Organization:	[ ] Fixed at _____ [v] Configurable, range 0 to 135000 - Configurable by DNP3 Communication Builder [ ] Configurable, selectable from ____,____,____ [ ] Configurable, other, describe_____
ANALOG OUTPUT STATUS AND ANALOG OUTPUT CONTROL BLOCK Analog Output Status Object Number: 40 Analog Output Control Block Object Number 41 Analog Output Event Object Number 42	
Static Analog Output Status Variation reported when variation 0 requested or in response to Class 0 polls	[ ] Variation 1 - 32-bit with flag [ ] Variation 2 - 16-bit with flag [ ] Variation 3 - single-precision floating point with flag [ ] Variation 4 - double-precision floating point with flag [v] Based on point index (Variation 1, 2 or 3)
Analog Output Status included in Class 0 response:	[v] Always [ ] Never [ ] Only if point is assigned to a class [ ] Based on point index

Continues on the next page

Table Appendix 2.2-1 Capabilities for device database (Table continued)

Event Variation reported when variation 0 requested or in response to Class 0 polls:	[ ] Variation 1 - 32-bit without time [ ] Variation 2 - 16-bit without time [ ] Variation 3 - 32-bit with time [ ] Variation 4 - 16-bit with time [ ] Variation 5 - single-precision floating point w/o time [ ] Variation 6 - double-precision floating point w/o time [ ] Variation 7 - single-precision floating point with time [ ] Variation 8 - double-precision floating point with time [v] Based on point index (Variation 3, 4 or 7)
Event reporting mode:	[ ] Only most recent [v] All events
Maximum Time between Select and Operate:	[ ] Not Applicable [ ] Fixed at seconds [v] Configurable, range from 1 to 600 seconds - by DNP3 Communication Builder (default=5) [ ] Configurable, range to seconds [ ] Configurable, selectable from seconds [ ] Configurable, other, describe: [ ] Variable, explain: [ ] Based on point index
Analog Outputs Event Buffer Organization:	[ ] Fixed at _____ [v] Configurable, range 0 to 135000 - Configurable by DNP3 Communication Builder [ ] Configurable, selectable from _____,_____,_____ [ ] Configurable, other, describe_____

This Device Properties is referred to "DNP3 SPECIFICATION, Version 2013, November-2013".

Appendix 2.3 Implementation table

Table Appendix 2.3-1 Implementation table

DNP OBJECT GROUP & VARIATION			REQUEST (SCS will parse)		RESPONSE (SCS will respond)	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
1	0	Binary Input - Any variation (Variation 0 is used to request default variation)	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	-	-
1	1	Binary Input - Packed format	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
1	2	Binary Input - With flags	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
2	0	Binary Input Change Event - Any variation (Variation 0 is used to request default variation)	1 (read)	06 (all), 07, 08 (limited qty)	-	-
2	1	Binary Input Change Event - Without time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
2	2	Binary Input Change Event - With absolute time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
10	0	Binary Output Status - Any variation (Variation 0 is used to request default variation)	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	-	-
10	1	Binary Output Status - Packed format	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
10	2	Binary Output Status - Output status with flags	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
11	0	Binary Output Event - Any variation (Variation 0 is used to request default variation)	1 (read)	00, 01 (start-stop), 06 (all)	-	-
11	1	Binary Output Event - Status without time	1 (read)	00, 01 (start-stop), 06 (all)	129 (response)	17, 28 (index)
11	2	Binary Output Event - Status with time	1 (read)	00, 01 (start-stop), 06 (all)	129 (response)	17, 28 (index)

Continues on the next page

Table Appendix 2.3-1 Implementation table (Table continued)

DNP OBJECT GROUP & VARIATION			REQUEST (SCS will parse)		RESPONSE (SCS will respond)	
Object Group Number	**Variation Number**	**Description**	**Function Codes (dec)**	**Qualifier Codes (hex)**	**Function Codes (dec)**	**Qualifier Codes (hex)**
12	1	Binary Output Command - Control relay output block (CROB)	03 (select), 04 (operate), 05 (direct operate), 06 (direct op, no ack)	17, 28 (index)	129 (response)	17, 28 (index)
20	0	Counter - Any variation (Variation 0 is used to request default variation)	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	-	-
			7 (freeze), 8 (freeze no ack), 9 (freeze & clear), 10 (frz & clr, no ack)	00, 01 (start-stop), 06 (all)	-	-
20	1	Counter - 32-bit with flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
20	2	Counter - 16-bit with flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
20	5	Counter - 32-bit without flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
20	6	Counter - 16-bit without flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
21	0	Frozen Counter -Any variation (Variation 0 is used to request default variation)	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	-	-
21	1	Frozen Counter - 32-bit with flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)

Continues on the next page

Table Appendix 2.3-1 Implementation table (Table continued)

DNP OBJECT GROUP & VARIATION			REQUEST (SCS will parse)		RESPONSE (SCS will respond)	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
21	2	Frozen Counter - 16-bit with flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
21	5	Frozen Counter - 32-bit with flag and time	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
21	6	Frozen Counter - 16-bit with flag and time	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
21	9	Frozen Counter - 32-bit without flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
21	10	Frozen Counter -16-bit without flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
22	0	Counter Change Event - Any variation (Variation 0 is used to request default variation)	1 (read)	06 (all), 07, 08 (limited qty)	-	-
22	1	Counter Change Event - 32-bit with flag	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
22	2	Counter Change Event - 16-bit with flag	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
22	5	Counter Change Event -32-bit with flag and time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
22	6	Counter Change Event -16-bit with flag and time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
23	0	Frozen Counter Change Event - Any variation (Variation 0 is used to request default variation)	1 (read)	06 (all), 07, 08 (limited qty)	-	-
23	1	Frozen Counter Change Event - 32-bit with flag	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
23	2	Frozen Counter Change Event - 16-bit with flag	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)

Continues on the next page

Table Appendix 2.3-1 Implementation table (Table continued)

DNP OBJECT GROUP & VARIATION			REQUEST (SCS will parse)		RESPONSE (SCS will respond)	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
23	5	Frozen Counter Change Event - 32-bit with flag and time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
23	6	Frozen Counter Change Event - 16-bit with flag and time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
30	0	Analog Input - Any variation (Variation 0 is used to request default variation)	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	-	-
30	1	Analog Input - 32-bit with flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
30	2	Analog Input - 16-bit with flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
30	3	Analog Input - 32-bit without flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
30	4	Analog Input - 16-bit without flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
30	5	Analog Input - Single-precision, floating-point with flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
32	0	Analog Input Change Event - Any variation (Variation 0 is used to request default variation)	1 (read)	06 (all), 07, 08 (limited qty)	-	-
32	1	Analog Input Change Event - 32-bit without time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
32	2	Analog Input Change Event - 16-bit without time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
32	3	Analog Input Change Event - 32-bit with time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
32	4	Analog Input Change Event - 16-bit with time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)

Continues on the next page

Table Appendix 2.3-1 Implementation table (Table continued)

DNP OBJECT GROUP & VARIATION			REQUEST (SCS will parse)		RESPONSE (SCS will respond)	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
32	5	Analog Input Change Event - Single-precision, floating-point without time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
32	7	Analog Input Change Event - Single-precision, floating-point with time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
34	0	Analog Input Deadband - Any variation (Variation 0 is used to request default variation)	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	-	-
34	1	Analog Input Deadband - 16-bit	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
34	2	Analog Input Deadband - 32-bit	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
34	3	Analog Input Deadband - Single-precision, floating-point	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
40	0	Analog Output Status - Any variation (Variation 0 is used to request default variation)	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	-	-
40	1	Analog Output Status - 32-bit with flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
40	2	Analog Output Status - 16-bit with flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)
40	3	Analog Output Status - Single-precision, floating-point with flag	1 (read)	00, 01 (start-stop), 06 (all), 07, 08 (limited qty), 17, 28 (index)	129 (response)	00, 01 (start-stop), 17, 28 (index)

Continues on the next page

Table Appendix 2.3-1 Implementation table (Table continued)

DNP OBJECT GROUP & VARIATION			REQUEST (SCS will parse)		RESPONSE (SCS will respond)	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
41	1	Analog Output Command - 32-bit	03 (select), 04 (operate), 05 (direct operate), 06 (direct op, no ack)	17, 28 (index)	129 (response)	17, 28 (index)
41	2	Analog Output Command - 16-bit	03 (select), 04 (operate), 05 (direct operate), 06 (direct op, no ack)	17, 28 (index)	129 (response)	17, 28 (index)
41	3	Analog Output Command - Single-precision, floating-point	03 (select), 04 (operate), 05 (direct operate), 06 (direct op, no ack)	17, 28 (index)	129 (response)	17, 28 (index)
42	0	Analog Output Change Event - Any variation (Variation 0 is used to request default variation)	1 (read)	06 (all), 07, 08 (limited qty)	-	-
42	1	Analog Output Change Event - 32-bit without time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
42	2	Analog Output Change Event - 16-bit without time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
42	3	Analog Output Change Event - 32-bit with time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
42	4	Analog Output Change Event - 16-bit with time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
42	5	Analog Output Change Event - Single-precision, floating-point without time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)
42	7	Analog Output Change Event - Single-precision, floating-point with time	1 (read)	06 (all), 07, 08 (limited qty)	129 (response)	17, 28 (index)

Continues on the next page

Table Appendix 2.3-1 Implementation table (Table continued)

DNP OBJECT GROUP & VARIATION			REQUEST (SCS will parse)		RESPONSE (SCS will respond)	
Object Group Number	**Variation Number**	**Description**	**Function Codes (dec)**	**Qualifier Codes (hex)**	**Function Codes (dec)**	**Qualifier Codes (hex)**
50	1	Time and Date - Absolute time	1 (read)	07 (quantity = 1)	129 (response)	07 (quantity = 1)
			2 (write)	07 (quantity = 1)	-	-
50	3	Time and Date - Absolute time at last recorded time	2 (write)	07 (quantity = 1)	-	-
60	1	Class 0 Data	1 (read)	06 (all)	-	-
60	2	Class 1 Data	1 (read)	06 (all), 07, 08 (limited qty)	-	-
60	3	Class 2 Data	1 (read)	06 (all), 07, 08 (limited qty)	-	-
60	4	Class 3 Data	1 (read)	06 (all), 07, 08 (limited qty)	-	-
80	1	Internal Indications - Packed format	1 (read)	00, 01 (start-stop)	-	-
			2 (write)	00 index=7 (start-stop)	-	-

This Implementation Table is referred to "DNP3 SPECIFICATION, Volume 6 Part2, Objects, DNP3 OBJECT LIBRARY Version 2.04, 15-March-2009".

Revision information

Title : Engineering Guide Vol. 2

Manual No. : IM 32P01C20-01EN

Dec. 2023/10th Edition/R4.10 or later

A1	Added SYS_CPUDSP.
A6.2	Updated descriptions of SCS link transmission.
A7	Updated descriptions of inter-SCS safety communication.

Nov. 2022/9th Edition/R4.08

F1.5.2	Updated reference numbers of Modbus Address Builder.

Jan. 2022/8th Edition/R4.07

B5.1.3	Added function blocks that use the output status.
D4.17	Updated descriptions from FAST/TOOLS to CI Server.

Feb. 2021/7th Edition/R4.06

A2, A3.4.1, A3.4.3, A3.4.4, A9.1, B8.1.4, B8.1.5, B8.2.6, D4.1	Added IOM for SIL2.
A3.3, B1, B7.1.5, B7.2.1, B7.2.4, B8.1.4, D2.9, D4.7, F4	Added SCS for SIL2
A6.1, A7	Added descriptions of SIL2.
B8.1.4	Added nodes for SIL2.
B2, B8.1.6, B8.2.5	Updated description because CENTUM VP supported UACS.
C3.2	Support for Windows 10
A, D4.17, F1.5, G1, G2.2, G3.1	Updated descriptions from FAST/TOOLS to CI Server.

Dec. 2019/6th Edition/R4.05

Introduction	Updated descriptions of registered trademarks and trademarks.
B5.1.2, B5.3.1	Updated descriptions because of the change in the operation of HIS when password entry is skipped for a manual operation block.
B5.1.6, B5.3.2	Updated descriptions due to the changes made to the mapping block data item of the manual operation block.
B8.1.4	Added descriptions regarding the operation data reset switch.

Aug. 2018/5th Edition/R4.04

Introduction	Updated description of registered trademarks of YOKOGAWA.
A3.3, A3.4, A3.4.2	Added descriptions regarding the modules that are not subject to the device reset function.
C3.1.2	Updated descriptions regarding VS2017.

Oct. 2017/4th Edition/R4.03.10

Introduction	Added fire and gas communication module
A1, B1, B2, B3.1, B3.3, B7.1, B8.1.3	Added description regarding safety subsystem communication I/O FB

B7.1.3	Added the procedure for changing alarm display colors.
B7.2.4	Added precautions for when performing CENTUM integration
B8.1.4	Added number of locks for safety subsystem communication I/O
D1.3	Added descriptions of the conversion of real-type input data.
D1.4, D2.4, D3.3, D4.12, D4.14.2	Added safety communication I/O editor
E	Added description regarding safety subsystem communication
E1	Added description regarding fire and gas communication
Appendix 1	Added descriptions of information about engineering of subsystems.

May 2017/3rd Edition/R4.03

Entire manual	Changed description regarding the start menu
Introduction	Deleted Windows Vista from the explanation of trademarks
A3.3, A3.4, A3.4.1, A3.4.2, A3.4.3, A3.4.4, A3.5	Added explanations regarding the functions for fire and gas device applications
A8.5, B1, B2, B3.1, B3.3, B7.1, B8.1.3	Added explanations regarding HSDTR and GASDTR
B7.1, B8.2.6	Added an explanation of chattering alarm suppression

Oct. 2016/2nd Edition/R4.02

Entire manual	Changed the symbols that indicate warning and caution.
Introduction	Updated descriptions in "■ Safety, Protection, and Modification of the Product," "■ Symbols," and "■ Trademark Acknowledgments." Added a new term in "■ Full Names and Simplified Terms."
A	Changed configurations.
A1, A1.1, A1.2, A4, A4.6, B2, B7, B7.1.4, B7.2	Added descriptions of iDefine.
A3, A8.5, B2, B3.2, B7.1.4, B7.1.5, B7.1.6, B8	Updated descriptions of tools.
D2.9, D4.7	Updated conditions for the number of mounts.
D3.1,E2.1, E3.1	Added descriptions of the number of mounts.
F1, F1.1, F3.2.1, F3.2.2, F3.7	Added descriptions of the duplexed interface for DNP3 communication.
F2.4	Updated descriptions of time synchronization.
Appendix1.1	Added IOM Definition Editor.

Dec. 2015/1st Edition/R4.01

Newly published.

■ For Questions and More Information Online Query: A query form is available on the following URL for online query. http://www.yokogawa.com/iss
■ Written by Yokogawa Electric Corporation
■ Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Attachment 9.4 Installation Guide

IM32P01C50-01EN

User's
Manual

ProSafe-RS
ProSafe-RS Lite

Installation Guide

IM 32P01C50-01EN

YOKOGAWA
Yokogawa Electric Corporation

IM 32P01C50-01EN
11th Edition

Introduction

This manual describes the procedure for setting up ProSafe-RS.

When you integrate ProSafe-RS with FAST/TOOLS, replace "Vnet/IP" in the descriptions in this manual with "Vnet/IP-Upstream."

This manual consists of the following parts:

- Part A Overview
  This part provides an overview of ProSafe-RS setup.
- Part B: New Setup
  This part describes the procedure for a new setup of ProSafe-RS.
- Part C Maintenance
  This part describes the tasks to be done while a ProSafe-RS system is used.
- Part D Connection with Other Products
  This part describes how to connect ProSafe-RS to other YOKOGAWA products and provides cautionary notes.
- Appendix
  This section describes hardware settings and cautionary notes.

11th Edition : Dec. 2023 (YK)
All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Safety Precautions for Use

Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Be sure to confirm the specifications and required settings of the devices that are used in combination with the Product by referring to the instruction manual or other documents of the devices.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:



Indicates that caution is required. This symbol for the Product indicates the possibility of dangers such as electric shock on personnel and equipment, and also indicates that the user must refer to the User's Manuals for necessary actions. In the User's Manuals, this symbol is used together with a word "CAUTION" or "WARNING" at the locations where precautions for avoiding dangers are described.

<French> Signale qu'il faut faire preuve de prudence. Ce symbole pour le produit signale la possibilité d'un danger pour le personnel et l'équipement comme un choc électrique, et signale également que l'utilisateur doit se référer au Manuel de l'utilisateur afin de prendre les mesures nécessaires. Dans le Manuel de l'utilisateur, ce symbole est utilisé conjointement avec la mention «CAUTION» ou «WARNING» aux endroits où sont décrites les précautions pour éviter les dangers.



Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.

<French> Signale qu'il faut faire preuve de prudence avec la surface brûlante. Les appareils sur lesquels est apposé ce symbole risquent de devenir brûlants. Tout contact physique ou matériel avec ces appareils risque de provoquer des brûlures ou des dommages.



Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.



Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.

Indicates an AC supply.

Indicates a DC supply.

| Indicates that a component such as a power supply switch is turned ON.

○ Indicates that a component such as a power supply switch is turned OFF.

Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

Warning and Disclaimer

- Except as specified in the warranty terms, YOKOGAWA shall not provide any warranty for the Product.
- YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Product.

Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the Software Product's merchantability or suitability for any particular purpose, except as specified in the warranty terms.
- Purchase the appropriate number of licenses of the Software Product according to the number of computers to be used.
- No copy of the Software Product may be made for any purpose other than backup; otherwise, it is deemed as an infringement of YOKOGAWA's Intellectual Property rights.
- Keep the software medium of the Software Product in a safe place.
- No reverse engineering, reverse compiling, reverse assembling, or converting the Software Product to human-readable format may be performed for the Software Product.
- No part of the Software Product may be transferred, converted, or sublet for use by any third-party, without prior written consent from YOKOGAWA.

Documentation Conventions

Symbols

The following symbols are used in the User's Manuals.

 WARNING	Indicates precautions to avoid a danger that may lead to death or severe injury.
 CAUTION	Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.
IMPORTANT	Indicates important information required to understand operations or functions.
TIP	Indicates additional information.
	Indicates referenced content. In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

Typographical Conventions

The following typographical conventions are used throughout the User's Manuals.

Commonly Used Conventions throughout the User's Manuals

- Δ Mark
  Indicates that a space must be entered between character strings.
  Example:

  ```
  .ALΔPIC010Δ-SC
  ```

- Character string enclosed by braces { }
  Indicates character strings that may be omitted.

  Example:

  ```
  .PRΔTAG{Δ.sheet name}
  ```

Conventions Used to Show Key or Button Operations

- Characters enclosed by brackets [ ]
  When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a button name in a window, or an item in a list box displayed in a window.

  Example:

  To alter the function, press the [ESC] key.

Conventions of a User-defined Folder

- User-defined folder name enclosed by parenthesis ( )
  User definable path is written in a pair of parentheses.

  Example:

  ```
  (RS Project Folder)\SCS0101
  ```

If the RS Project Folder is `C:\MYRSPJT`, the above path becomes `C:\MYRSPJTSCS0101`.

Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.
If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

Definitions of Node and Module Terms

In the User's Manuals, nodes and modules are referred to by using collective terms, another terms, or abbreviations based on the following definitions:

- Definitions of nodes
  - Node: A node is a collective term for an FIO node and an N-IO node.
  - FIO node: This is a collective term for a safety control unit, a safety node unit, and a unit for optical ESB bus repeater module.
  - CPU node: This is another term for a safety control unit. The abbreviation of safety control unit is SCU.
  - I/O node: This is another term for a safety node unit. The abbreviation of safety node unit is SNU.
  - N-IO node: This is a collective term for a node interface unit and an N-IO I/O unit. The abbreviation of node interface unit is NIU.
- Definitions of modules
  - I/O module: This is a collective term for an FIO I/O module and an N-IO I/O module.
  - FIO I/O module: This is a collective term for an analog I/O module and a digital I/O module for FIO, and a communication module.
  - N-IO I/O module: This is a collective term for the modules that can be mounted on an N-IO I/O unit.
  - AIO/DIO module: This is a collective term for an analog I/O module, a digital I/O module, and a universal type I/O module.
  - Analog I/O module: This is a collective term for an analog input module and an analog output module.
  - Digital I/O module: This is a collective term for a digital input module and a digital output module.
  - Universal type I/O module: This is a collective term for the I/O modules for which the channel signal category can be changed by software.

- Input module: This is a collective term for an analog input module, digital input module, and a universal type I/O module with defined input channels.
- Output module: This is a collective term for an analog output module, digital output module, and a universal type I/O module with defined output channels.
- Communication module: This is a collective term for a serial communication module, an Ethernet communication module, and a fire and gas communication module.

Full Names and Simplified Terms

In the User's Manuals, simplified terms listed in the following table are used.

Table Info-1 Full Names and Simplified Terms

Full Name	Simplified Term
Automation Design Suite	AD Suite
Automation Design Organizer	AD Organizer
Automation Design Server	AD Server
Automation Design project	AD project
Automation Design Master Database	ADMDB
Automation Design Suite Administration Tool	ADS Administration Tool
iDefine for ProSafe-RS	iDefine
Modification Package	ModPack
SCSV1-S (SCS supporting the SSC10S/SSC10D safety control units)	SCSV1
SCSP1-S (SCS supporting the SSC50S/SSC50D safety control units)	SCSP1
SCSP2-S (SCS supporting the SSC60S/SSC60D safety control units)	SCSP2
SCSP3-S (SCS supporting the S2SC70S/S2SC70D safety control units)	SCSP3
SCSL2-S (SCS supporting the L1SC70S/L1SC70D safety control units)	SCSL2
SCSU1-S (SCS supporting the SSC57S/SSC57D safety control units)	SCSU1

Copyright and Trademark Notices

All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, PRM, Exaopc, FieldMate Validator, and STARDOM are registered trademarks or trademarks of Yokogawa Electric Corporation.
- The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

Installation Guide

IM 32P01C50-01EN 11th Edition

CONTENTS

PART-A Overview.....A-1
A1. How to Read This Document..... A1-1
A2. Overview of Setup Tasks.....A2-1
A2.1 Before You Set Up.....A2-2
A2.2 Procedures for New Setup..... A2-3
A2.2.1 Setup Procedure for a ProSafe-RS System.....A2-4
A2.2.2 Setup Procedure for ProSafe-RS Running on a Virtual Machine on the Virtualization Platform..... A2-7
A2.2.3 Setup Procedure for SENG.....A2-10
A2.2.4 Setup Procedure for a Computer Installed with Only AD Server..... A2-13
A2.2.5 Setup Procedure for a File Server..... A2-14
A2.2.6 Setup Procedure for a Computer Dedicated to License Management A2-15
A2.3 Explanation for Maintenance..... A2-16

Installation Guide

IM 32P01C50-01EN 11th Edition

CONTENTS

PART-B New Setup..... B-1

B1. Preparing for the Setup..... B1-1

B1.1 Items to be Determined Before the Setup..... B1-2

B1.2 Precautions for Setup..... B1-4

B1.3 Precautions for Setting Up ProSafe-RS on a Virtual Machine on the Virtualization Platform..... B1-8

B2. Setting Up the Windows Domain Environment..... B2-1

B2.1 Overview of Setting Up the Domain Environment..... B2-2

B2.2 Configuring the domain controller..... B2-5

B2.3 Configuring Security Settings for the Domain Controller..... B2-6

B2.4 Creating Domain Users..... B2-13

B2.5 Adding Computers to the Domain..... B2-17

B2.6 Setting Up Redundant Domain Controllers..... B2-19

B2.7 Setting Up Time Synchronization in Windows Domain Environment..... B2-20

B2.7.1 Implementing Time Synchronization in a System Consisting of Only ProSafe-RS..... B2-21

B2.7.2 Implementing Time Synchronization When Integrated with CENTUM..... B2-24

B3. Setup of an SENG or a Computer Installed with Only AD Server..... B3-1

B3.1 Setting Up the Hardware..... B3-2

B3.2 Setting Up Windows..... B3-7

B3.2.1 Setting of Common Windows OS Items..... B3-8

B3.2.2 Setting of Items Specific to Windows 10..... B3-10

B3.2.3 Setting of Items for Windows Server 2016, Windows Server 2019, and Windows Server 2022..... B3-14

B3.3 Configuring Network Settings..... B3-18

B3.3.1 Installing the Control Bus Driver..... B3-19

B3.3.2 Setting Up the RIP Listener Service on a Virtual Machine..... B3-21

B3.3.3 Installing the Vnet/IP Open Communication Driver..... B3-22

B3.3.4 Installing the Vnet/IP Interface Package on a Virtual Machine..... B3-24

B3.3.5 Configuring Windows Network Settings..... B3-27

B3.4 Notes on Using a Virtual Machine..... B3-37
B3.5 Installing the ProSafe-RS Software..... B3-39
B3.6 Configuring IT Security Settings..... B3-44
B3.6.1 Running the IT Security Tool..... B3-46
B3.6.2 Precautions for Coexistence with Other Product..... B3-51
B3.6.3 Running Domain Link Management Tool..... B3-52
B3.7 Distributing and Accepting Licenses..... B3-55
B3.8 Creating User Accounts..... B3-56
B3.8.1 When the Standard Model with Standalone Management Security Settings are Applied..... B3-57
B3.8.2 When the Legacy Model of Security Settings are Applied..... B3-58
B3.9 Configuring Windows Environment Settings for Each User..... B3-59
B3.9.1 Setting of Items Common to Windows 10, Windows Server 2016, Windows Server 2019, and Windows Server 2022..... B3-60
B3.9.2 Setting of Items Specific to Windows 10..... B3-63
B3.10 Configuring the Uninterruptible Power Supply (UPS) Service..... B3-65
B4. Configuring the Functions Specific to SENG..... B4-1
B4.1 Setting the Manual Browsing Environment..... B4-2
B4.2 Settings of Project Database Folder..... B4-3
B4.3 Settings for Message Cache Tool..... B4-4
B4.4 Settings Required to Use the Forced I/O Viewer Function..... B4-5
B4.5 Settings Required for OPC Communication..... B4-6
B4.6 Setup when Using the Access Control and Operation History Management Package..... B4-8
B4.6.1 Setup Procedure when Using Access Control and Operation History Management Functions..... B4-10
B4.6.2 Security Settings for the Operation History Database..... B4-11
B5. Setting Up a File Server..... B5-1
B5.1 Setting Up a Computer that Serves Only as a File Server..... B5-2
B5.2 Setting Up the File Server Function on an SENG or a Computer Installed with Only AD Server..... B5-12
B5.3 Setting Up the Computer that Serves as Both File Server and License Management Station..... B5-14
B6. Setting Up the Computer Dedicated to License Management..... B6-1
B7. Configuring the Hardware of SCS and Devices for Connection between Domains..... B7-1
B8. Installing the Functions that Operate with CENTUM VP Licenses..... B8-1

Installation Guide

IM 32P01C50-01EN 11th Edition

CONTENTS

PART-C Maintenance C-1

C1. Adding Licenses and Changing License Assignments C1-1

C1.1 Adding a License C1-2

C1.2 Changing License Assignments C1-3

C2. Setting Up the Windows Domain Environment Later C2-1

C3. Backing Up the System C3-1

C3.1 Backing Up the Entire Windows C3-2

C3.2 Backing Up the ProSafe-RS Engineering Data C3-3

C4. Upgrading the ProSafe-RS Software C4-1

C4.1 Installation for Upgrading C4-2

C4.1.1 Upgrading the Version of ProSafe-RS Software C4-5

C4.1.2 Upgrading the Revision of ProSafe-RS Software C4-9

C4.2 Settings after Upgrading ProSafe-RS Software C4-14

C4.2.1 Updating the engineering data after an upgrade C4-15

C4.2.2 Upgrading an SCS project C4-18

C4.2.3 Cautionary notes for upgrading to R4.10 ..... C4-19

C4.2.4 Procedures for using new functions C4-22

C4.3 Upgrading the Computer Dedicated to License Management C4-26

C5. Uninstalling the ProSafe-RS Software C5-1

C5.1 Uninstallation on SENG C5-2

C5.1.1 Uninstalling the ProSafe-RS Software C5-3

C5.1.2 Uninstalling the Network Drivers C5-5

C5.2 Uninstallation on the computer Dedicated to License Management C5-10

C6. Reinstalling the ProSafe-RS Software C6-1

C6.1 When the Computer Used is the Same C6-2

C6.2 When the Computer Used is Not the Same C6-6

C7. Troubleshooting C7-1

C7.1 Windows Related Troubleshooting C7-2

C7.2 Troubleshooting Related to Network C7-4

C7.2.1 Precaution on Network Cable Connection C7-5

C7.2.2 Problems Related to Installation and Deletion of Drivers C7-6

Installation Guide

IM 32P01C50-01EN 11th Edition

CONTENTS

PART-D Connection with Other Products..... D-1

D1. Connecting YOKOGAWA products..... D1-1

D1.1 CENTUM VP and ProSafe-RS..... D1-3

D1.1.1 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS Safety System Engineering and Maintenance Function..... D1-4

D1.1.2 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS SOE Viewer Package..... D1-6

D1.1.3 CENTUM VP SOE Viewer Package and ProSafe-RS Safety System Engineering and Maintenance Function..... D1-7

D1.1.4 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS SOE OPC Interface Package..... D1-8

D1.1.5 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS Forced I/O Viewer Package..... D1-12

D1.1.6 CENTUM VP System Builder Function and ProSafe-RS CENTUM VP Integration Package..... D1-13

D1.1.7 CENTUM VP System Builder Function and ProSafe-RS Safety System Engineering and Maintenance Function..... D1-14

D1.1.8 CENTUM VP Engineering Server Function and ProSafe-RS Safety System Engineering and Maintenance Function..... D1-15

D1.1.9 CENTUM VP System Builder Function and ProSafe-RS Engineering Server Function..... D1-16

D1.2 ProSafe-RS and iDefine..... D1-17

D1.2.1 ProSafe-RS Safety System Engineering and Maintenance Function and iDefine for ProSafe-RS..... D1-18

D1.2.2 ProSafe-RS functions other than Safety System Engineering and Maintenance Function and iDefine for ProSafe-RS..... D1-20

D1.3 ProSafe-RS and PRM..... D1-22

D1.3.1 ProSafe-RS SOE OPC Interface Package and PRM Server..... D1-23

D1.3.2 PRM Client and Forced I/O Viewer Package..... D1-25

D1.4 ProSafe-RS and Exaquantum..... D1-26

D1.4.1 ProSafe-RS SOE OPC Interface Package and Exaquantum PIMS Server..... D1-27

Installation Guide

IM 32P01C50-01EN 11th Edition

CONTENTS

Appendix

Appendix 1. Setting Switches..... App.1-1
Appendix 2. Procedure for Erasing VI702 Internal Settings.....App.2-1
Appendix 3. Vnet/IP Interface Management Tool..... App.3-1
Appendix 4. Antistatic Precautions When Handling Hardware..... App.4-1
Appendix 5. Customization at Installation of Windows 10.....App.5-1
Appendix 6. Compatibility between Revisions and Cautionary Notes for Upgrading..... App.6-1
Appendix 6.1 Cautionary Notes for Upgrading to R4.01.....App.6-2
Appendix 6.2 Cautionary Notes for Upgrading to R4.02.....App.6-4
Appendix 6.3 Cautionary Notes for Upgrading to R4.03.....App.6-10
Appendix 6.4 Cautionary Notes for a Revision Upgrade to R4.03.10.....App.6-13
Appendix 6.5 Cautionary Notes for Revision Upgrade to R4.04.....App.6-15
Appendix 6.6 Cautionary Notes for Revision Upgrade to R4.05.....App.6-17
Appendix 6.7 Cautionary notes for upgrading to R4.06..... App.6-21
Appendix 6.8 Cautionary notes for upgrading to R4.07..... App.6-24
Appendix 6.9 Cautionary notes for upgrading to R4.08..... App.6-26
Appendix 6.10 Cautionary notes for upgrading to R4.09..... App.6-28

A. Overview

This section explains how to read this document, types of ProSafe-RS setup tasks and their workflows.

A1. How to Read This Document

This document explains the setup procedures for the ProSafe-RS software. This document does not touch upon installation procedures of Windows OS, related service packs, and Microsoft security patches. Also, this document does not touch upon the procedure for installing iDefine and how to configure the security settings on the computer on which iDefine is to be installed.

To use the software packages installed on an SENG, licenses must be distributed to and activated on the SENG by using a program called License Manager. Procedures for the tasks performed using License Manager are described in the License Management IM. You are guided to refer to the License Management IM as necessary in the explanation of setup procedures.

You are also guided to refer to the Security Guide IM for information about functions that reinforce security of the system.

SEE ALSO

For more information about the procedure for installing the Windows operating systems, related service packs and the Microsoft security patches, refer to:

the information provided by Microsoft

For more information about Microsoft security patches, refer to:

Microsoft Security Update Policy (TI 33Y01B30-02E)

For more information about the procedure for distributing and activating the licenses on the stations, refer to:

1., “Overview of license management” in License Management Guide (IM 32P01C60-01EN)

For more information about system security, refer to:

1., “Overview” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

For more information about the procedure for installing iDefine, refer to:

iDefine Installation Guide (PR03076-MAN-991_01)

For more information about how to configure the security settings on the computer on which iDefine is to be installed, refer to:

iDefine Security Manual (PR03076-MAN-981_01)

Structure of This Document

This document consists of the following parts:

- Part A Overview

  This part describes how to read this document, various types of ProSafe-RS setup tasks along with their workflows are explained.

- Part B New Setup

  This part explains the procedures for setting up each station.

- Part C Maintenance

  This part describes maintenance tasks that are required after the stations have been set up and went into operation.

- Part D Connection with Other Products

  This part describes the required settings when connecting ProSafe-RS with other YOKOGAWA products, such as CENTUM VP, PRM, and Exaquantum.

A2. Overview of Setup Tasks

This section describes the workflows of setup tasks and provides the information you should understand before you set up individual stations.

SEE ALSO For more information about the operating environment of ProSafe-RS, refer to:

A1., “Requirements” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

A2.1 Before You Set Up

This section describes the relationship between installation and licensing of ProSafe-RS software.

Installation and Licensing of Software Packages

In order to use ProSafe-RS software packages, it is necessary to install the ProSafe-RS software on a computer and then grant licenses to the computer to enable the use of the software packages.

The tasks of installing the software packages on each computer are performed using a program called an installer. The tasks of giving licenses are executed using software called License Manager. License Manager is automatically installed when the ProSafe-RS software is installed on a computer.

Among computers installed with License Manager, the computer that is given the role of managing licenses of each computer in the system is called the license management station. The license management station distributes licenses to each computer on which the software packages are installed. On a computer to which licenses have been distributed, the software packages can be made available for use by accepting the distributed licenses.

TIP

- It is possible to install only License Manager on a computer and use it as the computer dedicated to license management.
- License management for iDefine is based on a hardware key. It is not controlled by License Manager.

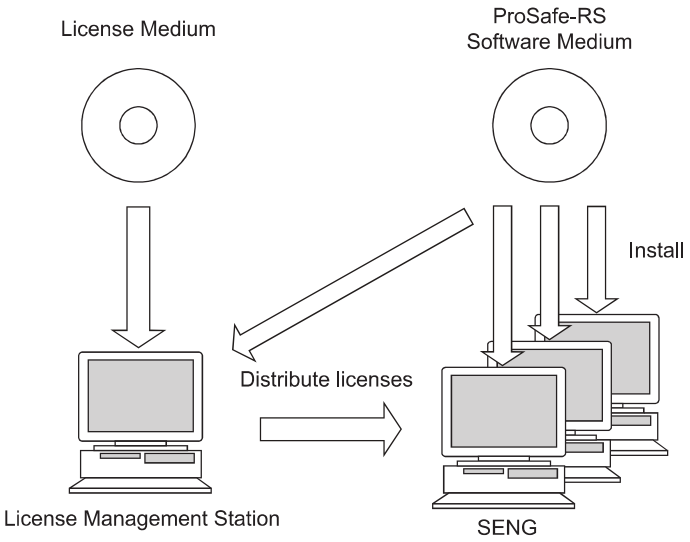


Figure A2.1-1 License Distribution

SEE ALSO

For more information about the details of licenses, refer to:

1., “Overview of license management” in License Management Guide (IM 32P01C60-01EN)

For more information about license management for iDefine, refer to:

License User Guide (PR03076-MAN-971_02)

A2.2 Procedures for New Setup

This section describes the overall procedures for setting up a ProSafe-RS system and for setting up each type of station or computer using flowcharts. As ProSafe-RS system setup procedures, it also describes the procedure for setting up a ProSafe-RS system that runs on a virtual machine on the virtualization platform.

The procedures for the following types of stations and computers are described.

- Safety engineering PC (SENG)
- Computer installed with only Automation Design Server (AD Server)
- File server
- Computer dedicated to license management

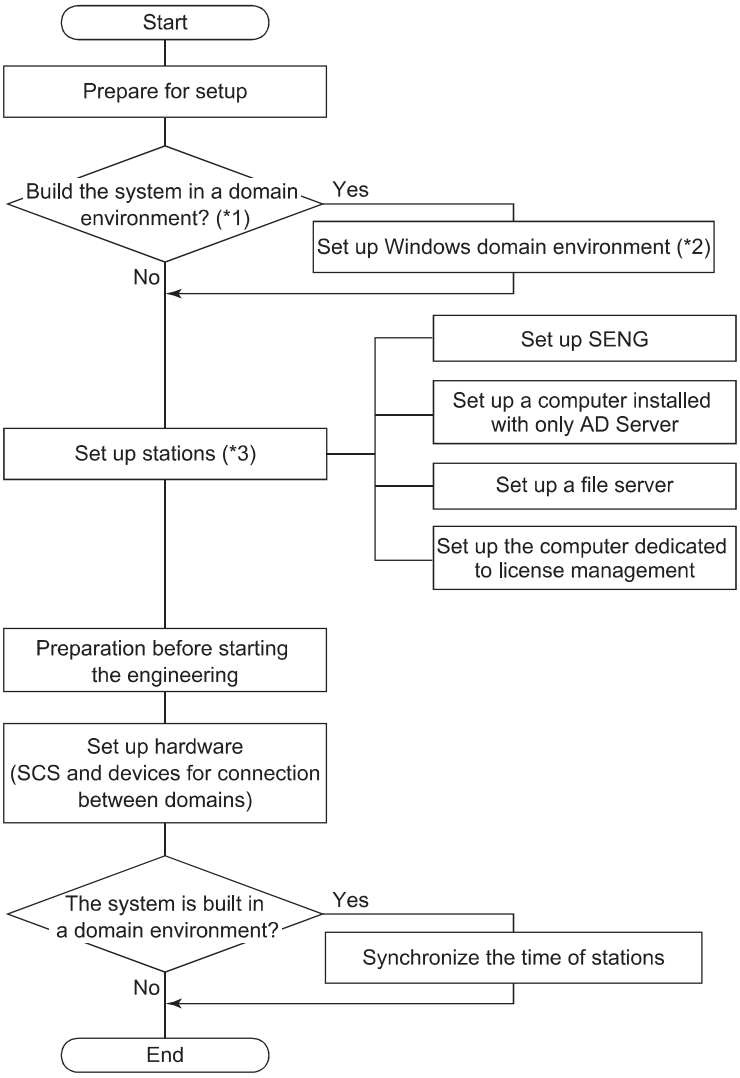
A computer installed with only AD Server, file server, and computer dedicated to license management should be provided in the system as necessary.

SEE ALSO For more information about the virtualization platform, refer to:

A., “Overview” in Virtualization Platform Setup (IM 30A05B20-01EN)

A2.2.1 Setup Procedure for a ProSafe-RS System

The following figure shows the overall procedure for setting up a ProSafe-RS system.



*1: You may set up the domain environment at a later stage.
*2: If linked domain management is selected for the user management type of IT security settings, do not add the client computer to the domain before you set up the station.
*3: Start by setting up the station that is to be used as the license management station.

Figure A2.2.1-1 Setup Procedure for a ProSafe-RS System

You can jump to the explanation of each task that appears in the flowchart from the reference link that is provided in the following subsections.

Prepare for Setup

Determine the required items such as station number for setting up a ProSafe-RS system.

SEE ALSO For more information about the items that must be determined before setting up a ProSafe-RS system, refer to:

B1., “Preparing for the Setup” on page B1-1

Set Up the Windows Domain Environment

When using ProSafe-RS in a Windows domain environment, set up the Windows domain environment. You may also set up the Windows domain environment at a later stage.

SEE ALSO For more information about setting up a Windows domain environment, refer to:

B2., “Setting Up the Windows Domain Environment” on page B2-1

Set Up Each Station

Set up SENG, file server, and other stations to be used in the ProSafe-RS system.

In a ProSafe-RS system, you must first set up the license management station, which is used to grant licenses for software packages. The license management station can be set up on an SENG or a computer dedicated to license management.

Software packages installed on other stations become available for use once the stations accept the licenses distributed from the license management station.

SEE ALSO For more information about the procedure for setting up an SENG, refer to:

A2.2.3, “Setup Procedure for SENG” on page A2-10

For more information about the procedure for setting up a computer installed with only AD Server, refer to:

A2.2.4, “Setup Procedure for a Computer Installed with Only AD Server” on page A2-13

For more information about the procedure for setting up a file server, refer to:

A2.2.5, “Setup Procedure for a File Server” on page A2-14

For more information about the procedure for setting up a computer dedicated to license management, refer to:

A2.2.6, “Setup Procedure for a Computer Dedicated to License Management” on page A2-15

Preparation for starting engineering

The following tasks are required as the preparation for starting engineering.

- Creating an Automation Design project (AD project)
- Creating an RS project
- Registering the RS project in the AD project

SEE ALSO For more information about preparation for starting engineering, refer to:

C1., “AD Server administration functions” in Engineer's Reference Manual (IM 32P04B10-01EN)

Set Up the Hardware of SCS and Devices Used for Connection between Domains

Set up the hardware of SCS and devices used for connection between domains.

SEE ALSO For more information about setting up the hardware of SCS and devices for connection between domains, refer to:

B7., “Configuring the Hardware of SCS and Devices for Connection between Domains” on page B7-1

Set Up Time Synchronization in Windows Domain Environment

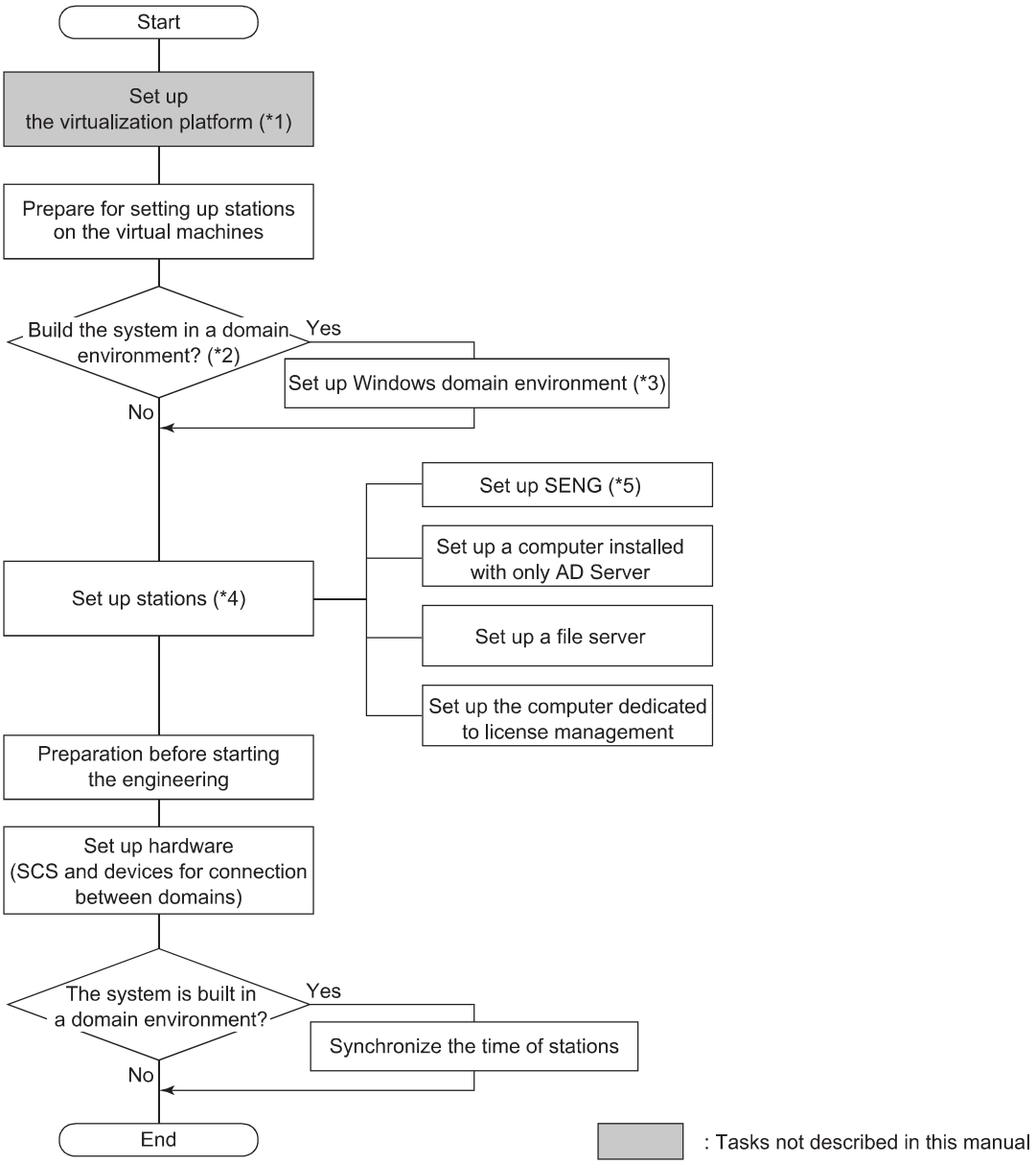
When using ProSafe-RS in a Windows domain environment, synchronize the time on the domain controller with the time on computers used in the ProSafe-RS system.

SEE ALSO For more information about setting up time synchronization in a Windows domain environment, refer to:

B2.7, “Setting Up Time Synchronization in Windows Domain Environment” on page B2-20

A2.2.2 Setup Procedure for ProSafe-RS Running on a Virtual Machine on the Virtualization Platform

The following figure shows the overall procedure for setting up a ProSafe-RS system running on a virtual machine on the virtualization platform.



*1: Prepare a computer for virtualization host, and install the virtualization platform.
*2: You may set up the domain environment at a later stage.
*3: If linked domain management is selected for the user management type of IT security settings, do not add the client computer to the domain before you set up the station.
*4: Start by setting up the station that is to be used as the license management station.
*5: You do not need to set up a Vnet/IP interface card. Install the Vnet/IP Interface Package.

Figure A2.2.2-1 Setup Procedure for a ProSafe-RS System Running on the Virtualization Platform

You can jump to the explanation of each task that appears in the flowchart from the reference link that is provided in the following subsections.

Setup for a Virtualization Platform

Before setting up ProSafe-RS, prepare the virtualization host computer and set up the virtualization platform.

SEE ALSO For more information about the setup procedure for a virtualization platform, refer to:

B., “Working with virtualization host computer” in Virtualization Platform Setup (IM 30A05B20-01EN)

Preparing to Set Up Stations that Run on Virtual Machines

Decide on the required information, such as station numbers, for setting up a ProSafe-RS system.

When installing software on a virtual machine, you must create an ISO format file of the contents of the software medium to be installed and mount it.

SEE ALSO For more information about the items that must be determined before setting up a ProSafe-RS system, refer to:

B1., “Preparing for the Setup” on page B1-1

For more information about the procedure and precautions when setting up ProSafe-RS that runs on the virtualization platform, refer to:

B1.3, “Precautions for Setting Up ProSafe-RS on a Virtual Machine on the Virtualization Platform” on page B1-8

Set Up the Windows Domain Environment

You can use a computer in the existing physical environment as the domain controller, or you can build the domain controller on the virtual machine.

You may also set up the Windows domain environment at a later stage.

SEE ALSO For more information about the procedure for setting up a domain controller on a physical computer, refer to:

B2., “Setting Up the Windows Domain Environment” on page B2-1

For more information about the domain controller on the virtualization platform, refer to:

- “■ Domain controller” in A1.3, “Other devices” in Virtualization Platform Setup (IM 30A05B20-01EN)
- “■ Domain controller” in A3.3, “Other devices” in Virtualization Platform Setup (IM 30A05B20-01EN)

Set Up Each Station

Set up SENG, file server, and other stations to be used in the ProSafe-RS system.

In a ProSafe-RS system, you must first set up the license management station, which is used to grant licenses for software packages. The license management station can be set up on an SENG or a computer dedicated to license management.

Software packages installed on other stations become available for use once the stations accept the licenses distributed from the license management station.

You can use a computer in the existing physical environment as the license management station, or you can build the license management station on the virtual machine.

SEE ALSO For more information about the procedure for setting up an SENG, refer to:

A2.2.3, “Setup Procedure for SENG” on page A2-10

For more information about the procedure for setting up a computer installed with only AD Server, refer to:

A2.2.4, “Setup Procedure for a Computer Installed with Only AD Server” on page A2-13

For more information about the procedure for setting up a file server, refer to:

A2.2.5, “Setup Procedure for a File Server” on page A2-14

For more information about the procedure for setting up a computer dedicated to license management, refer to:

A2.2.6, “Setup Procedure for a Computer Dedicated to License Management” on page A2-15

Preparation for Starting Engineering

The following tasks are required as the preparation for starting engineering.

- Creating an Automation Design project (AD project)
- Creating an RS project
- Registering the RS project in the AD project

SEE ALSO For more information about preparation for starting engineering, refer to:

C1., “AD Server administration functions” in Engineer's Reference Manual (IM 32P04B10-01EN)

Set Up the Hardware of SCS and Devices Used for Connection between Domains

Set up the hardware of SCS and devices used for connection between domains.

SEE ALSO For more information about setting up the hardware of SCS and devices for connection between domains, refer to:

B7., “Configuring the Hardware of SCS and Devices for Connection between Domains” on page B7-1

Set Up Time Synchronization in a Windows Domain Environment

When using ProSafe-RS in a Windows domain environment, synchronize the time on the domain controller with the time on computers used in the ProSafe-RS system.

On the virtualization platform, you must synchronize the time of the entire virtualization platform using the SNTP server.

Do not use the host OS or virtual machine of the virtualization host computer as the top level SNTP server for time synchronization. Also, do not use the domain controller as the SNTP server.

SEE ALSO For more information about setting up time synchronization in a Windows domain environment, refer to:

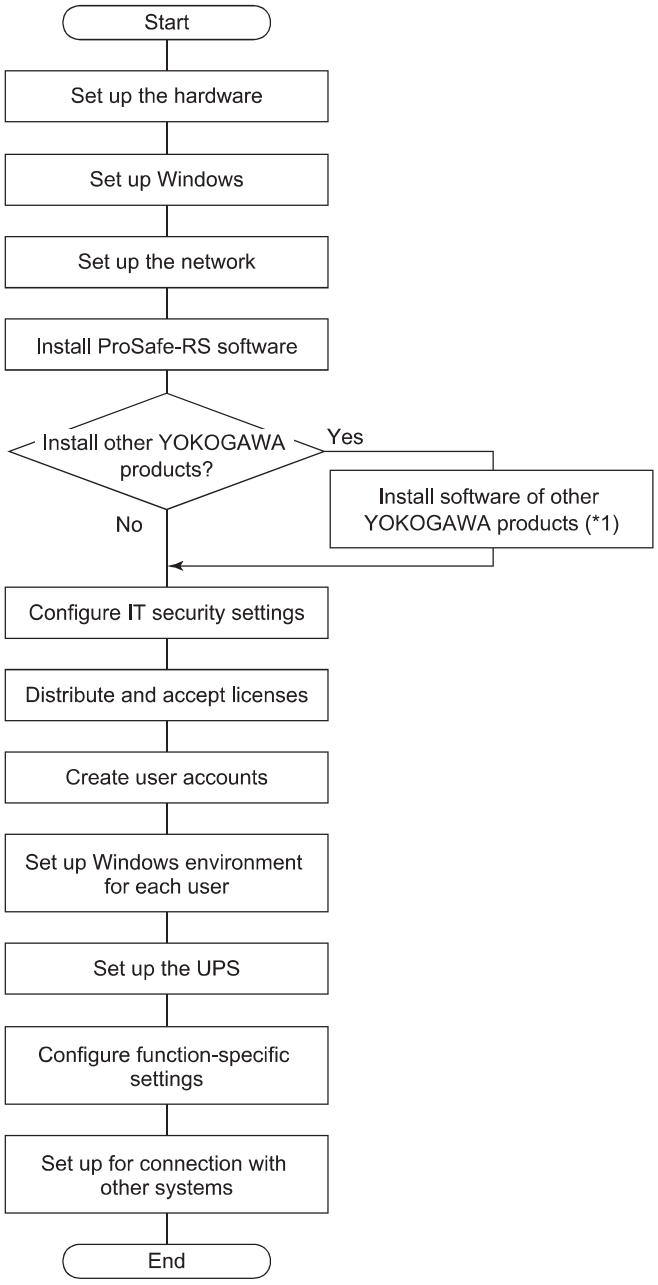
B2.7, “Setting Up Time Synchronization in Windows Domain Environment” on page B2-20

For more information about the virtualization platform time synchronization, refer to:

“■ SNTP server” in A1.3, “Other devices” in Virtualization Platform Setup (IM 30A05B20-01EN)

A2.2.3 Setup Procedure for SENG

The following figure shows the setup procedure for SENG.



*1: You may install other products later. If you install later, you need to configure IT security settings again.

Figure A2.2.3-1 Setup Procedure for SENG

You can jump to the explanation of each task that appears in the flowchart from the reference link that is provided in the following subsections.

Set Up the Hardware

Set up the Vnet/IP interface card to be installed in the SENG.

In the case of SENG that runs on a virtual machine, there is no interface card setting because it does not use the Vnet/IP interface card.

SEE ALSO For more information about setting up the hardware of SENG, refer to:

B3.1, “Setting Up the Hardware” on page B3-2

Set Up Windows

Configure Windows settings on the computer.

SEE ALSO For more information about setting up Windows, refer to:

B3.2, “Setting Up Windows” on page B3-7

Set Up the Network

Configure the network settings.

In the case of SENG that runs on a virtual machine, after installing the Vnet/IP Interface Package, you need to configure the network settings.

SEE ALSO For more information about configuring network settings, refer to:

B3.3, “Configuring Network Settings” on page B3-18

Install the ProSafe-RS Software

Install the ProSafe-RS software.

SEE ALSO For more information about installing the ProSafe-RS software, refer to:

B3.5, “Installing the ProSafe-RS Software” on page B3-39

Configure IT Security Settings

Configure IT security settings.

SEE ALSO For more information about configuring IT security settings, refer to:

B3.6, “Configuring IT Security Settings” on page B3-44

Distribute and Accept Licenses

Distribute licenses to the SENG from the license management station, and accept the licenses on the SENG.

SEE ALSO For more information about distributing and accepting licenses, refer to:

B3.7, “Distributing and Accepting Licenses” on page B3-55

Create User Accounts

Create user accounts.

SEE ALSO For more information about creating user accounts, refer to:

B3.8, “Creating User Accounts” on page B3-56

Configure Windows Environment Settings for Each User

Configure Windows environment settings for each user.

SEE ALSO For more information about configuring Windows environment settings for each user, refer to:

B3.9, “Configuring Windows Environment Settings for Each User” on page B3-59

Set Up the Uninterruptible Power Source (UPS) Service

If necessary, set up the uninterruptible power source (UPS) service.

SEE ALSO For more information about configuring the UPS service, refer to:

B3.10, “Configuring the Uninterruptible Power Supply (UPS) Service” on page B3-65

Configure Function-Specific Settings

Configure the settings specific to certain functions of the SENG.

SEE ALSO For more information about configuring the settings specific to each function of SENG, refer to:

B4., “Configuring the Functions Specific to SENG” on page B4-1

Set Up for Connection with Other Systems

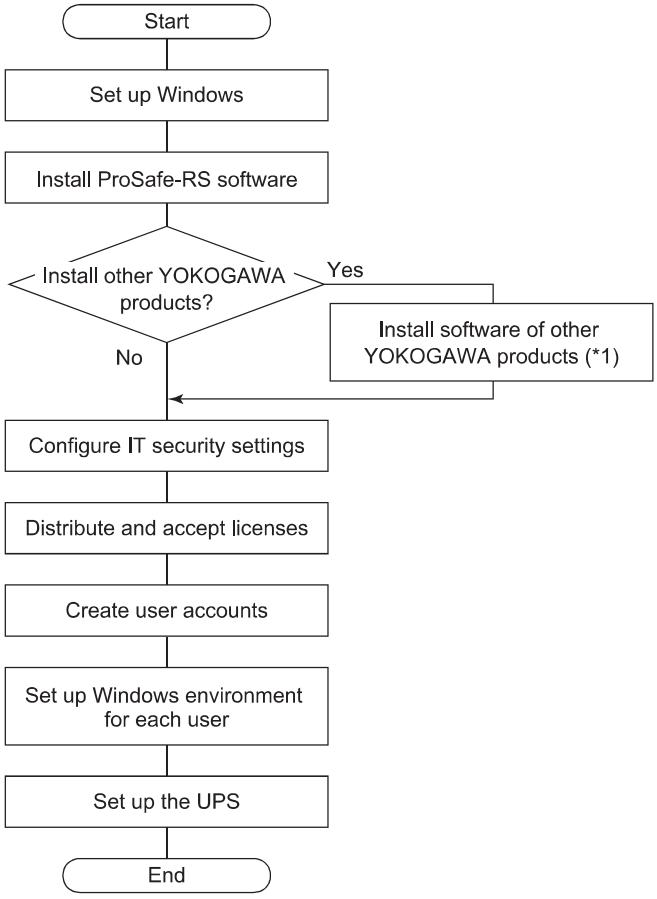
As necessary, set up for connection with other YOKOGAWA products.

SEE ALSO For more information about the settings required to connect with other YOKOGAWA products, refer to:

D1., “Connecting YOKOGAWA products” on page D1-1

A2.2.4 Setup Procedure for a Computer Installed with Only AD Server

The following figure shows the setup procedure for a computer installed with only AD server.



*1: You may install other products later. If you install later, you need to configure IT security settings again.

Figure A2.2.4-1 Setup Procedure for a Computer Installed with Only AD Server

SEE ALSO

For more information about setting up Windows, refer to:

B3.2, “Setting Up Windows” on page B3-7

For more information about installing the ProSafe-RS software, refer to:

B3.5, “Installing the ProSafe-RS Software” on page B3-39

For more information about configuring IT security settings, refer to:

B3.6, “Configuring IT Security Settings” on page B3-44

For more information about distributing and accepting licenses, refer to:

B3.7, “Distributing and Accepting Licenses” on page B3-55

For more information about creating user accounts, refer to:

B3.8, “Creating User Accounts” on page B3-56

For more information about configuring Windows environment settings for each user, refer to:

B3.9, “Configuring Windows Environment Settings for Each User” on page B3-59

For more information about configuring the UPS service, refer to:

B3.10, “Configuring the Uninterruptible Power Supply (UPS) Service” on page B3-65

A2.2.5 Setup Procedure for a File Server

You can provide a file server in the system if centralized management is required for project databases. The following figure shows the setup procedure for a file server.

TIP This flowchart illustrates the procedure for setting up a computer that serves only as a file server.

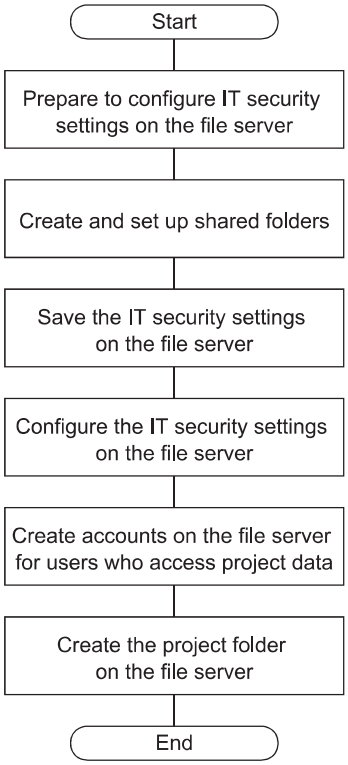


Figure A2.2.5-1 Setup Procedure for a File Server

SEE ALSO For more information about setting up a computer that serves only as a file server, refer to:

B5.1, “Setting Up a Computer that Serves Only as a File Server” on page B5-2

For more information about the procedure to set up a computer as both a file server and a license management station, refer to:

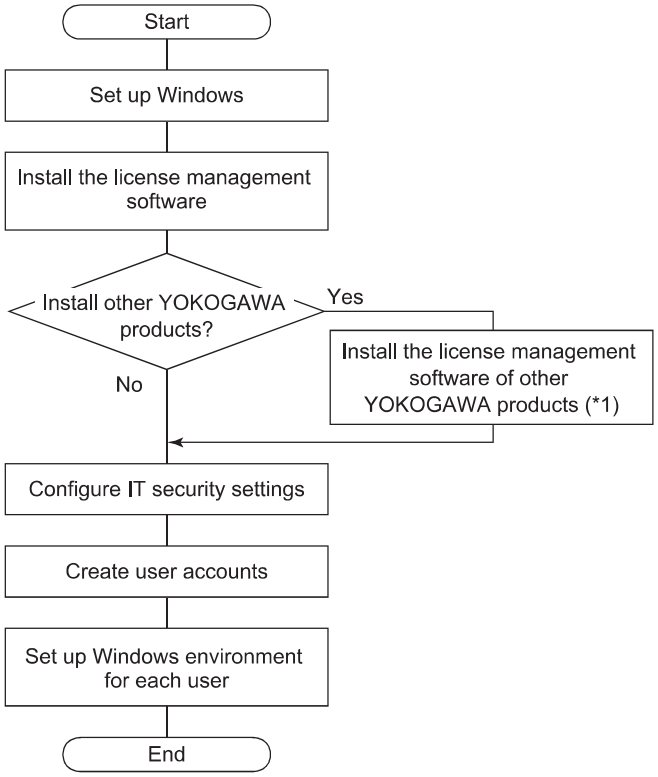
B5.3, “Setting Up the Computer that Serves as Both File Server and License Management Station” on page B5-14

For more information about setting up the file server function on SENG, refer to:

B5.2, “Setting Up the File Server Function on an SENG or a Computer Installed with Only AD Server” on page B5-12

A2.2.6 Setup Procedure for a Computer Dedicated to License Management

You can provide a computer dedicated to license management according to the scale and operation policy of the system. The following figure shows the setup procedure for a computer dedicated to license management.



*1: You may install other products later. If you install later, you need to configure IT security settings again.

Figure A2.2.6-1 Setup Procedure for a Computer Dedicated to License Management

SEE ALSO For more information about setting up a computer dedicated to license management, refer to:

B6., “Setting Up the Computer Dedicated to License Management” on page B6-1

A2.3 Explanation for Maintenance

When you perform the following maintenance tasks, refer to Part C.

- Add licenses and change license assignments
- Set up the domain environment later
- Back up the system
- Upgrade the ProSafe-RS software
- Find out cautionary notes for upgrading and compatibility with the previous revision
- Uninstall the ProSafe-RS software
- Reinstall the ProSafe-RS software
- Troubleshooting

B. New Setup

This section describes the procedure for setting up the devices such as the SENG, file server, computer dedicated to license management.

B1. Preparing for the Setup

This section explains the items that must be determined before you start setting up a station and precautions for the setup.

B1.1 Items to be Determined Before the Setup

This section lists the items that need to be determined before you start the setup tasks.

Domain Number/Station Number

A domain number is a number assigned to a group of stations connected on a control bus network. Set a domain number from 1 to 31 (1 to 16 when integrating with CENTUM).

A station number is a number assigned to each station. In each domain, station numbers should be set within a range from 1 to 64.

Computer Name/Station Name

A computer name is a name used to identify each computer on the Windows network. You can set the computer name from Windows Control Panel.

A station name is a unique name that is assigned based on the control bus address in the ProSafe-RS system.

Examples: HISddss (HIS/SENG)

STNddss (SENG)

(ddss: “dd” is the domain number and “ss” is the station number.)

It is recommended to match the computer name and the station name of a station.

IP Address

Determine the IP addresses of stations for control bus and Ethernet.

When using Vnet/IP without installing Ethernet, also determine the IP addresses for Vnet/IP open communication.

Subnet Mask

Determine the subnet masks of stations for control bus and Ethernet.

When using Vnet/IP without installing Ethernet, also determine the subnet masks for Vnet/IP open communication.

SEE ALSO For more information about IP addresses and subnet mask for control bus, refer to:

“● Setting IP Address for Vnet” on page B3-33

For more information about IP addresses and subnet mask for VnetIPOpen, refer to:

“● IP Address for VnetIPOpen” on page B3-33

For more information about IP addresses and subnet mask for Ethernet, refer to:

“● Setting IP Address for Ethernet” on page B3-33

Administrative User's Account and Password

Determine the name and password for the administrative user account of the computer.

If the system is used in a domain environment, determine the name and password for the administrative user of the domain.

Security Model and User Management Type

Determine the security model and user management type.

IMPORTANT

- Be sure to determine the policies for security settings of the entire system before you start the setup tasks because some of the setup procedures vary depending on the security model and user management type.
- If you select the Legacy model, restrictions related to Windows are in effect in some environments. For that reason, we recommend you select the Standard model.

SEE ALSO For more information about IT security, refer to:

1., “Overview” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

License Assignment

Determine the license assignments for the computers you are going to set up.

IMPORTANT

In a ProSafe-RS system, you need to decide on one computer to be used as the license management station. The license management station can be set up on a computer where SENG runs.

When setting up each station, you must set up the license management station first. Then, set up the computers that will be used as license-assigned stations. The software packages installed on each license-assigned station become available for use after you distribute the licenses from the license management station and accept them.

If an independent license management station is desired, you can also set it up as the computer dedicated to license management.

SEE ALSO For more information about licenses, refer to:

1., “Overview of license management” in License Management Guide (IM 32P01C60-01EN)

B1.2 Precautions for Setup

Take note of the following precautions before you start the setup.

In this manual, whenever Windows 10, Windows Server 2019, or Windows Server 2022 is mentioned in the explanations hereafter, the IoT versions are also included.

Changes in Windows Settings

Installing the ProSafe-RS software changes the following Windows settings.

Table B1.2-1 Changes in Windows Settings

Items	Setting	Purpose
Account name display in logon screen	Disable	To protect logon account names from unauthorized use.
Fast user switching	Disable	Simultaneous logon of multiple users is not supported.

When the System Contains Different Revisions

- The SENGs in the same RS project should have the software of the same release number.
- The SCS system program release number of SCSs in a system should basically be the same, but mixture of different release numbers is allowed. However, release numbers of SCSs communicating with each other by Inter-SCS safety communication must be in accordance with the explanation in this manual.

SEE ALSO For more information about compatibility in inter-SCS safety communication between different revisions, refer to:

- "● Important issues to consider" in "■ Precaution for engineering" in A7., "Inter-SCS safety communication" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)
- Appendix 6., "Compatibility between Revisions and Cautionary Notes for Upgrading" on page App.6-1
- Appendix 4.2, "Inter-SCS safety communication in a V net domain" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)
- C5., "Upgrading to R3.02.20" and Appendix 4., "Compatibility between Revisions and Cautionary Notes for Upgrading" in Installation for ProSafe-RS R3 (IM 32Q01C50-31E)

When a User Account Control Dialog Box Appears

During installation, a user account control dialog box may be displayed on certain circumstances.

If displayed, click [Yes] or [Continue] (for uninstallation, [Yes] or [Allow]) to continue.

Downloading the Windows Update Programs (Windows 10 Enterprise LTSC 2021)

Download and apply the following Windows update programs. If not applied, it may not be possible to connect to the shared folders of the computer from another computer by specifying the IP address.

If you have applied the Windows update programs to the SOE OPC server computer, be sure to apply the Windows update programs to the OPC client computers as well. If not applied, the OPC clients may not be able to connect to the SOE OPC server.

- 2023-06 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5027215)

TIP

This information is current as of June 2023. The latest information is provided as Endpoint Security Service. For information about the Endpoint Security Service, contact YOKOGAWA.

Downloading the Windows Update Programs (Windows 10 Enterprise LTSC 2019)

Download and apply the following Windows update programs. If not applied, access permissions for some ProSafe-RS installation folders may not be set properly, or it may not be possible to connect to the shared folders of the computer from another computer by specifying the IP address.

If you have applied the Windows update programs to the SOE OPC server computer, be sure to apply the Windows update programs to the OPC client computers as well. If you do not apply these updates, the OPC clients may not be able to connect to the SOE OPC server.

- 2021-08 Servicing Stack Update for Windows 10 Version 1809 for x64-based Systems (KB5005112)
- 2023-05 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5026362)

TIP

This information is current as of June 2023. The latest information is provided as Endpoint Security Service. For information about the Endpoint Security Service, contact YOKOGAWA.

Downloading the Windows Update Programs (Windows 10 Enterprise 2016 LTSB)

Download and apply the following Windows update programs.

If you have applied the Windows update programs to the SOE OPC server computer, be sure to apply the Windows update programs to the OPC client computers as well. If you do not apply these updates, the OPC clients may not be able to connect to the SOE OPC server.

- 2023-03 Servicing Stack Update for Windows 10 Version 1607 for x64-based Systems (KB5023788)
- 2023-05 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB5026363)

TIP

This information is current as of June 2023. The latest information is provided as Endpoint Security Service. For information about the Endpoint Security Service, contact YOKOGAWA.

Downloading the Windows Update Programs (Windows Server 2022)

Download and apply the following Windows update programs. If not applied, it may not be possible to connect to the shared folders of the computer from another computer by specifying the IP address.

If you have applied the Windows update programs to the SOE OPC server computer, be sure to apply the Windows update programs to the OPC client computers as well. If not applied, the OPC clients may not be able to connect to the SOE OPC server.

- 2023-06 Cumulative Update for Microsoft server operating system Version 21H2 for x64-based Systems (KB5027225)

TIP

This information is current as of June 2023. The latest information is provided as Endpoint Security Service. For information about the Endpoint Security Service, contact YOKOGAWA.

Downloading the Windows Update Programs (Windows Server 2019)

Download and apply the following Windows update programs. If not applied, access permissions for some ProSafe-RS installation folders may not be set properly, or it may not be possible to connect to the shared folders of the computer from another computer by specifying the IP address.

If you have applied the Windows update programs to the SOE OPC server computer, be sure to apply the Windows update programs to the OPC client computers as well. If you do not apply these updates, the OPC clients may not be able to connect to the SOE OPC server.

- 2021-08 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB5005112)
- 2023-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5026362)

TIP

This information is current as of June 2023. The latest information is provided as Endpoint Security Service. For information about the Endpoint Security Service, contact YOKOGAWA.

IMPORTANT

For Windows update programs, be sure to apply the servicing stack update before applying the cumulative update.

Downloading the Windows Update Programs (Windows Server 2016)

Download and apply the following Windows update program. If you do not apply this update, installation of Windows update programs fails on the virtualization platform.

- 2023-03 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5023788)

In addition, download and apply the following Windows update program. If you do not apply this update, error log overflow occurs in system log collection in RIP Listener on the virtualization platform.

- 2023-05 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5026363)

If you have applied the Windows update programs to the SOE OPC server computer, be sure to apply the Windows update programs to the OPC client computers as well. If you do not apply these updates, the OPC clients may not be able to connect to the SOE OPC server.

TIP

This information is current as of June 2023. The latest information is provided as Endpoint Security Service. For information about the Endpoint Security Service, contact YOKOGAWA.

When Connecting with Other Products

When connecting ProSafe-RS to other YOKOGAWA products, configuration of IT security settings or other tasks may be required.

SEE ALSO

For more information about the tasks when connecting CENTUM VP with other products, refer to:

D., “Connection with Other Products” on page D-1

Notes on Initial Data of IT Security Settings

On a file server or domain controller, it is necessary to save the state before applying IT security settings as initial data.

When changing the user management type or IT security setting items, use the saved initial data to restore the state before applying the IT security settings, and then apply the IT security settings again.

About a file server, when changing the security settings, the following saved data of IT security settings is required depending on the user management type.

- When the user management type is standalone management or linked domain management in Standard model:

  Data saved before the first application of IT security settings in the standalone state

- When the user management type is Domain management or Combination management in Standard model:

  Data saved before applying IT security settings after adding to the domain

SEE ALSO For more information about saving of IT security settings of the computer that serves only as a file server, refer to:

"■ Procedure 4: Save the Initial Data of the IT Security Settings" on page B5-5

For more information about the procedure for reapplying IT security, refer to:

6.5.2, "Procedure for a File Server or Domain Controller" in ProSafe-RS Security Guide (IM 32P01C70-01EN)

B1.3 Precautions for Setting Up ProSafe-RS on a Virtual Machine on the Virtualization Platform

The following are precautions on setting up ProSafe-RS on a virtual machine on the virtualization platform.

Creating and Mounting ISO Format Files

A virtual machine on the virtualization platform cannot access the optical drive on the virtualization host computer. When using DVD-ROM or other media, for setting up a virtual machine, you must convert the media to ISO format and save it in an accessible folder on the host OS.

Create an ISO Format File

On the host OS, save the contents of the software media to an ISO format file by using free software or other means.

Mounting an ISO Format File on a Virtual Machine

Follow these steps to mount an ISO format file on a virtual machine:

1. Sign in to the host OS of virtualization host computer as an administrative user.
2. Copy an ISO format file of the software to mount and paste it into a folder on the host OS.
3. Select [Start] > [Server Manager].
   Server Manager starts.
4. Select [Tools] > [Hyper-V Manager].
   Hyper-V Manager starts.
5. On the left pane, select the virtualization host computer.
   Virtual machines on the virtualization host computer are displayed on the middle pane.
6. Right-click on the virtual machine that the ISO format file is mounted and select [Connect].
   The virtual machine connection window appears.

TIP The virtual machine connection window may appear full-screen. If it appears full-screen, click [Undo] to exit full-screen.

7. Select [Media] > [DVD Drive] > [Insert Disk].
   A file opening dialog box appears.
8. Select the ISO format file of the software to mount and click [Open].
   The selected ISO format file is mounted on the virtual machine.

Replacement in Descriptions when Installing on a Virtual Machine on the Virtualization Platform

When you install software on a virtual machine on the virtualization platform, replace “Insert the xxx software medium into the drive.” with “Specify the ISO format file of the xxx software.” as you read the descriptions of procedures.

B2. Setting Up the Windows Domain Environment

This section describes the required settings when ProSafe-RS is used in a Windows domain environment. You may also set up the Windows domain environment at a later stage.

SEE ALSO For more information about how to set up the Windows domain environment later, refer to:

C2., “Setting Up the Windows Domain Environment Later” on page C2-1

Consolidated Management of IT Security Settings Using the Domain Controller

ProSafe-RS allows for consolidated management of IT security settings using the domain controller.

To perform consolidated management of IT security settings, set IT securities on all clients first, and then use the domain controller to set consolidated management of IT security settings.

TIP You can build a domain controller with an OS supported by ProSafe-RS R4.07 or later, and join a computer on which R3.01 or later ProSafe-RS software installed to it. However, the Active Directory-based consolidated management of IT security settings can be applied to computers on which R4.03 or later ProSafe-RS software installed.

SEE ALSO For more information about the procedure for setting IT security on a client, refer to:

B3.6, “Configuring IT Security Settings” on page B3-44

For more information about setting up consolidated management of IT security settings, refer to:

6.10, “Active Directory-Based Consolidated Management of IT Security Settings” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

B2.1 Overview of Setting Up the Domain Environment

This section explains the overview of setting up the Windows domain environment.

It is recommended to provide dual-redundant domain controllers because the entire system will have troubles if the only domain controller fails.

Workflow

The following figure shows the procedure for setting up the Windows domain environment.

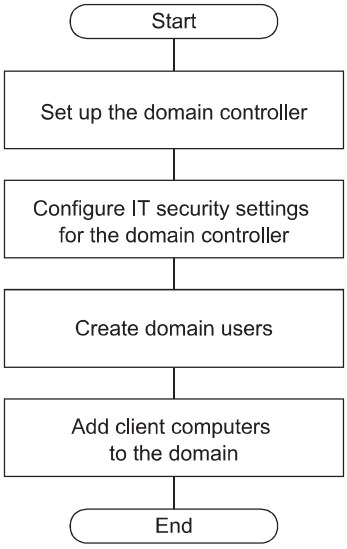


Figure B2.1-1 Flow of setting up the Windows domain environment

The timing for adding the client computer to the domain differs depending on whether the user management type of the IT security settings of the client computer is linked domain management or domain/combination management.

SEE ALSO For more information about the timing for adding client computers to the domain, refer to:

B2.5, “Adding Computers to the Domain” on page B2-17

Items to be Determined in Advance

- Domain name
- IP Address of the domain controller

Items to be Prepared

- Computer for the domain controller
- ProSafe-RS software medium
  This is required for configuration of IT security settings.

Items to be Set to the Domain Controller in Advance

- IP address
- Password for the Administrator account

Forest and Domain Function Level Settings

To configure the domain controller, the forest function level and domain function level must be set. The function level to be set varies depending on whether a new forest and domain will be configured or the domain controller will be added to an existing forest and domain.

Function Level to Be Set When Configuring a New Forest and Domain

Set the lowest function level that can be commonly set on all domain controller server OSs supported by ProSafe-RS.

If the following domain controller server OSs are supported by ProSafe-RS, for example, the lowest function level is Windows Server 2008:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

TIP

Set the lowest function level, considering the possibility that a server OS of low function level may be added as a domain controller.

Functional Level to Be Set When Adding a Domain Controller to an Existing Forest and Domain

In this case, the functional level of the existing forest and domain is set. Accordingly, which server OS can be used for the domain controller is limited by the functional level of the existing forest and domain.

The following table shows a list server OSs that can be selected for different functional levels of the existing forest and domain.

Table B2.1-1 Functional Levels of Existing Forest and Server OSs Selectable for ProSafe-RS

Functional level of existing forest	Server OSs Selectable for ProSafe-RS
Windows Server 2003	Windows Server 2016
Windows Server 2008	Windows Server 2016 Windows Server 2019 Windows Server 2022
Windows Server 2008 R2	Windows Server 2016 Windows Server 2019 Windows Server 2022
Windows Server 2012 R2	Windows Server 2016 Windows Server 2019 Windows Server 2022
Windows Server 2016	Windows Server 2016 Windows Server 2019 Windows Server 2022

Table B2.1-2 Functional Levels of Existing Domain and Server OSs Selectable for ProSafe-RS

Functional level of existing domain	Server OSs Selectable for ProSafe-RS
Windows Server 2003	Windows Server 2016
Windows Server 2008	Windows Server 2016 Windows Server 2019 Windows Server 2022

Continues on the next page

Table B2.1-2 Functional Levels of Existing Domain and Server OSs Selectable for ProSafe-RS (Table continued)

Functional level of existing domain	Server OSs Selectable for ProSafe-RS
Windows Server 2008 R2	Windows Server 2016 Windows Server 2019 Windows Server 2022
Windows Server 2012 R2	Windows Server 2016 Windows Server 2019 Windows Server 2022
Windows Server 2016	Windows Server 2016 Windows Server 2019 Windows Server 2022

For example, if the function level of the existing forest is Windows Server 2012 R2 and the function level of the domain is Windows Server 2016, the server OS versions selectable for ProSafe-RS are as follows.

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

B2.2 Configuring the domain controller

Configure the domain controller using Windows Server 2016, Windows Server 2019, or Windows Server 2022.

SEE ALSO

For more information about how to configure the domain controller using Windows Server 2016, Windows Server 2019, or Windows Server 2022, refer to:

Windows-related manual or the web site of Microsoft Corporation

B2.3 Configuring Security Settings for the Domain Controller

In a system that uses the Standard model of security settings, you need to run the IT Security Tool on the domain controller as well to apply the Standard model of security settings.

TIP

If you do not run the IT Security Tool on the domain controller because of the security policy of the user environment, manually create a domain user group.

SEE ALSO

For more information about domain user groups required by ProSafe-RS, refer to:

- "● Type 3: Standard Model/Strengthened Model - Domain Management" in "■ Combination of User Management and Security Model for Windows" in 2.2.3, "User/Group Management" in ProSafe-RS Security Guide (IM 32P01C70-01EN)
- "● Type 4: Standard Model/Strengthened Model - Combination Management" in "■ Combination of User Management and Security Model for Windows" in 2.2.3, "User/Group Management" in ProSafe-RS Security Guide (IM 32P01C70-01EN)
- "● Type 5: Standard Model/Strengthened Model - Linked Domain Management" in "■ Combination of User Management and Security Model for Windows" in 2.2.3, "User/Group Management" in ProSafe-RS Security Guide (IM 32P01C70-01EN)

■ Installing Windows Update Programs

Download and apply the Windows update programs for your Windows OS.

SEE ALSO

For more information about downloading the Windows Server 2022 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2022)" on page B1-5

For more information about downloading the Windows Server 2019 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2019)" on page B1-6

For more information about downloading the Windows Server 2016 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2016)" on page B1-6

■ Disabling the Automatic Cleanup Task

When using Windows Server as a domain controller, disable Automatic cleanup task.

SEE ALSO

For more information about the procedure for disabling the Automatic cleanup task, refer to:

"■ Disabling the Automatic Cleanup Task" on page B3-15

■ Installation of Microsoft Visual C++ 2017 Redistributable Package

Before you can run the IT Security Tool, you must install the Microsoft Visual C++ 2017 redistributable package.

Follow these steps to install the Microsoft Visual C++ 2017 redistributable package:

1. Log on to the domain controller as an administrative user.
2. Insert the ProSafe-RS software medium into the drive.
3. Using Explorer, double-click `<DVD drive>:\ProSafe-RS\vcredist_x86_2017\VC_redist.x86.exe`.
4. Agree to the license terms and perform the installation.

Preparing for Running the IT Security Tool

1. Log on to the domain controller as an administrative user.
2. Open the Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Active Directory Users and Computers].
   The Active Directory Users and Computers window appears.
4. In the left pane, right-click the [Users] folder and then select [New] > [Group].
   The New Object - Group dialog box appears.

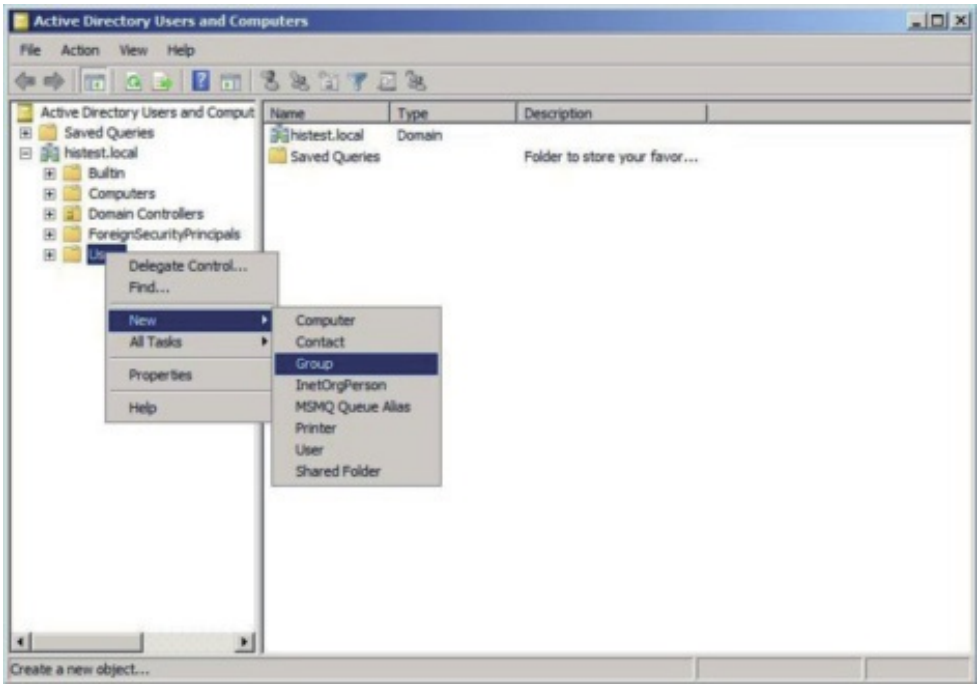


Figure B2.3-1 Active Directory Users and Computers

5. Enter `PSF_MAINTENANCE` in the Group name box, select the Group scope and Group type options, and then click [OK].

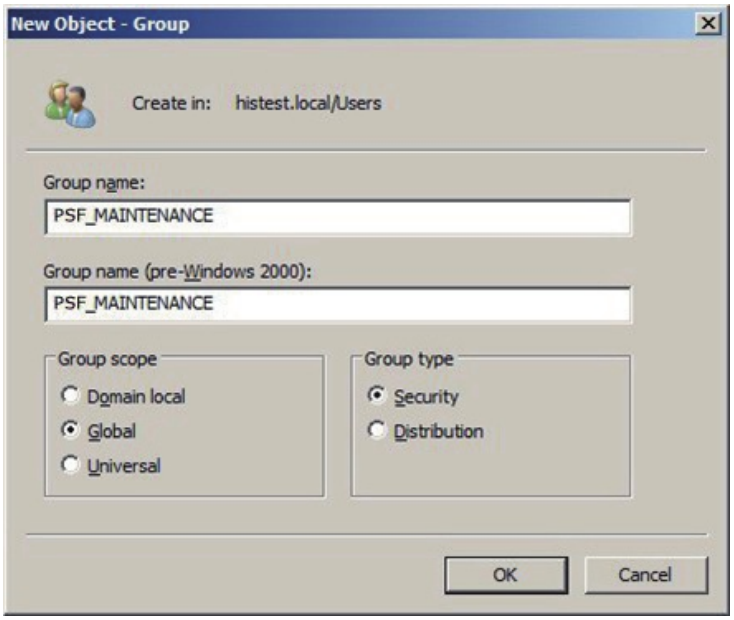


Figure B2.3-2 New Object - Group

6. Check the right pane to confirm that the PSF_MAINTENANCE group has been created in Users.

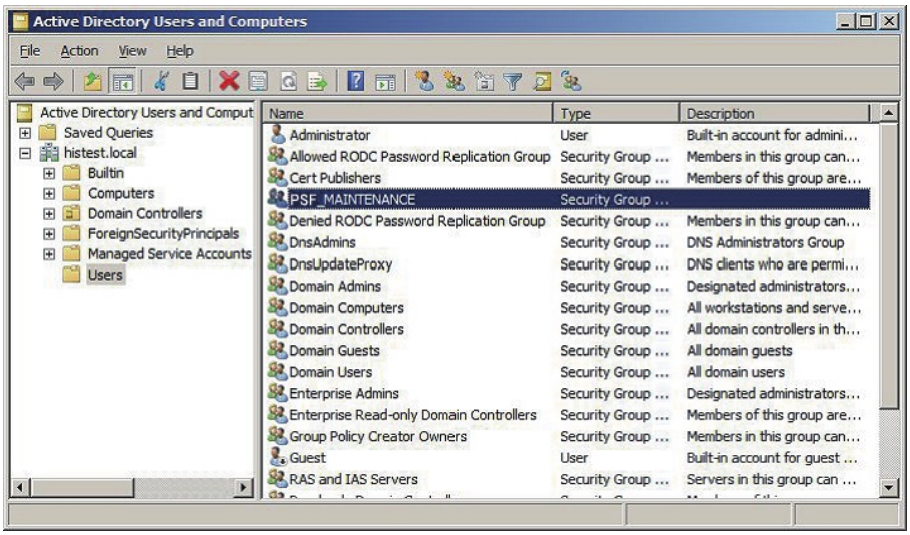


Figure B2.3-3 Activate Directory Users and Computers (after creating a new group)

7. Add the logged on user to the PSF_MAINTENANCE and Domain Admins groups.

TIP

If the domain controller is shared with CENTUM VP, the user must also belong to the CTM_MAINTENANCE group.

SEE ALSO

For more information about how to add uses to user groups, refer to:

"■ Adding Domain Users to Domain Groups" on page B2-14

Saving the Initial IT Security Settings

IMPORTANT

- When changing the IT security setting items, you need to use the initial data that was saved beforehand to restore the state before applying the IT security settings, and then apply the IT security settings again. Therefore, before you run the IT Security Tool to configure IT security settings for the first time after the Windows domain has been set up, be sure to save the security settings on the computer.
- When configuring the security settings for the second time onward, basically the security settings need not be saved. To configure the security settings by using the IT Security Tool of R3.01 to R4.02 and change the IT security version to 2.0 by using the IT Security Tool of R4.03 or later, save the initial security setting data again.
- To save the initial security setting data again, restore the security settings that were saved before by using the IT Security Tool. Then, perform this procedure to save the security settings. From then on, the data you have saved again will be used when the security settings are initialized; accordingly, keep the saved data in a safe place.

Follow these steps to save the security settings before your run the IT Security Tool:

1. Log on to the computer as the user who belongs to the Domain Admins and PSF_MAINTENANCE groups.
2. Insert the ProSafe-RS software medium into the drive.
   - If the AutoPlay dialog box appears, click [Run Launcher.exe].
   - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the software medium.

   The installation menu appears.
3. Click [Setting IT Security (File server/domain controller use)].
   The IT Security Tool starts.

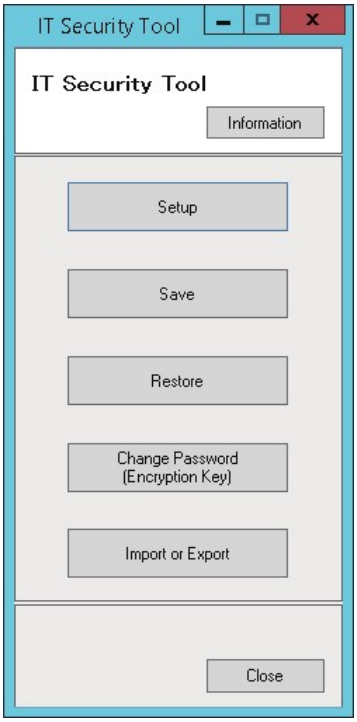


Figure B2.3-4 IT Security Tool menu

4. Click [Save].
   The Specify destination page appears.
5. Specify the destination folder and enter following setting items.
   - Distinguished Name
   - Support Product
   - Support OS
   - File Version

TIP

The [Distinguished Name] and [File Version] are omissible.

6. Click [Next].
   The Type default account password page appears.
7. Enter the password for use as the initial account password and click [Next].
   The Type password (Encryption Key) page appears.

TIP

This initial password will be set when the account saved with this tool is recovered. If the saved accounts are not found on the computer when you recover the accounts, new accounts are created. This password will be set as the initial password for the newly created account.

Even when multiple accounts have been created, the same initial password is assigned to all.

If the set password does not meet the password policy in the environment where the account is to be recovered, an error will occur when recovering an account.

This password is set as the initial password for the account. Accordingly, you will be prompted to change the password when you log on for the first time using this account.

8. Enter the password for encrypting the saved data, and click [Next].
   Saving of the security settings starts.

IMPORTANT

- If this password (encryption key) is lost, the saved security settings cannot be restored. The password (encryption key) must be carefully kept by the customer.
- The password (encryption key) must be at least one character.
- The password can consist of upper-case and lower-case alphanumeric characters and the following symbols: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . /
  Double-byte characters cannot be used.

9. When the saving is completed, click [Finish].
   If the saving failed, the details of the failure are displayed.
10. On the IT Security Tool menu, click [Close].

TIP If any save failures are displayed, contact YOKOGAWA Service.

Configuring IT Security Settings

1. From the IT Security Tool menu, click [Setup].
   A confirmation dialog box appears.
2. If you have saved the aforementioned security setting data for initialization, click [OK].
   The Select Security Model page appears.

TIP If you have not saved the initial security setting data, click [Cancel] to go back to the main menu and save the current security settings.

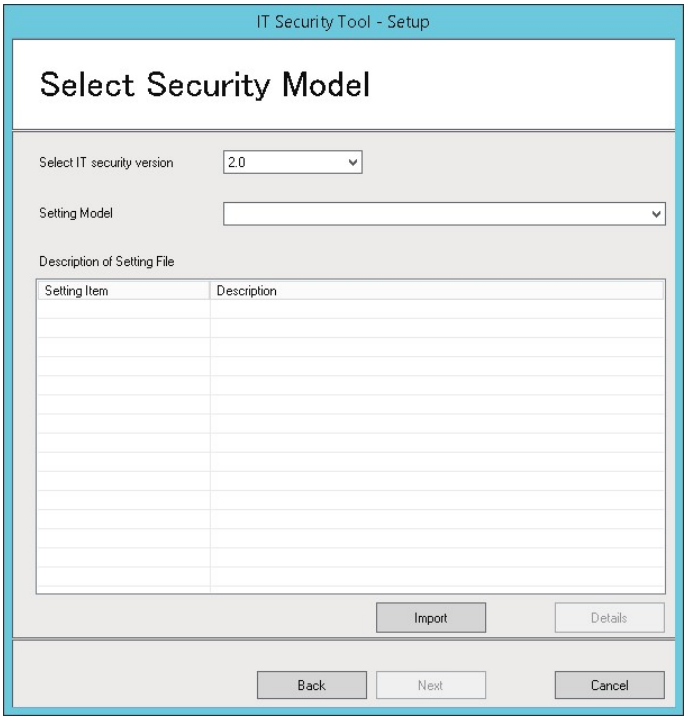


Figure B2.3-5 Select Security Model

3. From the Select IT security version drop-down list, select the IT security version.
4. From the Setting Model drop-down list, select [Domain Controller Standard Model Domain/Combination Management].

5. Click [Next].
   The Confirm Setting Information page appears.

TIP

If you click [Details], the Select Setting Items page appears.

6. For the rest of steps, perform the same operations as when the IT Security Tool is run immediately after installing the ProSafe-RS software.

TIP

If the domain controller is shared with CENTUM VP, start the IT Security Tool for file server and domain controller from the installation menu of CENTUM VP R6.04 or later software medium and set IT security for CENTUM VP as well.

SEE ALSO

For more information about the IT security setting operations that are performed following the ProSafe-RS software installation, refer to:

B3.6.1, “Running the IT Security Tool” on page B3-46

For more information about the procedure for importing the IT security settings, refer to:

6.8, “Exporting/Importing the IT Security Setting File” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

B2.4 Creating Domain Users

This section explains how to create domain users and add them to the domain groups.

IMPORTANT

When you change the rights of domain users, the changes may not be applied immediately. If this happens, log on and log off twice on each computer after you have changed users' rights.

Do the same thing when you have deleted rights from domain users.

Creating a Domain User

1. Open the Control Panel.
2. Select [System and Security] > [Administrative Tools] > [Active Directory Users and Computers].
   The Activate Directory Users and Computers window appears.
3. In the left pane, right-click the [Users] folder and then select [New] > [User].

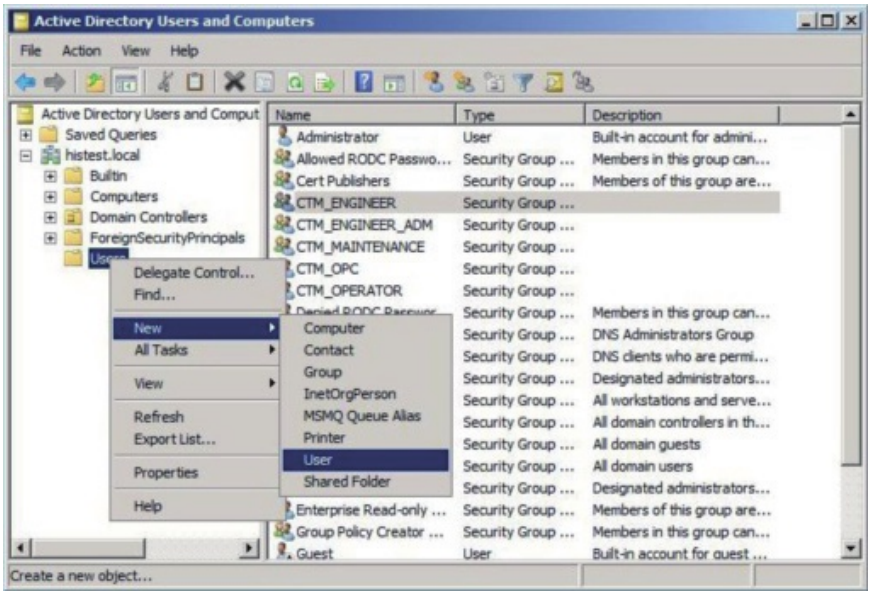


Figure B2.4-1 Activate Directory Users and Computers

4. The New Object-User dialog box is displayed. Input the necessary information.

TIP

Full name and User logon name have to be input in this dialog box. Additionally, if the User logon name is input, another logon name which is located under the above-mentioned User logon name is automatically input. However, the name is changeable.

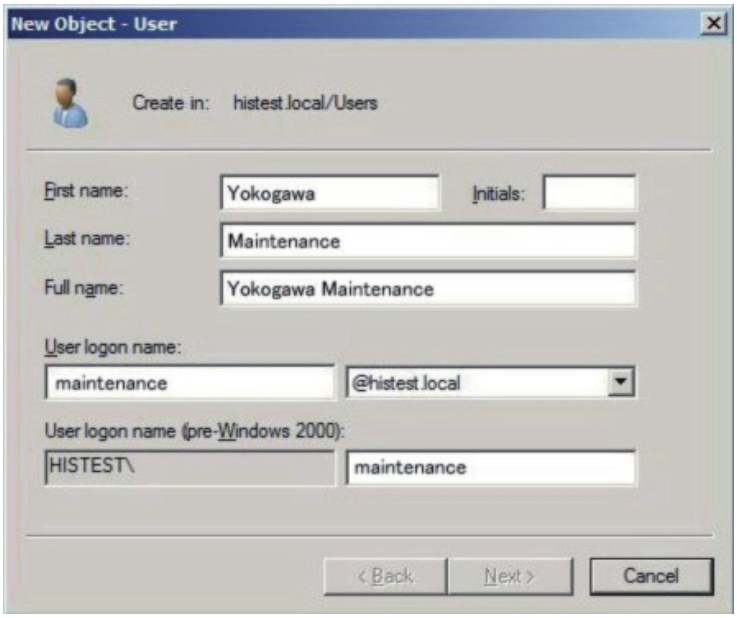


Figure B2.4-2 New Object-User

5. Click [Next].
   A dialog box appears, prompting you to enter the password.
6. Enter the password, select the check boxes of the required items, and click [Next].
   A confirmation dialog box appears.
7. Click [Finish].
8. Open the Users folder and check the right pane to confirm that the new domain user has been added.

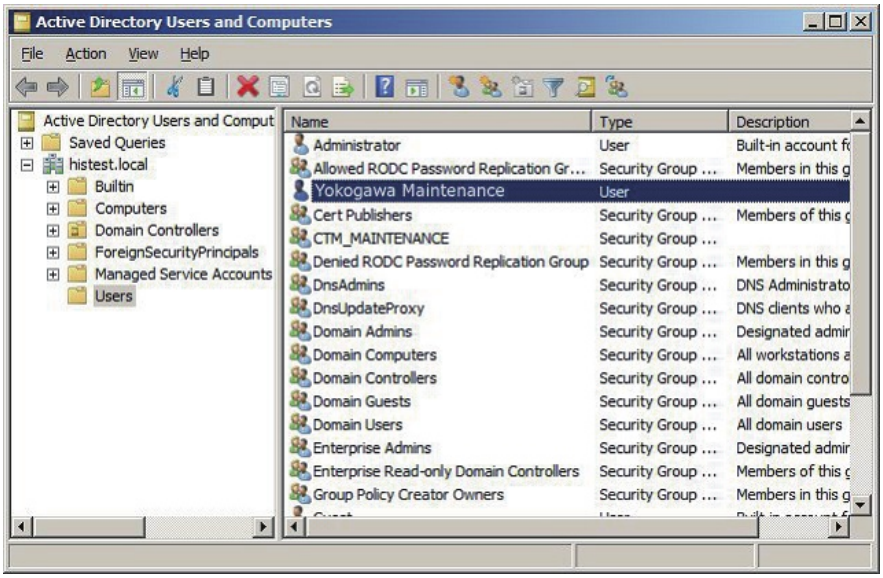


Figure B2.4-3 Activate Directory Users and Computers (confirmation of newly created user)

Adding Domain Users to Domain Groups

When applying the Standard model of security settings, you must add the domain users to appropriate domain groups.

After you run the IT Security Tool on the domain controller, the following ProSafe-RS domain groups have been created.

- PSF_OPERATOR
- PSF_ENGINEER
- PSF_OPC
- PSF_MAINTENANCE
- ADS_MANAGER

Adding a Domain User to a Domain Group

This section describes an example of adding a domain user (the user “yokogawa”) to the PSF_MAINTENANCE group.

TIP

For domain users who belong to a domain group which requires administrative rights, you also need to perform the procedure in the next section "●Setting Administrative Rights."

1. In the Active Directory Users and Computers window, double click the user that you want to grant the group's rights.
   The properties dialog box for the selected user appears.
2. Select the [Member Of] tab and click [Add].
   The Select Groups dialog box appears.
3. Click [Advanced].
   The advanced settings are displayed in the Select Groups dialog box.
4. Click [Find] to display the list of available groups. Select the PSF_MAINTENANCE group and click [OK].

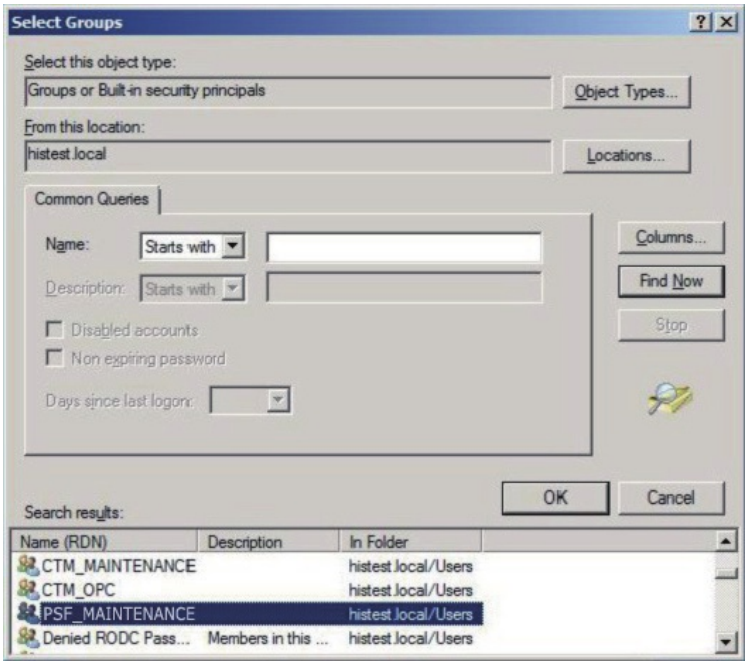


Figure B2.4-4 Select Groups dialog box - Search results

5. In the Select Groups dialog box, ensure that PSF_MAINTENANCE appears and click [OK].
6. In the Properties dialog box, confirm that PSF_MAINTENANCE is displayed in the Member of list.

Setting Administrative Rights

Follow these steps to assign administrative rights to a domain user who belongs to a domain group which requires administrative rights:

1. Add the domain user to the Domain Admins group.
2. Open the properties dialog box for the user. Click the [Member Of] tab, select [Domain Admins], and click [Set Primary Group].
   The primary group of the user changes to Domain Admins.
3. Select [Domain Users] and click [Remove].
4. Confirm that Domain User has been removed from the Member of list and click [OK].

B2.5 Adding Computers to the Domain

To add computers to a domain, computer accounts of the computers need to exist on the domain controller. Computer accounts can be created in two ways: creating on the domain controller or on computers.

When creating a computer account on the domain controller, the computer can be added to the domain by configuring on the computer after the computer account is created. When creating a computer account on the computer, the computer is added to the domain at the same time the computer account is created.

This section explains the procedure for the case where computer accounts are created on the domain controller and computer can be added to the domain by configuring on the computer. In the procedure, you are required to enter the user name and password of the administrative user of the domain when you configure on a computer.

Precautions When Setting Up Computers

This section describes precautions on operating the client computer with linked domain management for its user management type of the IT security settings.

- After you run IT Security Tool on the client computer, add the computer to the domain before you run Domain Link Management Tool.

The following are precautions on operating the client computer with domain or combination management for its user management type of the IT security settings.

- Before you install the ProSafe-RS software, add the client computer to the domain.
- If you are unable to add the computer to the domain in advance, set the Legacy model or the Standard model applying Standalone management temporarily in the IT security setting configuration that is performed following the ProSafe-RS software installation. Then, add the computer to the domain and change to the Standard model applying Domain management or Combination management.
- If a user who belongs to a domain group is used to install the ProSafe-RS software on a computer added to the domain, an administrative user for installing the ProSafe-RS software on the domain controller must be created in advance. Add the administrative user to the Domain Admins and PSF_MAINTENANCE user groups in advance.
- After installing the ProSafe-RS software, add the administrative user of the computer to the PSF_MAINTENANCE_LCL group.

SEE ALSO For more information about changing the security model, refer to:

6.4, “Changing the IT Security Settings” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

Configuration on the Domain Controller

1. Open the Control Panel.
2. Select [System and Security] > [Administrative Tools] > [Active Directory Users and Computers].
   The Active Directory Users and Computers window is displayed.
3. Right-click the Computers folder, and select [New] > [Computers].
   The New Object - Computer dialog box appears.
4. Enter the [Computer Name], and click [OK].
5. Confirm that the new computer has been added in the Computers folder.
   Configuration on the domain controller is finished. Go on to the procedure for configuration on the computer.

Configuration on a Computer

Follow these steps to add a computer to the domain:

1. Open the Control Panel.
2. Select [System and Security] > [System].
   The System window appears.
3. Click [Change Settings].
   The System Properties dialog box appears.
4. Select the [Computer Name] tab and click [Change].
   The Computer Name/Domain Changes dialog box appears.
5. Select [Domain], enter the domain name, and click [OK].
   The Windows Security dialog box appears.
6. Enter the user name and password of the administrative user of the domain and click [OK].

TIP

An error message dialog box may appear, indicating that the domain name cannot be changed. However, you can click [OK] to proceed because the computer has been added to the domain successfully.

7. On the Computer Name/Domain Changes dialog box, click [OK].
8. On the dialog box for confirmation of restarting, click [Restart Now] to restart the computer.

B2.6 Setting Up Redundant Domain Controllers

It is recommended to provide another domain controller for redundancy because the entire system will have troubles if the only domain controller fails.

Setup Procedure

1. Add the second domain controller computer to the existing domain.
2. Configure IT security settings.

SEE ALSO For more information about IT security settings, refer to:

B2.3, “Configuring Security Settings for the Domain Controller” on page B2-6

B2.7 Setting Up Time Synchronization in Windows Domain Environment

When using ProSafe-RS in a Windows domain environment, the time on computers used in the ProSafe-RS system and the time on the domain controller must be synchronized.

Because the time synchronization service of a ProSafe-RS system uses the time on the control bus as the time master, the time of the domain controller should be synchronized to the time of client computers if the system is used in a domain environment.

This section describes how to set up time synchronization in a system that consists of only ProSafe-RS.

Cautionary Note on Time Synchronization

A computer installed with the ProSafe-RS software is automatically configured so as not to use the domain controller as the time master for time synchronization, even if the computer is added to the Windows domain.

B2.7.1 Implementing Time Synchronization in a System Consisting of Only ProSafe-RS

This section describes how to implement time synchronization in a system consisting of only ProSafe-RS for the following cases:

- V net — Not synchronize to the Coordinated Universal Time (UTC)
- Vnet/IP — Synchronize to the Coordinated Universal Time (UTC)
- Vnet/IP — Not synchronize to the Coordinated Universal Time (UTC)

For V net — Not Synchronize to the Coordinated Universal Time (UTC)

Configure a station connected to the V net domain as the SNTP server. Times on the computers within the V net domain are synchronized using the V net time synchronization function. Time synchronization of the entire system is achieved by synchronizing the time on the domain controller to the SNTP server.

TIP

When a station is used as the SNTP server, the system time is not synchronized to UTC but to the time on the hardware of the SNTP server.

- On the computers connected on V net, do not use the Windows W32Time service to perform time synchronization. If used, times on the computers are synchronized to the time on the domain controller and synchronization with the SNTP server is prevented.
- On the domain controller, use the Windows W32Time service to synchronize its time with the SNTP server.

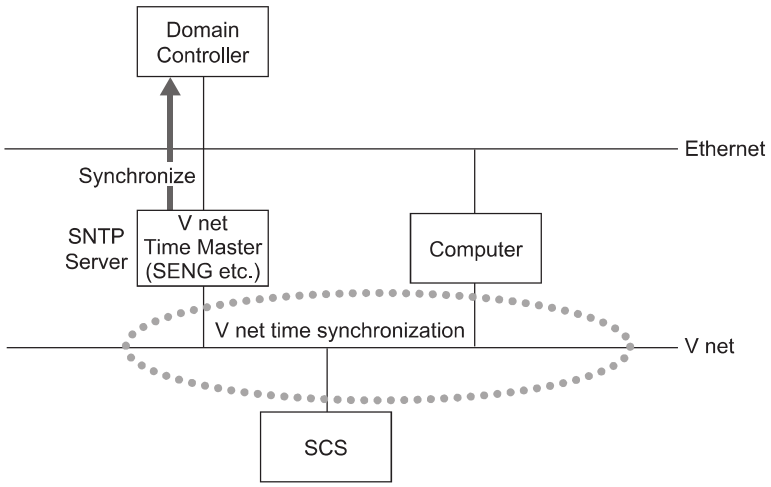


Figure B2.7.1-1 Implementing Time Synchronization (V net — Not Synchronize to UTC)

SEE ALSO

For more information about how to configure a station as the SNTP server, refer to:

"● Setting a Station as the SNTP Server" on page B2-23

For Vnet/IP — Synchronize to the Coordinated Universal Time (UTC)

- Introduce an SNTP server and make it synchronize with UTC. Configure the domain controller and the Vnet/IP system so that they will reference the time of the same SNTP server.

- On the computers connected on Vnet/IP, do not use the Windows W32Time service to perform time synchronization. If used, times on the computers are synchronized to the time on the domain controller and synchronization with the SNTP server is prevented.

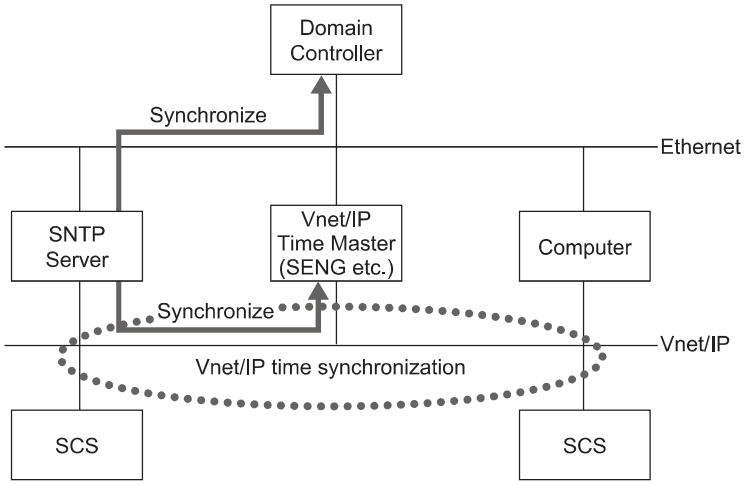


Figure B2.7.1-2 Implementing Time Synchronization (Vnet/IP — Synchronize to UTC)

For Vnet/IP — Not Synchronize to the Coordinated Universal Time (UTC)

Configure a station connected to the Vnet/IP domain as the SNTP server. Times on the computers within the Vnet/IP domain are synchronized using the Vnet/IP time synchronization function. Time synchronization of the entire system is achieved by synchronizing the time on the domain controller to the SNTP server.

TIP

When a station is used as the SNTP server, the system time is not synchronized to UTC but to the time on the hardware of the SNTP server.

- On the computers connected on Vnet/IP, do not use the Windows W32Time service to perform time synchronization. If used, times on the computers are synchronized to the time on the domain controller and synchronization with the SNTP server is prevented.
- On the domain controller, use the Windows W32Time service to synchronize its time with the SNTP server.

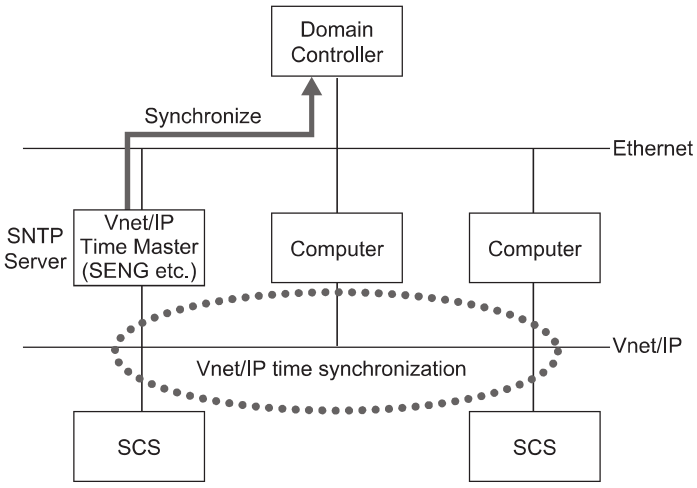


Figure B2.7.1-3 Implementing Time Synchronization (Vnet/IP — Not Synchronize to UTC)

Setting a Station as the SNTP Server

1. Use an administrative user account to log on to the station you want to set up as the SNTP server.
2. Right-click the following file and select [Run As Administrator].
   `(Drive of ProSafe-RS software medium):\ProSafe-RS\TOOLS\BeNtpServer.cmd`
   The Command Prompt window appears and displays "Enable NTP Server? (y/n/quit)."

TIP

If the IT security settings have been configured to apply software restriction policies, right-click [Command Prompt] and select [Run As Administrator]. Then, run the program in the Command Prompt that is opened.

3. Enter "`y`," and then press the [Enter] key.

B2.7.2 Implementing Time Synchronization When Integrated with CENTUM

When the system is integrated with CENTUM, set up time synchronization by following the explanation provided in the manual of CENTUM. If the system consists of multiple V net domains or a mixture of Vnet/IP domain and V net domain, also follow the explanation in the manual of CENTUM.

SEE ALSO

For more information about how to set up time synchronization in Windows domain environment for a system integrated with CENTUM, refer to:

B2.7, "Setting Up Time Synchronization in Windows Domain Environment" in CENTUM VP Installation (IM 33J01C10-01EN)

B3. Setup of an SENG or a Computer Installed with Only AD Server

This section describes the tasks required for setting up an SENG or a computer installed with only AD Server.

IMPORTANT

In a ProSafe-RS system, you need to decide on one computer for use as the license management station. The license management station can be set up on a computer where SENG runs.

Among stations of the system, you must set up the license management station first. Then, set up the computers that will be used as license-assigned stations. The software packages installed on the license-assigned stations become available for use after the licenses are distributed from the license management station and accepted on the license-assigned stations.

If an independent license management station is desired, you can also set it up as the computer dedicated to license management.

SEE ALSO For more information about how to set up the computer dedicated to license management, refer to:

B6., “Setting Up the Computer Dedicated to License Management” on page B6-1

Items to be Prepared

Have the following item at hand before new installation of the ProSafe-RS software.

- ProSafe-RS software medium

Also have the following items at hand if the SENG is to be used as a license management station. These are required when distributing licenses.

- ProSafe-RS license medium
- ProSafe-RS license sheet (with project ID)

B3.1 Setting Up the Hardware

This section describes the settings for a Vnet/IP interface card to be installed in SENG. In the case of a computer installed with only AD Server and SENG that runs on a virtual machine, setting is not required because a Vnet/IP interface card is not used.

CAUTION

When removing and installing the cards to set DIP switches, take measure to prevent the damages caused by static electricity.

SEE ALSO For more information about antistatic measures, refer to:

Appendix 4., “Antistatic Precautions When Handling Hardware” on page App.4-1

Front panel of the Vnet/IP interface card

- RDY lamp
  This lamp illuminates to indicate that the card is working properly as the result of the periodic diagnosis.
- RCV lamp
  This lamp illuminates when a signal is received.
- SND lamp
  This lamp illuminates when a signal is sent.
- Vnet/IP connector
  These connectors are used for connecting with the Layer2 Switch.

  The connector type is RJ45.

The front panel of VI702 is shown as follows:

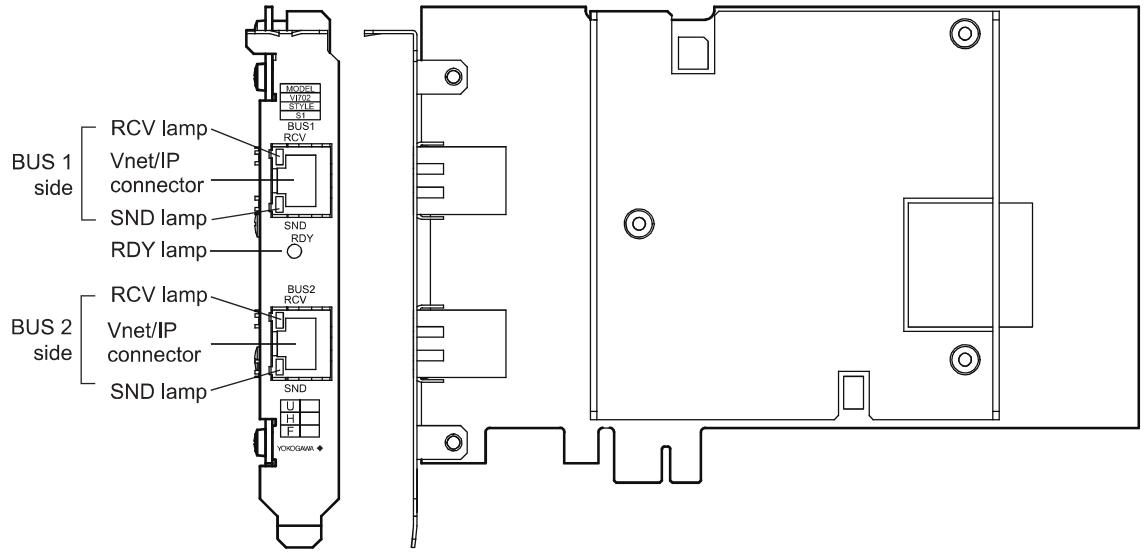


Figure B3.1-1 Vnet/IP Interface Card (VI702)

IMPORTANT

Note the following points when installing and uninstalling the VI702.

- Always install the VI702 before installing the control bus driver and Vnet/IP open communication driver.
  If the VI702 is installed after the control bus driver, the VI702 is not recognized. In this case, delete the driver, install the VI702, and then install the driver again.
- If the control bus driver and Vnet/IP driver are installed and you want to uninstall the VI702, delete these drivers first. If this procedure is not followed, an error dialog box will be displayed after restarting the PC and communication might not be possible.

Setting Up the Vnet/IP Interface Card

You need to install a Vnet/IP interface card (VI702) in the computer that is to be connected on a Vnet/IP network.

VI702 is for PCI Express.

The Vnet/IP interface card has DIP switches for setting the domain number, station number and action mode. The combination of domain number and station number determines the station address.

You must set the DIP switches before you configure network settings.

This section describes how to set the DIP switches.

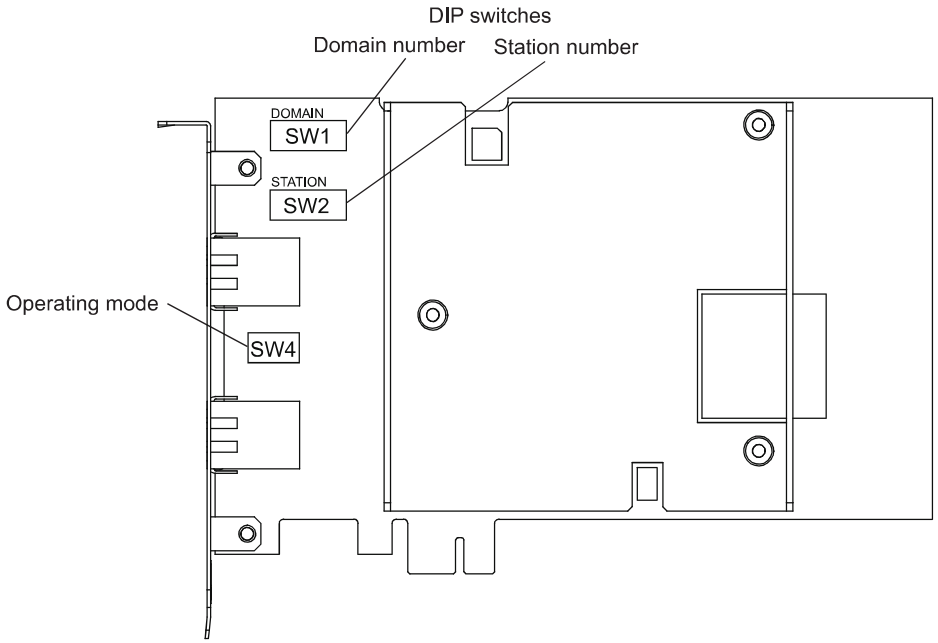


Figure B3.1-2 Locations of DIP Switches

Setting the Domain Number

A domain is a collection of stations that are connected on one control bus network. Set a domain number from 1 to 31 (1 to 16 when integrating with CENTUM).

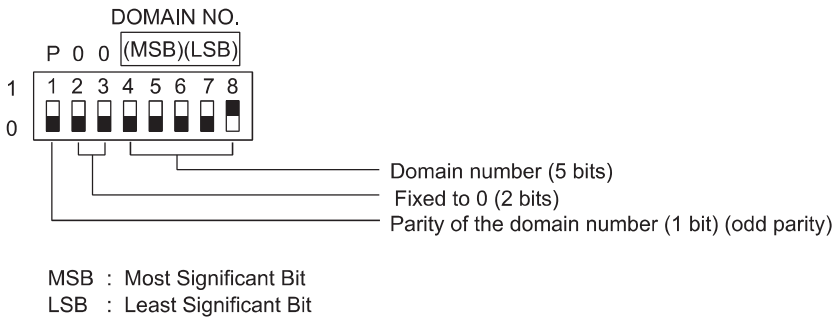


Figure B3.1-3 Domain Number Setting DIP Switches

SEE ALSO For more information about domain numbers and corresponding DIP switch positions, refer to:

"■ Domain Numbers and DIP Switch Positions" on page App.1-1

Setting the Station Number

Station numbers should be set in the range of 1 to 64; it is recommended to set starting from 64 in the descending order.

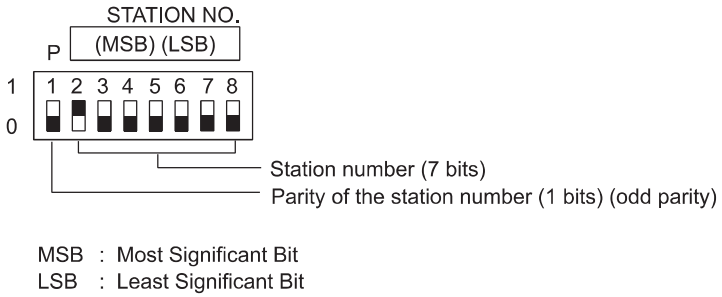


Figure B3.1-4 Station Number Setting DIP Switches

SEE ALSO For more information about station numbers and corresponding DIP switch positions, refer to:

"■ Station Numbers and DIP Switch Positions" on page App.1-2

Action Mode Switch

SW4 on the printed circuit board is the action mode switch.

Use the card with all the bits of this DIP switch set to OFF (factory set defaults). The meaning of DIP switch bits are as follows:

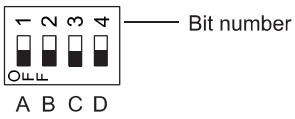


Figure B3.1-5 Action Mode Switch

Table B3.1-1 DIP Switch Usage

	DIP switch ON	DIP switch OFF	Remarks
A (bit 1)	-	Always OFF	Reserved
B (bit 2)	100 Mbps	1 Gbps	Communication speed (Default: OFF)
C (bit 3)	Force	Auto	Negotiation (Default: OFF)
D (bit 4)	-	Always OFF	Reserved

Precautions on Installing the Vnet/IP Interface Card

- Install VI702 in the computer after setting up Windows but before configuring the network settings.
- Install network drivers when you restart the computer after installing VI702. Follow the procedure in this manual to install the drivers.
- If you reuse VI702 that was used in another system for a stand-alone ProSafe-RS system, erase the settings in the VI702 before installing it in the computer. When using such VI702 in a system integrated with CENTUM, you do not need to erase the settings in the VI702.

SEE ALSO

For more information about the procedure to install the network driver in a computer, refer to:

- B3.3.1, “Installing the Control Bus Driver” on page B3-19
- B3.3.3, “Installing the Vnet/IP Open Communication Driver” on page B3-22

For more information about how to erase the internal settings of a VI702 card, refer to:

Appendix 2., “Procedure for Erasing VI702 Internal Settings” on page App.2-1

Installing the Vnet/IP Interface Card

After you have set the station address and action mode on the VI702 card, follow these steps to install it in the computer:

1. Turn off the power of the computer. For safety, remove the power plug from the outlet.
2. Remove the cover of the main unit of the computer.
3. Unscrew the screws fixing the slot cover and remove the slot cover.
4. Insert the VI702 card in the corresponding slot and fix it to the slot.
5. Mount the cover back on the computer.
6. Connect both the BUS1 and BUS2 cables to VI702 and Layer 2 switch. There is no need to turn off the power of the Layer 2 switch.
7. Connect the power cord of the computer back to the outlet and turn on the computer.
8. Make sure that the RDY lamp on VI702 is lit.
9. Write the station address on the label that comes with the VI702 card and paste it in the front or other easy-to-see location of the computer.

Attaching the Vnet/IP Station Address Label

You need to write the decided domain number and the station number to the station address seal attached to the VI702. And then stick the seal at the front side of the computer where the VI702 is installed or any other place that can be easily noticed.

STATION ADDRESS	
DOMAIN NO.	STATION NO.

Figure B3.1-6 Station Address Label

Procedures for removing the Vnet/IP interface card

IMPORTANT

Before removing the Vnet/IP interface card, uninstall the control bus driver and Vnet/IP open communication driver.

1. Turn off the power of the computer. For safety, remove the power plug from the outlet.
2. Disconnect the cables for both BUS1 and BUS2. There is no need to disconnect the cables from the Layer2 switch.
3. Remove the VI702 from the slot.

SEE ALSO For more information about the procedure for uninstalling the driver, refer to:

C5.1.2, “Uninstalling the Network Drivers” on page C5-5

B3.2 Setting Up Windows

Before installing the ProSafe-RS software, you need to change the Windows settings on your computer to the recommended settings.

This configuration is performed on the computer where the Windows OS has been installed.

Installing Windows Update Programs

Download and apply the Windows update programs for your Windows OS.

SEE ALSO

For more information about downloading the Windows 10 Enterprise LTSC 2021 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows 10 Enterprise LTSC 2021)" on page B1-4

For more information about downloading the Windows 10 Enterprise LTSC 2019 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows 10 Enterprise LTSC 2019)" on page B1-5

For more information about downloading the Windows 10 Enterprise 2016 LTSB update programs, refer to:

"■ Downloading the Windows Update Programs (Windows 10 Enterprise 2016 LTSB)" on page B1-5

For more information about downloading the Windows Server 2022 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2022)" on page B1-5

For more information about downloading the Windows Server 2019 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2019)" on page B1-6

For more information about downloading the Windows Server 2016 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2016)" on page B1-6

B3.2.1 Setting of Common Windows OS Items

This section describes how to set the items common to Windows 10, Windows Server 2016, Windows Server 2019, and Windows Server 2022.

File System

Ensure that the file system is in the NTFS format. If it is already formatted in the FAT format, reinstall the operating system and reformat partitions into NTFS. Partitions not installed with OS should also be formatted into NTFS.

System Performance

Follow these steps to configure the system performance setting:

1. Sign in as an administrative user.
2. Open the Control Panel.
3. Select [System and Security] > [System] > [Advanced system settings].
   The System Properties dialog box appears.
4. Select the [Advanced] tab and click [Settings] in the Performance section.
   The Performance Options dialog box appears.
5. On the [Visual Effects] tab, select [Let Windows choose what's best for my computer].
6. Click [OK].

Virtual Memory

ProSafe-RS does not require virtual memory configuration. However, if the ProSafe-RS and CENTUM VP software coexist on the same computer, virtual memory should be configured according to the instruction of CENTUM VP.

Power Options

This section describes how to configure the Power Options settings. Some of the items in the explanation may not be displayed on your computer, depending on the computer's hardware configuration. If not displayed, the function of that item is not available on your computer.

1. Log on as an administrative user.
2. Open the Control Panel.
3. Select [Hardware and Sound] > [Power Options].
   The Power Options window appears.

TIP For Windows Server, select [Hardware] > [Power Options].

4. Select [High performance] under Preferred plans and click [Change plan settings] on the right side.
   The Edit Plan Settings window appears.

TIP If High performance does not appear under Preferred plan, click [Show additional plans]. Select [High performance] and then click [Change plan settings] on the right side.

5. Click [Change advanced power settings].
   The Power Options dialog box appears, showing the advanced settings.

TIP

Depending on the computer configuration, the items of unavailable functions will not be displayed in the step results hereafter.

6. In the Power Options dialog box, set as follows:
   Hard disk

   [Turn off hard disk after]: Never

   Sleep

   [Sleep after]: Never

   [Allow hybrid sleep]: Off

   [Hibernate after]: Never

   [Allow wake timers]: Disable

   Power buttons and lid

   [Power button action]: Shut down

   Display

   [Turn off display after]: Never
7. Click [OK].

TIP

Configure the UPS settings after installing the ProSafe-RS software.

SEE ALSO

For more information about setting up UPS services, refer to:

B3.10, “Configuring the Uninterruptible Power Supply (UPS) Service” on page B3-65

B3.2.2 Setting of Items Specific to Windows 10

This section describes how to set the items specific to Windows 10.

Turning Off Fast Startup

You must turn off fast startup before installing the control bus driver or Vnet/IP open communication driver.

Follow these steps to turn off fast startup:

1. Use Windows Explorer to open the WIN10 folder under the following path in the ProSafe-RS software medium.
   `(Drive of ProSafe-RS software medium):\ProSafe-RS\TOOLS\WIN10`
2. Right-click [HiberbootDisabled.bat], and select [Run as administrator] from the context menu.
   The Command Prompt appears.
3. Confirm that the value of [HiberbootEnabled] is 0 as shown in the following figure.



Figure B3.2.2-1 Command Prompt

4. Hit the [Enter] key to restart the computer.

Windows Defender

The Windows Defender software detects and removes spy ware.

It is recommended to turn off this function because it is not used with this product.

In a domain environment, turn off Windows Defender on domain member PCs at a time by means of a domain management operation such as Group Policies.

In a workgroup environment, turn off Windows Defender by using the Local Group Policy Editor.

Turning Off Windows Defender in Local Group Policy Editor

Follow these steps to turn off Windows Defender:

1. Sign in as an administrative user.
2. Open Command Prompt.
3. Enter `gpedit.msc`.
   Local Group Policy Editor appears.
   The rest of the operation differs depending on the OS version.

TIP

- If the OS version is 1607 or earlier, [Windows Defender] is displayed instead of [Microsoft Defender Antivirus].
- If the OS version is 1703 to 1909, [Windows Defender Antivirus] is displayed instead of [Microsoft Defender Antivirus].
- If the OS version is 2004 or later, [Microsoft Defender Antivirus] is displayed.

4. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Microsoft Defender Antivirus].
5. In the right pane, double-click [Turn off Microsoft Defender Antivirus].
   The Turn off Microsoft Defender Antivirus dialog box appears.
6. Select [Enabled] and click [OK].

Defragment and Optimize Drives

The Defragmenter Tool can be used to reorganize the fragmented files on computer hard disk so as to improve the computer performance. Since the performance of this product may be affected when defragmenter is running, it is recommended to disable the schedule of the periodic disk defragmentation.

Moreover, you may manually start the disk defragmenter when you feel the disk performance is getting worse or when you perform system maintenance.

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Defragment and Optimize Drives].
   The Optimize Drives window appears.
4. Click [Change settings].
   The Optimize Drives dialog box appears.
5. Clear the [Run on a schedule (recommended)] check box and click [OK].

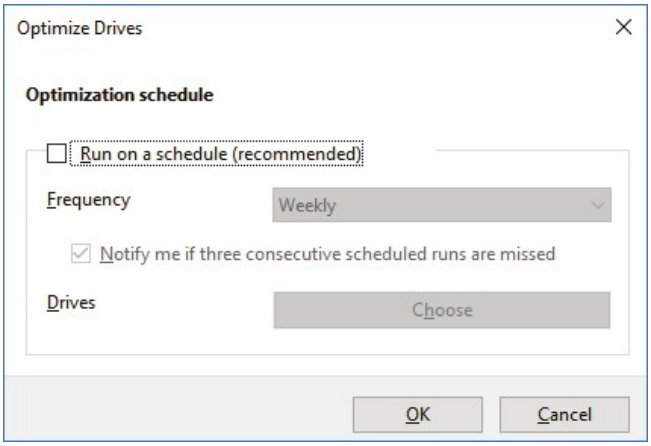


Figure B3.2.2-2 Optimize Drives dialog box

Disabling the Automatic Cleanup Task

A function is added to automatically clean up old files when update programs are applied.

Execution of Automatic cleanup may cause the degradation in system performance. For that reason, we recommend disabling Automatic cleanup for this product.

Follow these steps to disable the automatic cleanup task:

1. Sign in as an administrative user.
2. Open Control Panel.
3. From the menu, select [System and Security] > [Administrative Tools] > [Task Scheduler]. The Task Scheduler window appears.
4. In the left pane, select [Task Scheduler (Local)] > [Task Scheduler Library] > [Microsoft] > [Windows] > [Servicing].
5. In the middle pane, right-click [StartComponentCleanup] and select [Disable].
6. In the left pane, select [Task Scheduler (Local)] > [Task Scheduler Library] > [Microsoft] > [Windows] > [DiskCleanup].
7. In the middle pane, right-click [SilentCleanup] and select [Disable].

DCOM Settings

When Default Authentication Level in DCOM settings is set to [None], installation of applications such as redistributable modules fails. When installing this product, set the Default Authentication Level to [Connect].

Follow these steps to set Default Authentication Level to [Connect].

1. Sign in as an administrative user.
2. Open the Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Component Services]. The Component Services window appears.

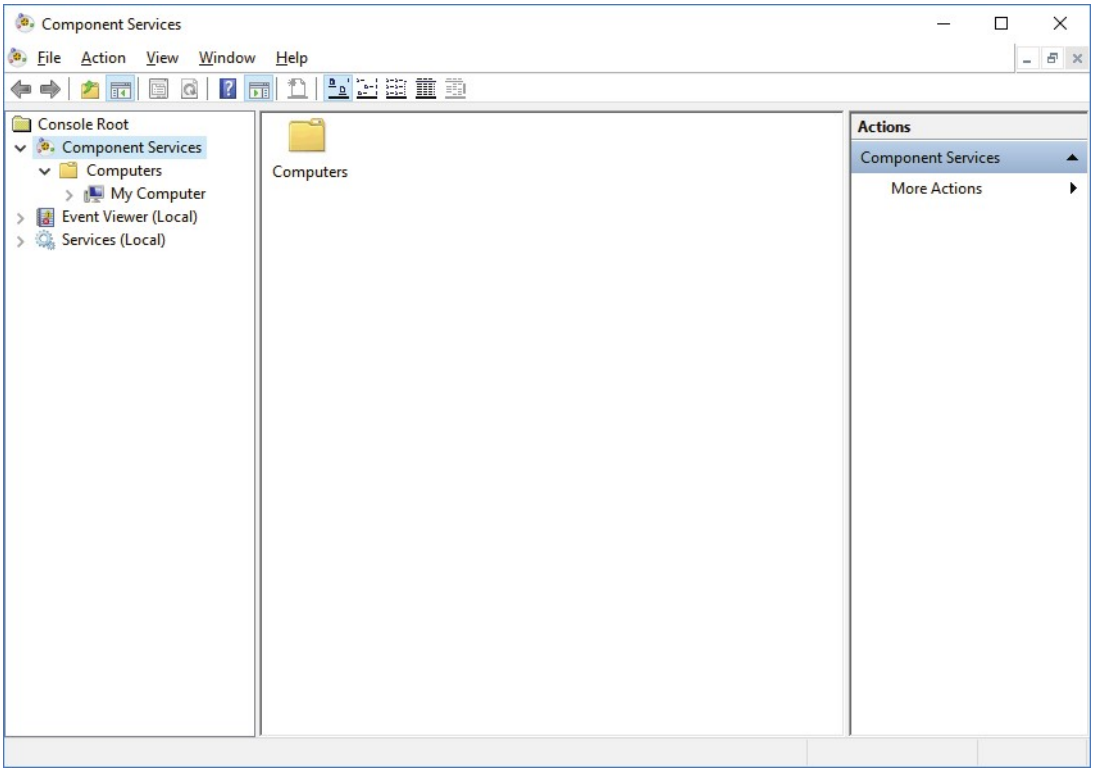


Figure B3.2.2-3 Component Services window

4. Select [Console Root] > [Component Services] > [Computers].
5. Right-click [My Computer] and select [Properties]. The My Computer Properties dialog box appears.

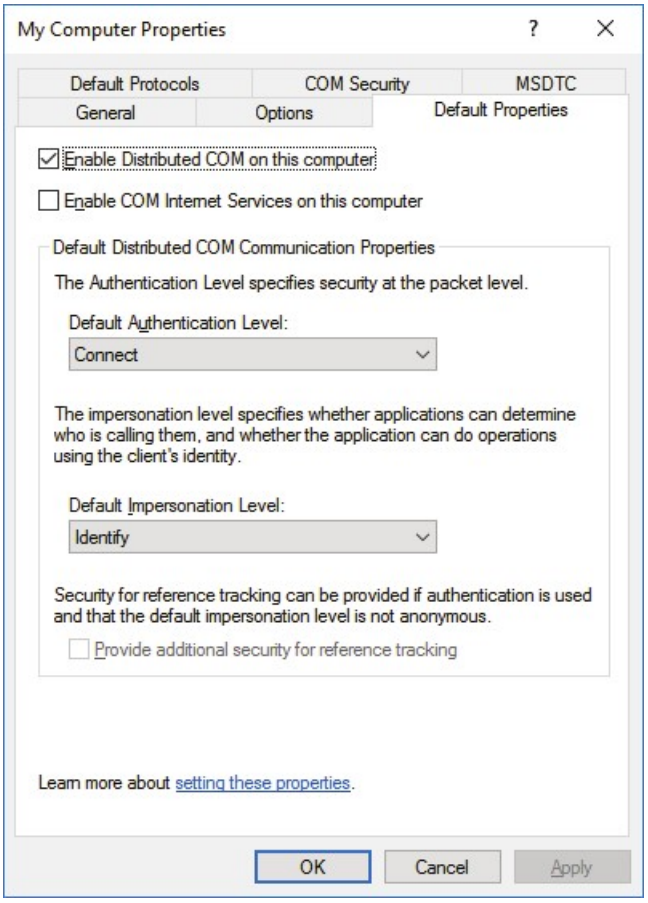


Figure B3.2.2-4 My Computer Properties dialog box

6. Open the [Default Properties] tab, from the Default Authentication Level drop-down list, select [Connect], and then click [OK].
7. Restart the computer.

B3.2.3 Setting of Items for Windows Server 2016, Windows Server 2019, and Windows Server 2022

This section describes how to set the items for Windows Server 2016, Windows Server 2019, and Windows Server 2022.

Windows Defender

The Windows Defender software detects and removes spy ware.

It is recommended to turn off this function because it is not used with this product.

In a domain environment, turn off Windows Defender on domain member PCs at a time by means of a domain management operation such as Group Policies.

In a workgroup environment, turn off Windows Defender by using the Local Group Policy Editor.

Turning off Windows Defender in Local Group Policy Editor

Follow these steps to turn off Windows Defender:

1. Sign in as an administrative user.
2. Open Command Prompt.
3. Enter `gpedit.msc`.
   Local Group Policy Editor appears.
   The rest of the operation differs depending on the OS version.

TIP

- If the OS version is 1607 or earlier, [Windows Defender] is displayed instead of [Microsoft Defender Antivirus].
- If the OS version is 1703 to 1909, [Windows Defender Antivirus] is displayed instead of [Microsoft Defender Antivirus].
- If the OS version is 2004 or later, [Microsoft Defender Antivirus] is displayed.

4. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Microsoft Defender Antivirus].
5. In the right pane, double-click [Turn off Microsoft Defender Antivirus].
   The Turn off Microsoft Defender Antivirus dialog box appears.
6. Select [Enabled] and click [OK].

Defragment and Optimize Drives

The Defragmenter Tool can be used to reorganize the fragmented files on computer hard disk so as to improve the computer performance. Since the performance of this product may be affected when the defragmenter is running, it is recommended to disable the schedule of the periodic disk defragmentation.

Moreover, you may manually start the disk defragmenter when you feel the disk performance is getting worse or when you perform system maintenance.

1. Sign in as an administrative user.
2. Open the Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Defragment and Optimize Drives].
   The Optimize Drives window appears.
4. Click [Change settings].
   The Optimize Drives dialog box appears.

5. Clear the [Run on a schedule (recommended)] check box and click [OK].

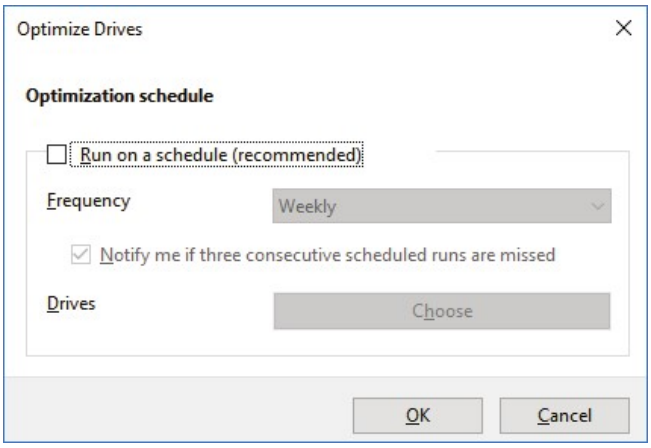


Figure B3.2.3-1 Optimize Drives dialog box

Disabling the Automatic Cleanup Task

A function is added to automatically clean up old files when update programs are applied.

Execution of Automatic cleanup may cause the degradation in system performance. For that reason, we recommend disabling Automatic cleanup for this product.

Follow these steps to disable the automatic cleanup task:

1. Sign in as an administrative user.
2. Open Control Panel.
3. From the menu, select [System and Security] > [Administrative Tools] > [Task Scheduler]. The Task Scheduler window appears.
4. In the left pane, select [Task Scheduler (Local)] > [Task Scheduler Library] > [Microsoft] > [Windows] > [Servicing].
5. In the middle pane, right-click [StartComponentCleanup] and select [Disable].
6. In the left pane, select [Task Scheduler (Local)] > [Task Scheduler Library] > [Microsoft] > [Windows] > [DiskCleanup].
7. In the middle pane, right-click [SilentCleanup] and select [Disable].

DCOM Settings

When Default Authentication Level in DCOM settings is set to [None], installation of applications such as redistributable modules fails. When installing this product, set the Default Authentication Level to [Connect].

Follow these steps to set Default Authentication Level to [Connect].

1. Sign in as an administrative user.
2. Open the Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Component Services]. The Component Services window appears.

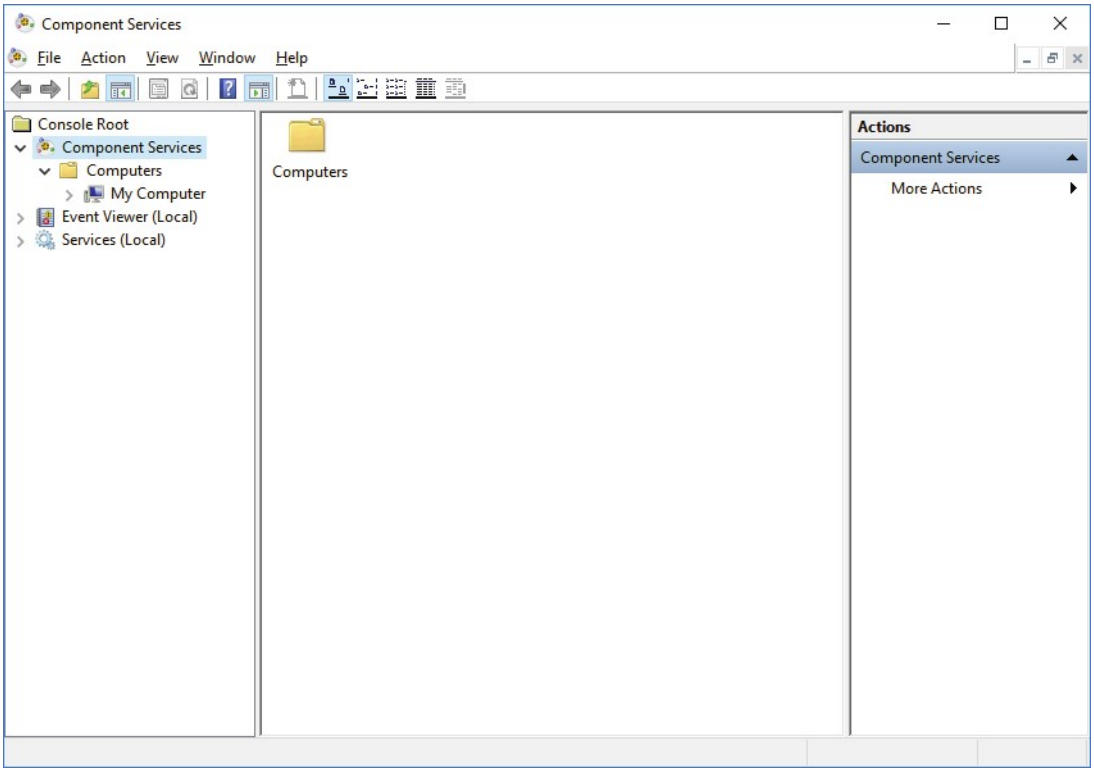


Figure B3.2.3-2 Component Services window

4. Select [Console Root] > [Component Services] > [Computers].
5. Right-click [My Computer] and select [Properties].
   The My Computer Properties dialog box appears.

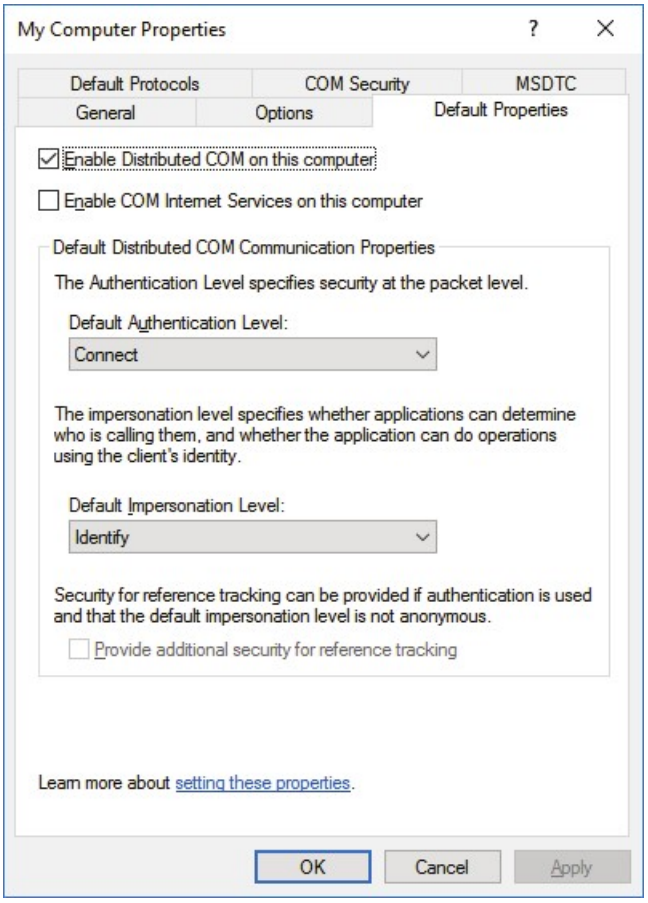


Figure B3.2.3-3 My Computer Properties dialog box

6. Open the [Default Properties] tab, from the Default Authentication Level drop-down list, select [Connect], and then click [OK].
7. Restart the computer.

B3.3 Configuring Network Settings

To use the control bus, you need to install the control bus driver. If Vnet/IP is used as the control bus, you need to install the Vnet/IP open communication driver as well.

This section describes how to install the control bus driver and the Vnet/IP open communication driver.

If you use the built-in Ethernet interface of the computer or an over-the-counter Ethernet card, read the attached instruction manual and install the proper Ethernet driver accordingly.

In the case of SENG that runs on a virtual machine, install the Vnet/IP Interface Package on the virtual machine. Also, do not install the Vnet/IP open communication driver.

TIP

On a network where there is a virtual machine with the Vnet/IP Interface Package installed, it cannot be configured when only Vnet/IP is installed.

After installing the driver and interface package, set up the Windows network.

B3.3.1 Installing the Control Bus Driver

This section describes the procedure for installing the control bus driver.

Precautions at Installation

Mount a control bus interface card or Vnet/IP interface card in computers to be connected on a control bus network. In addition, you must install the control bus driver. Observe the following precautions when you install the control bus driver.

- Before installing the control bus driver, be sure to install a control bus interface card or Vnet/IP interface card in the computer.
- For Windows 10, be sure to check that fast startup is turned off before installing the control bus driver. If fast startup is not turned off, turn it off and restart the computer.
- If you installed the control bus driver without installing a control bus interface card or Vnet/IP interface card by mistake, uninstall the control bus driver. Then, install a control bus interface card and install the driver again.
- If you want to change the slot in which a control bus interface card or Vnet/IP interface card is installed, uninstall the control bus driver first and then change the slot. After changing the slot, install the driver again.
- When you remove a control bus interface card or Vnet/IP interface card from the computer where the control bus driver was installed with the card installed, uninstall the driver before you remove the card from the slot.

TIP

- When installing the control bus driver, restarting the computer is basically not required. However, restart the computer if a dialog box indicating completion of the installation (restarting required) is displayed.
- After you install the driver, you need to configure network settings.

SEE ALSO

For more information about turning off fast startup, refer to:

"■ Turning Off Fast Startup" on page B3-10

Notes on Using SCS Simulator

To use the SCS simulator, an environment where ProSafe-RS is integrated with CENTUM is mandatory. You can run the SCS simulator even on a computer where a control bus interface card or Vnet/IP interface is not mounted; however, you must always install the control bus driver on such computers. Observe the following precautions when you install the control bus driver on a computer where these cards are not mounted in order to use the SCS simulator.

- Install the control bus driver, and then configure Windows network settings.
- If you use the expanded test functions to run SCS simulators on multiple computers, install the control bus driver in all the computers on which you run the SCS simulator without mounting a control bus card. If mounted, you cannot launch the SCS simulator remotely.

TIP

- If a control bus card is not mounted when you install the control bus driver, a control bus driver of the version for use without a control bus card is installed. This driver is used when the SCS simulator is run without mounting a control bus card.
- To reuse or divert a computer installed with a without-a-control-bus-card version of control bus driver for use in actual plant operation, uninstall the control bus driver, mount a control bus card, and then install the control bus driver again.

- The control bus driver should be installed according to the procedure for installing the control bus driver.

- For the IP address for the control bus driver on each computer, set the address of control bus, “domain number (dd) .station number (ss)”.
  Example: 172.16.dd.ss

  Note that dd.ss must not overlap with the addresses of the other stations. In particular, it must not overlap with the “domain number.station number” used for SCS and FCS.

Installation Procedure

1. Log on as an administrative user.
2. Insert the ProSafe-RS software medium into the drive.
   - If the AutoPlay dialog box appears, click [Run Launcher.exe].
   - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the ProSafe-RS software medium.

   The installation menu appears.
3. On the installation menu, click [Control Bus Driver].
   A dialog box appears, prompting you to confirm the setup.
4. Select [INSTALL] and click [OK].
   A dialog box appears, confirming to execute the installation.
5. Click [OK].

TIP

- If the Windows Security dialog box appears, select the [Always trust software from “Yokogawa Electric Corporation”] check box, and click [Install].
- Do not click [Don’t Install] on the Windows Security dialog boxes. If clicked, an error occurs.

6. When the message telling successful installation is displayed, click [OK].

TIP

If you have added or deleted any other devices before you install the control bus driver, a message prompting you to restart the computer may be displayed. In such a case, be sure to restart the computer.

B3.3.2 Setting Up the RIP Listener Service on a Virtual Machine

When using the virtualization platform, you must set up the RIP Listener service on a virtual machine.

This section describes enabling the RIP Listener service. The method for enabling the RIP Listener service is different between Windows Server 2019 or later and Windows Server 2016 running as the guest OS of the virtual machine.

SEE ALSO For more information about settings of the function for receiving RIP packet in Windows Server 2019 or later, refer to:

Virtualization Platform Setup (IM 30A05B20-01EN)

■ Enabling the RIP Listener Service: Windows Server 2016

If the guest OS of the virtual machine is Windows Server 2016, RIP Listener service is automatically installed when the OS is installed. Therefore, you do not need to install the RIP Listener service. However, the RIP Listener service is disabled by default, so you must enable the RIP Listener service.

● Enabling the RIP Listener Service: Windows Server 2016

Follow these steps to enable the RIP Listener Service:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Run the Command Prompt as Administrator.
3. Run the following command:
   `dism /online /enable-feature /featurename:rasrip /all`
4. Confirm that the message, “The operation completed successfully.” appears.
5. Check that the RIP Listener service has been enabled.
   a. Open Control Panel.
   b. Select [System and Security] > [Administrative Tools] > [Service].
      The Services window appears.
   c. Confirm that RIP Listener is shown and its Startup Type is [Automatic].

TIP If the Default Authentication Level of DCOM is set to “None,” you cannot enable the RIP Listener service.

SEE ALSO For more information about how to change the default authentication level of DCOM to “Connect”, refer to:

“■ DCOM Settings” on page B3-15

B3.3.3 Installing the Vnet/IP Open Communication Driver

When Vnet/IP is used as the control bus, the Vnet/IP open communication driver also needs to be installed. If Ethernet is also used, the installed Vnet/IP open communication driver must be disabled.

This section describes the procedure for installing the Vnet/IP open communication driver.

IMPORTANT

When the Vnet/IP interface card is mounted, always install the Vnet/IP open communication driver even if Vnet/IP open communication is not used.

■ Precautions at Installation

- Before installing the Vnet/IP open communication driver, be sure to install a Vnet/IP interface card in the computer. You cannot install the driver if the card is not installed.
- For Windows 10, be sure to check that fast startup is turned off before installing the Vnet/IP open communication driver. If fast startup is not turned off, turn it off and restart the computer.
- If you want to change the slot in which a Vnet/IP interface card is mounted, uninstall the Vnet/IP open communication driver and control bus driver and then change the slot. After changing the slot, install the drivers again.
- When removing a Vnet/IP interface card from a computer after the Vnet/IP open communication driver is installed, uninstall the driver before you remove the card from the slot.

TIP

- When installing the Vnet/IP open communication driver, restarting the computer is basically not required. However, restart the computer if a dialog box indicating completion of the installation (restarting required) is displayed.
- When Ethernet is also used, configure network settings after you install the Vnet/IP open communication driver and disable the driver.

  When Ethernet is not used, configure network settings after you install the Vnet/IP open communication driver.

SEE ALSO

For more information about turning off fast startup, refer to:

"■ Turning Off Fast Startup" on page B3-10

■ Installation Procedure

1. Log on as an administrative user.
2. Insert the ProSafe-RS software medium into the drive.
   - If the AutoPlay dialog box appears, click [Run Launcher.exe].
   - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the ProSafe-RS software medium.

   The installation menu appears.
3. On the installation menu, click the [Vnet/IP Open com driver].
   A dialog box appears, prompting you to confirm the setup.
4. Select [INSTALL] and click [OK].
   A dialog box appears, confirming to execute the installation.
5. Click [OK].

TIP

- If the Windows Security dialog box appears, select the [Always trust software from “Yokogawa Electric Corporation”] check box, and click [Install].
- Do not click [Don’t Install] on the Windows Security dialog box. If clicked, an error occurs.

6. When the message telling successful installation is displayed, click [OK].

TIP

If you have added or deleted any other devices before you install the Vnet/IP open communication driver, a message prompting you to restart the computer may be displayed. In such a case, be sure to restart the computer.

B3.3.4 Installing the Vnet/IP Interface Package on a Virtual Machine

When using the virtualization platform, you need to install the Vnet/IP Interface Package on a virtual machine.

Follow these steps to install the Vnet/IP Interface Package on a virtual machine.

The procedures explained here should be performed on the guest OS of the virtual machine.

IMPORTANT

- You do not need to install a Vnet/IP interface card in the virtualization host computer.
- When multiple products coexist in one virtual machine, you do not need to install the Vnet/IP Interface Package as long as a Vnet/IP Interface Package has already been installed on another product.
- After installing the Vnet/IP Interface Package, you need to configure the Windows network settings on the virtual machine.

SEE ALSO For more information about overview of virtualization platform and precautions on using ProSafe-RS with a virtual machine, refer to:

A7., “Virtualization platform” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

For more information about details of the virtualization platform, refer to:

- Virtualization Platform Setup (IM 30A05B20-01EN)
- Virtualization Platform Planning and Implementation Guide (TI 30A05B10-01EN)

Precautions When Installing the Vnet/IP Interface Package

Observe the following precautions when you install the Vnet/IP Interface Package.

Precautions at First-time Installation

Install the Vnet/IP Interface Package before applying IT security. If you install the Vnet/IP Interface Package for the first time on a computer after applying IT security, you must apply IT security again.

TIP After IT security is applied, you do not need to apply IT security again when you reinstall the Vnet/IP Interface Package.

Precautions at Reinstallation

Reinstalling the Vnet/IP Interface Package resets the password of the Vnet/IP Interface Package execution user. If you have changed the password, set it again.

Procedure to Install the Vnet/IP Interface Package

Follow these steps to install the Vnet/IP Interface Package.

Preparation

Install Windows update as a preparation.

SEE ALSO For more information about the Windows Server 2016 update programs to apply, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2016)" on page B1-6

Procedure 1: Install the Vnet/IP Interface Package

Follow these steps to install the Vnet/IP Interface Package.

TIP If you have added or deleted any other devices before you install the Vnet/IP Interface Package, a message prompting you to restart the computer may be displayed. If displayed, be sure to restart the virtual machine.

1. Sign in to the host OS of virtualization host computer as an administrative user.
2. Copy an ISO format file of the ProSafe-RS software medium and paste it into a folder on the host OS.
3. Select [Start] > [Server Manager].
   Server Manager starts.
4. Select [Tools] > [Hyper-V Manager].
   Hyper-V Manager starts.
5. On the left pane, select the virtualization host computer.
   Virtual machines on the virtualization host computer are displayed on the middle pane.
6. Right-click on the virtual machine that the ISO format file is mounted and select [Connect].
   The virtual machine connection window appears.

TIP The virtual machine connection window may appear full-screen. If it appears full-screen, click [Undo] to exit full-screen.

7. Select [Media] > [DVD Drive] > [Insert Disk].
   A file opening dialog box appears.
8. Select the copied ISO format file of the ProSafe-RS software medium and click [Open].
   The selected ISO format file is mounted on the virtual machine.
   - If the AutoPlay dialog box appears, click [Run Launcher.exe].
   - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the ISO format file of the ProSafe-RS software.

   The installation menu appears.
9. On the installation menu, click [Control Bus Driver].
   A dialog box appears, prompting you to confirm the setup.
10. Select [INSTALL] and click [OK].
    A dialog box appears, confirming to execute the installation.
11. Click [OK].

TIP
- If the Windows Security dialog box appears, select the [Always trust software from "Yokogawa Electric Corporation"] check box, and click [Install].
- Do not click [Don't Install] on the Windows Security dialog box. If clicked, an error occurs.

12. When the message telling successful installation is displayed, click [OK].

Procedure 2: Set the Domain Number and Station Number Managed by the Vnet/IP Interface Package

When the installation of the Vnet/IP Interface Package is complete, the Vnet/IP Interface Management Tool appears. Using this tool, set the domain number and station number that will be managed by the Vnet/IP Interface Package. Follow these steps to set the domain number and station number.

TIP

You can also set the domain number and station number managed by the Vnet/IP Interface Package later. You must restart the virtual machine to reflect the settings.

1. Open the Settings tab of the Vnet/IP Interface Management Tool.
2. Set the domain number in [Domain No] and the station number in [Station No], and then click [Save].

TIP

You can set a number in the range from 1 to 31 as the domain number (1 to 16 in the case of CENTUM integration), and from 1 to 64 as the station number. If both domain number and station number are set to 0, Vnet/IP communication is disabled and communication to the control network is not possible.

On a virtual machine where you run an FCS simulator that can be operated through remote connection from another HIS by installing the Expanded Test Functions and SCS Simulator Package, set both the domain number and the station number to 0.

Note that the license of Vnet/IP Interface Package is not required when using only the test function with the domain number and the station number set to 0.

3. Click [CLOSE], and restart the virtual machine.

SEE ALSO

For more information about Vnet/IP interface management tool, refer to:

"■ Changing the Domain Number and Station Number" on page App.3-1

Procedure 3: Activate License of the Vnet/IP Interface Package

Before you can use the Vnet/IP Interface Package, you must activate the license for the package. After installing the ProSafe-RS software, distribute and accept the license of the Vnet/IP Interface Package.

B3.3.5 Configuring Windows Network Settings

You must configure the Windows network settings after installing the network driver.

This section explains the procedures for configuring Windows network settings related to control bus, Vnet/IP open communication, and Ethernet.

Cautions on Cable Wiring

When the cable is wired for network connection, the network charm bar may appear.

SEE ALSO For more information about the Set Network Location dialog box and network charm bar, refer to:

C7.2.1, “Precaution on Network Cable Connection” on page C7-5

Checking the Card for Control Bus

Check the card for control bus that is installed on the computer.

When a Control Bus Interface Card is Installed

In a system using V net, a control bus interface card is installed in computers. In this case, configure Windows network settings for control bus communications and Ethernet communications.

When a Vnet/IP Interface Card is Installed

In a system using Vnet/IP, a Vnet/IP interface card is installed in computers.

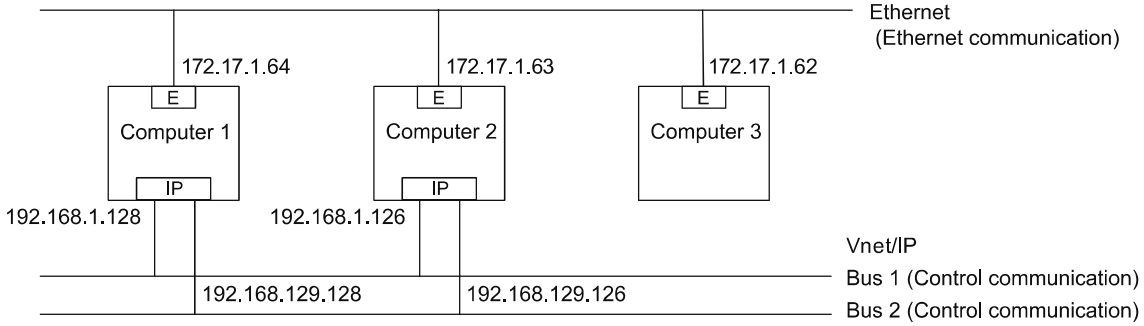
In this case, a combination of either control bus communications and Ethernet communications or control bus communications and Vnet/IP open communications is used. Configure the Windows network settings according to the network configuration of the system.

TIP The Vnet/IP open communication refers to Ethernet communication performed on bus 2 of Vnet/IP.

In a system using Vnet/IP open communications, bus 1 is normally used for control bus communications and bus 2 is used for Ethernet communications. If bus 1 fails, bus 2 is used for both control bus communications and Ethernet communications.

Vnet/IP Network Configurations and Windows Network Settings

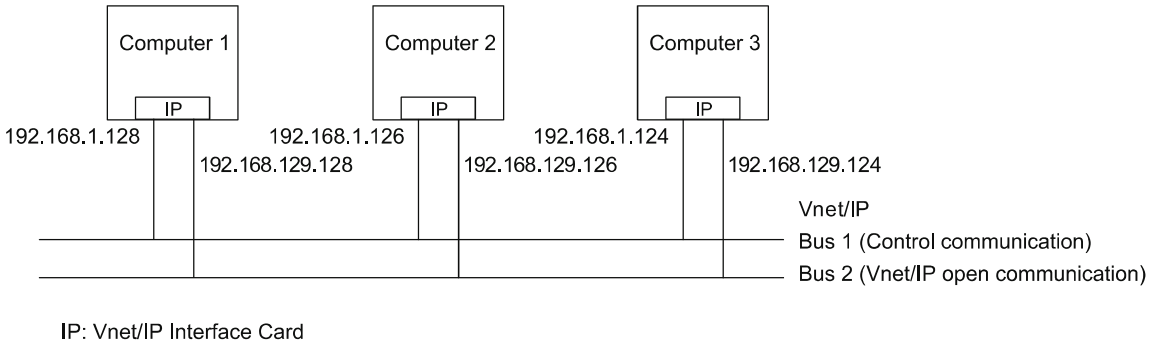
Vnet/IP network configurations and their required Windows network settings are describes as follows.



E: Ethernet Interface Card or Onboard NIC

IP: Vnet/IP Interface Card

Figure B3.3.5-1 Network Configuration and Interface (Vnet/IP and Ethernet are Installed)



IP: Vnet/IP Interface Card

Figure B3.3.5-2 Network Configuration and Interface (Only Vnet/IP is Installed)

Table B3.3.5-1 Network Configurations and Network Connections to be Set Up on Windows

Network Configuration	Computer (Example in the figures)	Network connection to be set up on Windows
Vnet/IP + Ethernet	Connected to Vnet/IP and Ethernet (Computers 1 and 2)	Control bus, Ethernet, and Vnet/IP open communications(*1)
	Connected to Ethernet only (Computer 3)	Ethernet communications
Vnet/IP only	Connected to Vnet/IP (Ethernet communication on bus 2) (Computers 1 to 3)	Control bus, Ethernet, and Vnet/IP open communications(*2)

*1: After installing the Vnet/IP open communication driver, you need to disable the corresponding device.
*2: You need to disable the Ethernet device.

SEE ALSO For more information about network construction when using Vnet/IP open communication, refer to:

Vnet/IP Network Construction Guide (Legacy Edition) (TI 30A10A10-01E)

Cautions on Using Vnet/IP

On the computers connected on Vnet/IP, you need to disable the unused devices according to the network configuration.

When Vnet/IP and Ethernet are Installed

IMPORTANT

In a system where both Vnet/IP and Ethernet are Installed, Vnet/IP open communications are not used. Even in this case, you need to install the Vnet/IP open communication driver and disable the driver on computers installed with a Vnet/IP interface card.

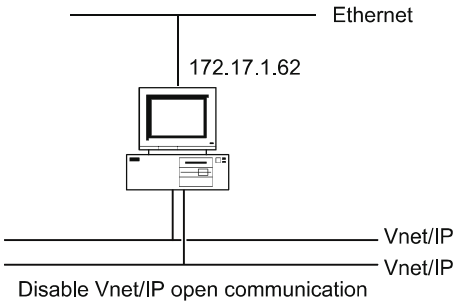


Figure B3.3.5-3 When Vnet/IP and Ethernet are Installed

On a computer installed with a Vnet/IP interface card, follow these steps to disable the Vnet/IP Open communication driver:

1. Log on as an administrative user.
2. Open the Control Panel.
3. Select [System and Security] > [System] > [Device Manager].
   Device Manager appears.
4. Unfold Network adapters.
5. Select [Vnet/IP Open Communication Driver (BUS2)] and then click the Disable button on the toolbar.

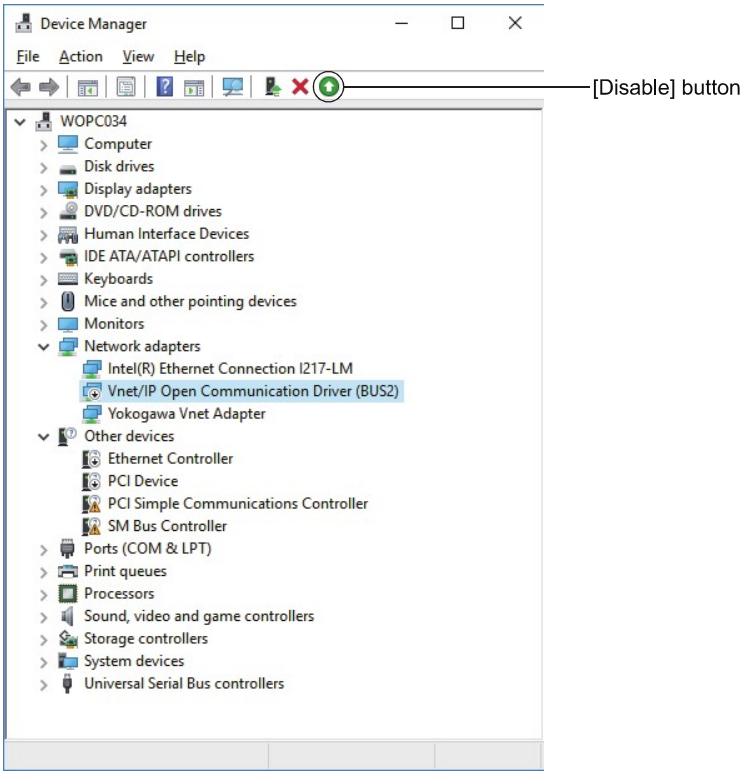


Figure B3.3.5-4 Disabling the Vnet/IP Open Communication Device

When Only Vnet/IP is Installed

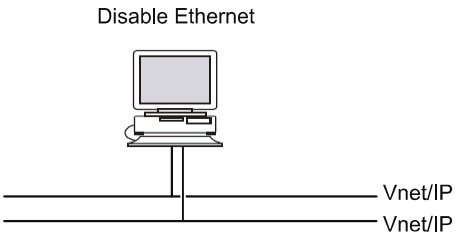


Figure B3.3.5-5 When Only Vnet/IP is Installed

On a computer in a system where only Vnet/IP is installed, follow these steps to disable the Ethernet device:

1. Log on as an administrative user.
2. Open the Control Panel.
3. Select [System and Security] > [System] > [Device Manager].
   Device Manager appears.

4. Unfold Network adapters.
5. Select the Ethernet device and then click the Disable button on the toolbar.

Prohibitions

Do not use the following features in ProSafe-RS.

- Internet Connection Sharing (ICS)
- Bridge Connection
- Homegroup

Internet Connection Sharing (ICS)

Do not select the [Allow other network users to connect through this computer's Internet connection] check box on the Sharing tab in the properties dialog box for V net, VnetIPOpen, or Ethernet (these connection names are set in the procedures described later).

TIP Internet Connection Sharing (ICS) is for sharing the internet connection by the computers in a small scale office network or home network.

Bridge Connection

Do not use bridge connection. If bridge connection is created in the computer, not only the control bus communication of the computer becomes abnormal, but also the communication of the whole control bus network may be jeopardized. (If the bridge connection is already created, you need to delete the bridge connection.)

Homegroup (Windows 10)

In a ProSafe-RS system, folders and printers are shared by using the file sharing function for the workgroup/network environment as with the earlier RS versions. For this reason, select [No] on the network charm bar.

Procedure 1: Rename Local Area Connections

A network after the installation is named "Local Area Connection." The network can be identified more easily if you rename the local area connection.

Rename the local area connections as necessary according to the network configuration of the system.

1. Open the Control Panel.
2. Select [Network and Internet] > [Network and Sharing Center].
   The Network and Sharing Center window appears.
3. Select [Change adapter settings].
   The Network Connections window appears.

TIP If connections are not displayed here, the corresponding installations have failed or the drivers are not working properly. Address the issues so that the connections are displayed here.

4. Right-click each of the Local Area Connection icons and select [Rename] to change the name.

Table B3.3.5-2 Renaming of Network Connections

Network type	Display on Network Connections window	Name
Ethernet	Ethernet driver names	Ethernet
Control bus	Yokogawa Vnet Adapter	Vnet
Vnet/IP open communication	Vnet/IP Open Communication Driver (BUS2)	VnetIPOpen

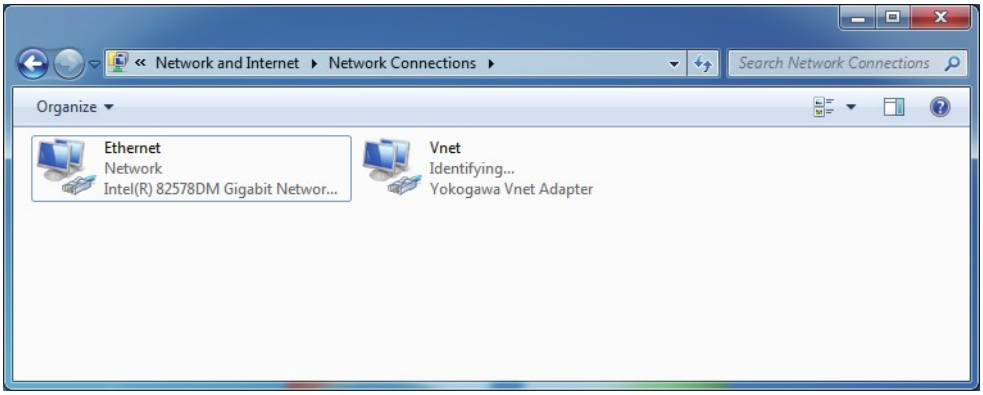


Figure B3.3.5-6 Network Connections – V net Network (After Renaming)

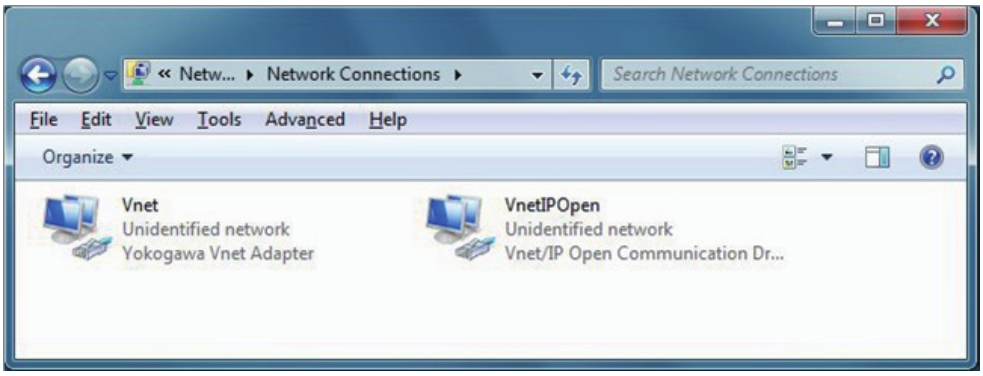


Figure B3.3.5-7 Network Connections – Vnet/IP Network (After Renaming)

TIP

In the instruction manuals until ProSafe-RS R2.03, it is instructed to change the name of control bus communication connection when Vnet/IP is used to “VnetIP” rather than “Vnet.”

SEE ALSO

For more information about the network settings for a virtual machine, refer to:

B3.4, “Notes on Using a Virtual Machine” on page B3-37

Procedure 2: Configure Properties

In the properties of each type of network connection, you need to configure the items to be used.

Configure the properties as necessary according to the network configuration of the system.

Table B3.3.5-3 List of Items Used for Network Connections

Item	Usage of the item (*1)		
	Ethernet	VnetIPOpen	Vnet
Client for Microsoft networks	Yes	Yes	No
QoS packet scheduler	Yes	Yes	No
File and printer sharing for Microsoft networks	Yes	Yes	No
Microsoft Network Adapter Multiplexor Protocol	No	No	No
Microsoft LLDP Protocol Driver	Yes	Yes	No
Yokogawa Vnet Protocol	No	No	Yes
Internet protocol version 6 (TCP/IPv6)	No	No	No
Internet protocol version 4 (TCP/IPv4)	Yes	Yes	Yes
Link-Layer Topology Discovery Mapper I/O Driver	Yes	Yes	No
Link-Layer Topology Discovery Responder	Yes	Yes	No

*1: Yes: Select the check box, No: Clear the check box

TIP

Items in the table, except “Yokogawa Vnet Protocol,” are installed during the Windows OS installation.

SEE ALSO

For more information about how to set the network adapters of the virtual machine, refer to:

“■ Configure Properties” on page B3-37

● V net Properties

1. In the Network Connections window, right-click [Vnet] and select [Properties].
   The Vnet Properties dialog box appears.
2. Configure Vnet according to “Table List of Items Used for Network Connections.”
3. After the setting is complete, click [OK].

● VnetIPOpen Properties

1. In the Network Connections window, right-click [VnetIPOpen] and select [Properties].
   The VnetIPOpen Properties dialog box appears.
2. Configure VnetIPOpen according to “Table List of Items Used for Network Connections.”
3. After the setting is complete, click [OK].

● Ethernet Properties

1. In the Network Connections window, right-click [Ethernet] and select [Properties].
   The Ethernet Properties dialog box appears.
2. Configure the Ethernet according to “Table List of Items Used for Network Connections.”
3. After the setting is complete, click [OK].

■ Procedure 3: Set IP Addresses

On Windows, DHCP is enabled by default after a network driver is installed. However, since ProSafe-RS does not use DHCP, you need to set IP addresses. You need to set IP addresses also when the system is used in the domain environment. Set the IP addresses according to the network configuration of the system.

SEE ALSO For more information about how to set IP addresses of the virtual machine, refer to:

"■ Set IP Addresses" on page B3-38

Setting IP Address for Vnet

1. In the Network Connections window, right-click the Vnet icon and select [Properties].
   The Vnet Properties dialog box appears.
2. Select [Internet Protocol Version 4 (TCP/Ipv4)] and click [Properties].
   The Internet Protocol Version 4(TCP/Ipv4) Properties dialog box appears.
3. Select [Use the following IP address] and set the IP address, subnet mask, and default gateway. Set the IP address to a standard value that is determined based on the station address of the computer as long as there is no special reason.

TIP The standard values for Vnet are as follows:

IP address:	172.16.Domain Number.Station Number(*1)
Subnet Mask:	255.255.0.0
Default gateway:	No setting is required.

*1: If the network address overlaps with the network address of the existing environment, you can use an address other than 172.16.

4. After the setting is complete, click [OK]. You do not need to restart the computer.

IP Address for VnetIPOpen

This setting is not required when Vnet/IP is used together with Ethernet.

1. In the Network Connections window, right-click the VnetIPOpen icon and select [Properties].
   The VnetIPOpen Properties dialog box appears.
2. Select [Internet Protocol Version 4 (TCP/IPv4)] and click the [Properties].
   The Internet Protocol Version 4 (TCP/IPv4) Properties dialog box appears.
3. Select [Use the following IP address] and specify the following values for the IP address, subnet mask, and default gateway.
   - If the computer is to be used in an existing environment, specify the values used in that network environment.
   - If the computer is to be used in a new environment, specify the standard values determined based on the station address.

TIP The standard values for VnetIPOpen are as follows:

IP address:	192.168.<128 + domain number>.<129 + station number>(*1)
Subnet Mask:	255.255.255.0
Default gateway:	Specify the IP address of L3SW if another Vnet/IP domain exists

*1: Normally, use a standard value. However, you can also use other address.

4. After the setting is complete, click [OK]. You do not need to restart the computer.

Setting IP Address for Ethernet

1. In the Network Connections window, right-click the Ethernet icon and select [Properties].
   The Ethernet Properties dialog box appears.
2. Select [Internet Protocol Version 4(TCP/IPv4)] and then click [Properties].

The Internet Protocol Version 4 (TCP/IPv4) Properties dialog box appears.

3. Select [Use the following IP address] and set the IP address, subnet mask, and default gateway for Ethernet as follows:
   - If the computer is to be used in an existing environment, specify the values used in that network environment.
   - If the computer is to be used in a new environment, specify the standard values determined based on the station address.

TIP

The standard values for Ethernet are as follows:

IP address:	172.17.Domain Number.Station Number(*1)
Subnet Mask:	255.255.0.0
Default gateway:	No setting is required.

*1: Normally, use a standard value. However, you can also use other address.

IMPORTANT

- In workgroup environment, do not change the settings for DNS server address and the settings accessed by clicking [Advanced].
- In Windows domain environment, you need to set the DNS server address according to the settings of Windows domain server.

4. After the setting is complete, click [OK]. You do not need to restart the computer.

Setup Procedure 4: Change Computer Name

It is recommended to set the station names used in the ProSafe-RS system as the computer names.

1. Open the Control Panel.
2. Select [System and Security] > [System] > [Advanced system settings].
   The System Properties dialog box appears.
3. In the Computer Name tab, click [Change].
   The Computer Name/Domain Changes dialog box appears.
4. Enter the station name as the new computer name (case-insensitive) for the computer.

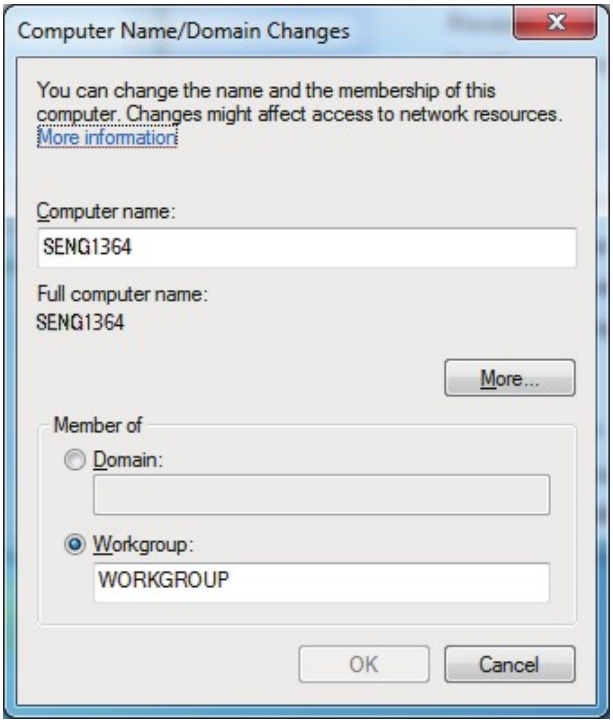


Figure B3.3.5-8 Computer Name/Domain Changes Dialog Box

5. Click [OK].
   A message box appears to prompt for restarting the computer.
6. Restart the computer.

Procedure 5: Repair TCP/IP Settings

Before you install the ProSafe-RS software, run the TCP/IP Inconsistency Detect Tool. If any inconsistency is found, use the TCP/IP Inconsistency Repair Tool and configure the TCP/IP settings again.

TIP

On a computer where the control bus driver or Vnet/IP open communication driver had ever been uninstalled, the TCP/IPv4 network settings of IP addresses, subnet masks, and default gateway addresses may be lost every time the computer is restarted. This problem is caused by errors of the Windows OS.

Running the TCP/IP Inconsistency Detect Tool

1. Use Windows Explorer to open the TOOLS directory under the following path in the ProSafe-RS software medium.
   `(Drive of ProSafe-RS software medium):\ProSafe-RS\TOOLS`

TIP

TCP/IP Inconsistency Detect Tool is installed in the following folder when you install the ProSafe-RS software:

`(ProSafe-RS Installation Folder)\ProSafe-RS\YOKOGAWA\net\tool`

2. Right-click [TcpipInconsistencyDetector.cmd], and select [Run as administrator] from the context menu.
   Messages are displayed according to the inconsistencies detected.
3. Click [OK] to end the tool.

If no inconsistency is detected, the computer can be connected on the network normally.

If no inconsistency is detected, the Windows system continues to work but the network connection may not. You need to use the TCP/IP Inconsistency Repair Tool and then configure the TCP/IP network settings again.

Running TCP/IP Inconsistency Repair Tool

IMPORTANT

TCP/IP Inconsistency Repair Tool resets the TCP/IP settings of all the network interface cards that are installed in the computer. Therefore, before you run the TCP/IP Inconsistency Repair Tool, you need to write down or save the current settings of the following TCP/IPv4 information for every network interface card:

- IP Address
- Subnet Mask
- Default Gateway

1. Use Windows Explorer to open the TOOLS directory under the following path in the ProSafe-RS software medium.
   `(Drive of ProSafe-RS software medium):\ProSafe-RS\TOOLS`

TIP

TCP/IP Inconsistency Repair Tool is installed in the following folder when you install the ProSafe-RS software:

`(ProSafe-RS Installation Folder)\ProSafe-RS\YOKOGAWA\net\tool`

2. Right-click [TcpipInconsistencyRepair.cmd], and select [Run as administrator] from the context menu.
   Messages are displayed according to the inconsistencies detected.
3. If no inconsistency is detected in the network settings, click [OK] to end the tool.
   The computer can be connected on the network normally.
4. If any inconsistency is detected, click [Yes]
   The network settings are reset and a message appears, prompting you to restart the computer.
5. Click [Yes] to restart the computer.
6. After the computer is restarted, re-configure the settings on the Internet Protocol Version 4 (TCP/IPv4) Properties windows for all the network interface cards.

B3.4 Notes on Using a Virtual Machine

When using a virtual machine, in addition to the control bus and Ethernet, you must configure the control network (Vnet/IP) and the remote UI network settings.

Rename Local Area Connections

Set the name of the local area connection of the virtual machine as follows.

Table B3.4-1 Renaming of Network Connections

Network type	Display on Network Connections window (*1)	Name
Control bus	Yokogawa Vnet Adapter	Vnet
Ethernet	Microsoft Hyper-V Network Adapter #n	Ethernet
Control network 1	Microsoft Hyper-V Network Adapter #n	VnetIPBUS1 (*2)
Control network 2	Microsoft Hyper-V Network Adapter #n	VnetIPBUS2 (*2)
Remote UI network	Microsoft Hyper-V Network Adapter #n	RemoteUINetwork

*1: These are the default names, where n = 1, 2, ..., which means the virtual NIC number.
*2: Be sure to set these names. The names are not case-sensitive.

Confirming the Network Type

Follow these steps to confirm the network type:

1. In the Network Connections window, right-click on a network and select [Properties].
2. Open the Network tab, and click [Configure].
3. Open the Advanced tab and confirm the Value that is displayed when you select Hyper-V Network Adapter Name in Properties.
   The device name that was set when the virtual machine was built is displayed.

TIP

For the Value that you confirm in the step 3, contact to the engineer who configured the virtual machine.

Configure Properties

In the properties of each type of network connection, you need to configure the items to be used. Configure the properties as shown in the following table.

Table B3.4-2 List of Items Used for Network Connections

Item	Usage of the item (*1)				
	Control bus	Ethernet	Control network 1	Control network 2	Remote UI network
Client for Microsoft Networks	No	Yes	No	No	Yes
QoS Packet Scheduler	No	Yes	No	No	Yes
File and Printer Sharing for Microsoft Networks	No	Yes	No	No	No
Microsoft Network Adapter Multiplexor Protocol	No	No	No	No	No
Microsoft LLDP Protocol Driver	No	Yes	No	No	Yes
Yokogawa Vnet Protocol	Yes (*2)	No	No	No	No
Internet protocol version 6 (TCP/IPv6)	No	No	No	No	No
Internet protocol version 4 (TCP/IPv4)	Yes	Yes	Yes	Yes	Yes
Link-Layer Topology Discovery Mapper I/O Driver	No	Yes	No	No	Yes

Continues on the next page

Table B3.4-2 List of Items Used for Network Connections (Table continued)

Item	Usage of the item (*1)				
	Control bus	Ethernet	Control network 1	Control network 2	Remote UI network
Link-Layer Topology Discovery Responder	No	Yes	No	No	Yes

*1: Yes: Select the check box, No: Clear the check box
*2: Do not clear the check box for “Yokogawa Vnet Protocol.”

Set IP Addresses

You do not need to set the IP address, subnet mask, and default gateway for the control network. They are automatically set by the Vnet/IP Interface Management Tool based on the settings values of the domain number and station number managed by the Vnet/IP Interface Package.

For the control bus, Ethernet, and remote UI network, it is recommended to set the IP address, subnet mask, and default gateway to the following values.

Table B3.4-3 IP Address

	Control bus	Ethernet	Remote UI network
IP Address	172.16. Domain number. Station number	172.17. Domain number. Station number	172.18. Domain number. Station number
Subnet Mask	255.255.0.0	255.255.0.0	255.255.0.0
Default gateway	No setting is required.	No setting is required.	No setting is required.

If the existing environment and network addresses overlap, IP addresses other than the recommended values can be used for the control bus, Ethernet, and remote UI network. However, you cannot set the address 192.168.xx.yy to the IP address of the control bus, Ethernet, or remote UI network. If you do, communication to the control network is impossible.

B3.5 Installing the ProSafe-RS Software

This section describes how to install the ProSafe-RS software.

Administrative User who Performs New Installation

When installing the ProSafe-RS software for the first time on a computer, the installation must be performed by an administrative user who belongs to the group shown in the following table.

The user who has installed the software is automatically added to the PSF_MAINTENANCE group.

IMPORTANT

- The initial password is set by default for the predefined user accounts in this product. Be sure to change the password because operating with the initial password may increase the security risk.
- If SOE OPC Interface Package is used, be sure to change the PSF_PROCESS password after configuring IT security settings. If you changed the password before configuring IT security settings, reset the password that you set.
- If you are going to change the initial password of PSF_PROCESS in an environment that AD Suite is used, activate the system project backup function with ADS Administration Tool before you change the password. If you change the password before activating the system project backup function, the [Backup System Projects prior to AD Project Export] check box in the ADS Administration Tool appears dimmed and you cannot select it. In that case, change the initial password of PSF_PROCESS after activating the system project backup function.
- When changing the password, ensure that the same password is set in the entire system.

Table B3.5-1 Groups to Which the User Who Performs New Installation Belongs

Security model and user management type to be applied		
Legacy model	Standard model	
	Standalone management/linked domain management	Domain/Combination management
Local user who belongs to the Administrators local group	Local user who belongs to the Administrators local group	• Domain user who belongs to the Domain Admins domain group • Domain user who belongs to the Administrators local group • Local user who belongs to the Administrators local group(*1) (*2)

*1: The domain user name and password must be entered during installation.
*2: When this user applies IT security and uses iDefine interface package, the following steps must be performed as a domain user who belongs to the Domain Admins domain group or as a domain user who belongs to the Administrators local group.
1. Run the 32 bit Command Prompt (%SystemDrive%\Windows\SysWOW64\cmd.exe) as Administrator.
2. Run either of the following batch files appropriate to the user management type.
%ProgramFiles(x86)%\YOKOGAWA\IA\iPCS\Platform\Security\Program
For Domain management: PSF_SetupSMSvcHostConfigDOM.cmd
For Combination management: PSF_SetupSMSvcHostConfigCMB.cmd

TIP

If the user management type is Domain or Combination management, install the software after the computer is added to the domain.

SEE ALSO For more information about user accounts that require password change, refer to:

2.2.3, “User/Group Management” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

Installation Procedure

Follow these steps to install the ProSafe-RS software:

1. Log on as an administrative user.
2. Terminate all running applications, including resident programs such as anti-virus software.
3. Insert the ProSafe-RS software medium into the drive.
   - If the AutoPlay dialog box appears, click [Run Launcher.exe].
   - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the ProSafe-RS software medium.

   The installation menu appears.

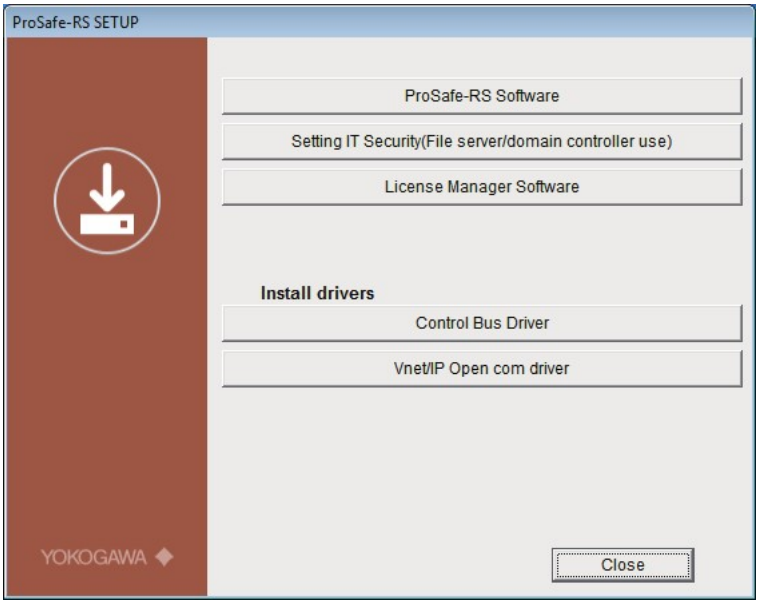


Figure B3.5-1 Installation Menu

4. Click [ProSafe-RS Software] in the installation menu.
5. If a dialog box appears, confirming to install Windows redistributable modules, click [Install].

TIP This dialog box appears when the Windows redistributable modules required to run ProSafe-RS are not already installed.

The following modules are necessary for ProSafe-RS:

- Microsoft .NET Framework 4.8
- Microsoft Visual C++ 2017 Redistributable Package
- Microsoft Access Database Engine 2016

If you click [Cancel], the installation of the ProSafe-RS software is discontinued.

Restarting the computer may be required after installing the modules. If required, restart the computer and then continue the ProSafe-RS installation.

Installation starts.

6. After the installation is completed, click [Close].
   The window closes.

IMPORTANT

If Microsoft Access Database Engine 2016 cannot be installed due to cancellation during installation of the redistributable module, an error occurs. In that case, click [OK]. To continue the installation, install ProSafe-RS again.

7. If the following dialog box appears, restart the computer and log on again using the same user account.



Figure B3.5-2 User Rights Setting Confirmation Dialog Box

TIP

Restarting the computer here grants the currently logged on user the rights required to perform the subsequent installation tasks.

Installation of the ProSafe-RS software starts and the Welcome dialog box appears.

8. Click [Next].
   A dialog box for entering user information and the installation folder appears.

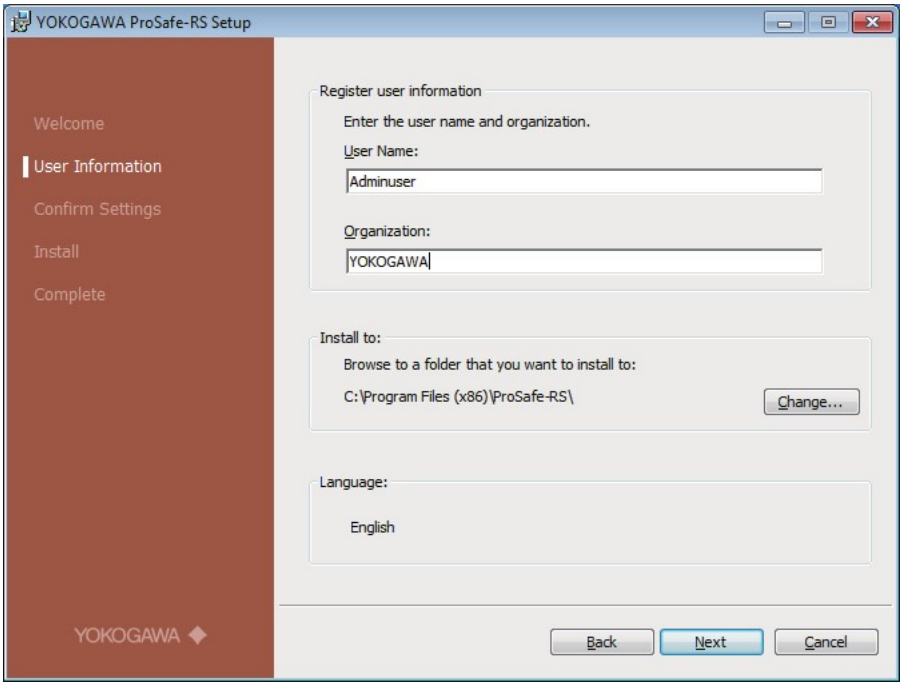


Figure B3.5-3 User Information Dialog Box

TIP

- If a different version of control bus driver or Vnet/IP open communication driver is already installed, a dialog box appears, prompting you to update the driver. Confirm the message and click [OK]. To update the control bus driver, uninstall the existing driver and then install the new one after you install the ProSafe-RS software. To update the Vnet/IP open communication driver, install the new driver after you install the ProSafe-RS software.
- After updating the Vnet/IP open communication driver, disable the driver if the computer is to be connected to Ethernet.

9. Enter the user name and company name. It is recommended not to change the installation folder from the default location.

TIP

- The user name and company name must be set within 100 characters.
- If you want to change the installation folder, click [Browse] and specify a new location within 50 characters.
- The language is determined automatically by the system language: if the system language is Japanese, the Japanese version software is installed, otherwise, the an English version is installed.

10. Click [Next].
    The Confirm Settings dialog box appears.
11. Confirm that the installation settings are correct, and click [Install].
    Installation of the ProSafe-RS software is started.
12. When the installation complete dialog box appears, perform either of the following operations.
    - If you install only ProSafe-RS, select [Yes, I want to set up IT security now.] and click [Finish]. The IT Security Tool then starts.
    - If you install another YOKOGAWA product, select [No, I want to install other software products.] and click [Finish] to complete the installation.

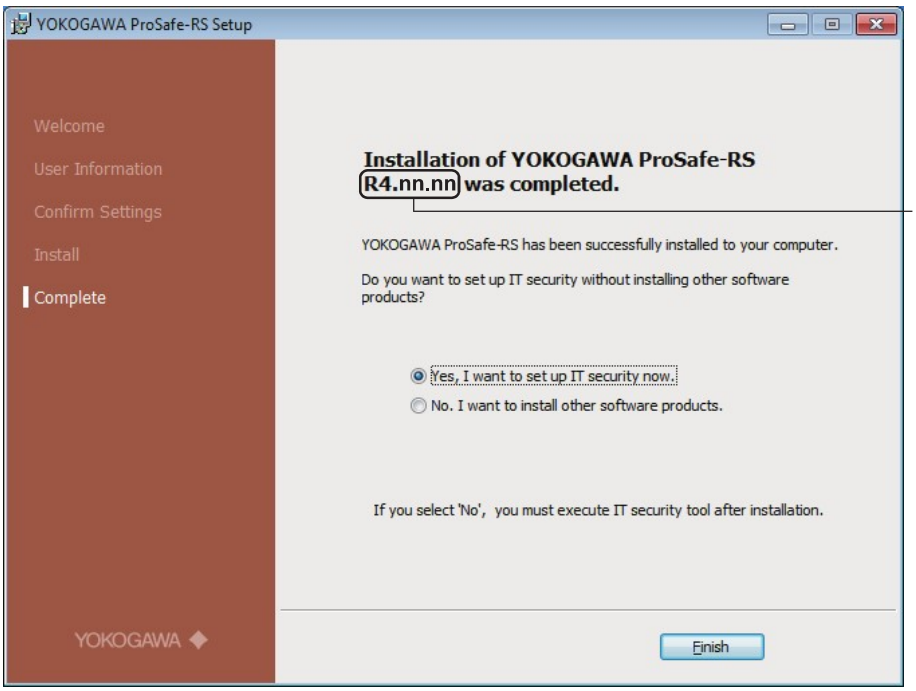


Figure B3.5-4 Installation Completed Dialog Box

IMPORTANT

After you have installed other YOKOGAWA products, be sure to run the IT Security Tool to configure IT security settings. The settings on the IT Security Tool will be valid to all the installed products.

If you do not configure IT security settings, the products will not function properly.

SEE ALSO For more information about configuring the IT security settings, refer to:

B3.6, “Configuring IT Security Settings” on page B3-44

B3.6 Configuring IT Security Settings

After installing the ProSafe-RS software, you need to configure settings to strengthen Windows IT security.

To configure IT security for linked domain management, use IT Security Tool and Domain Link Management Tool. For user management types other than linked domain management, use IT Security Tool to configure IT security settings.

IMPORTANT

- The initial password is set by default for the predefined user accounts in this product. Be sure to change the password because operating with the initial password may increase the security risk.
- The security model of IT security settings must be consistent in the entire system. Ensure that the user management type is unified to either standalone management or management using a domain controller. You can mix computers in domain management, combination management, or linked domain management.
- If you select the Legacy model, restrictions related to Windows are in effect in some environments. For that reason, we recommend you select the Standard model.
- If you operate the computer in the Standard model with linked domain management, apply IT security settings for the Standard model with standalone management. Next, join the computer to the domain and set with Domain Link Management Tool.
- If the computer contains YOKOGAWA products that do not support linked domain management and you use the installed YOKOGAWA product in a domain environment, set the user management type to domain management or combination management with IT Security Tool.
- If you have changed any security settings from their default values, always save the security settings by using the Save function of the IT Security Tool to enable security settings to be restored at computer failure.
- After you have activated the license of the SOE OPC Interface Package, be sure to run the IT Security Tool from the Start menu.
- Security settings customized by other than the IT Security Tool are overwritten with the setting information held by the IT Security Tool when the IT Security Tool is run. If you want to use the same security settings as before running the IT Security Tool, customize them again after running the IT Security Tool.

  Note that upgrading will run the IT Security Tool and overwrite the security settings.

TIP

Even when a domain controller is used to perform consolidated management of IT security settings, be sure to set IT security on each client. After setting IT security on all clients, use the domain controller to set up consolidated management of IT security settings.

SEE ALSO

For more information about precautions for coexistence with other YOKOGAWA product, refer to:

B3.6.2, “Precautions for Coexistence with Other Product” on page B3-51

For more information about user accounts that require password change, refer to:

2.2.3, “User/Group Management” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

For more information about details of the IT security settings, refer to:

6.1, “IT Security Tool” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

For more information about the procedure for performing consolidated management of IT security settings with a domain controller, refer to:

6.10, “Active Directory-Based Consolidated Management of IT Security Settings” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

B3.6.1 Running the IT Security Tool

This section describes the procedure for configuring the IT security settings following the completion of ProSafe-RS software installation.

IMPORTANT

If the following YOKOGAWA products have been installed and they do not support IT security version 2.0, the selection of IT security version 1.0 cannot be changed.

- CENTUM VP
- PRM

If they support IT security version 2.0, the IT security version can be kept or changed.

Follow these steps to run the IT Security Tool:

1. When the ProSafe-RS software installation is complete, a dialog box appears. Select [Yes, I want to set up IT security now.] and click [Finish].

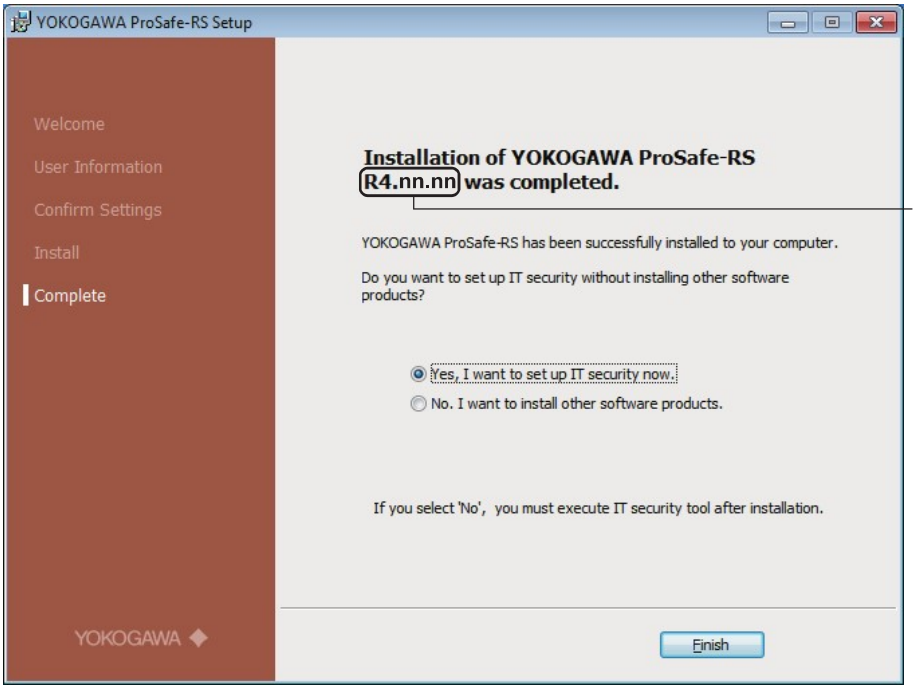
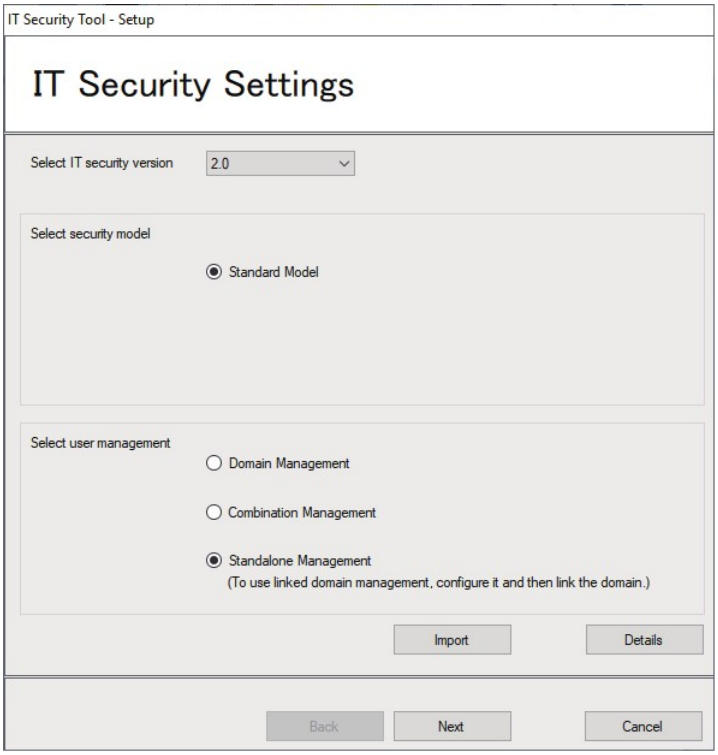


Figure B3.6.1-1 ProSafe-RS Setup Dialog Box (Completed)

The IT Security Tool starts.

TIP

If you are intending to select [No, I want to install other software products.] after the completion of installation, install other software products, and then run the IT Security Tool, start the IT Security Tool from the Start menu and click [Settings] on the menu.



TIP

The text To use linked domain management, configure it and then link the domain below Standalone Management is displayed when all of YOKOGAWA system products installed on the computer support the linked domain management.

Figure B3.6.1-2 IT Security Tool (Setup)

2. From the Select IT security version drop-down list, select the IT security version.
3. In the Select security model section, select either [Standard Model] or [Legacy Model].

TIP

If you select [2.0] for Select IT security version, only the [Standard model] can be selected.

4. In the Select user management section, select [Domain Management], [Combination Management], or [Standalone Management].

TIP

- When you select the Legacy model, you cannot change the user management type from Standalone management.
- When operating with linked domain management, select the standalone management in the Standard model.
- If you select [Standalone Management] on a Windows domain member computer, a confirmation message is displayed. You can go on by clicking [OK].

5. If you do not need to configure the individual setting items, click [Next]. IT security setting starts. When the setup is complete, the Setup Completed page appears. If there is any setting items that have failed, the failed items are displayed. To reconfigure the individual setting items, perform the following steps.

TIP

If IT security version 2.0 is selected, a confirmation dialog box appears. To apply the current settings, click [Yes].

a. To reconfigure the individual setting items, click [Details].
The Select Setting Items page appears.

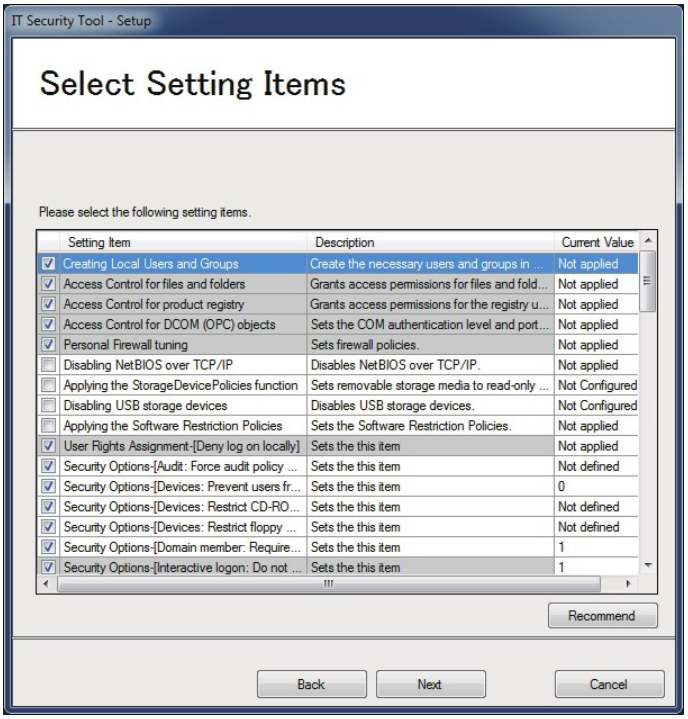


Figure B3.6.1-3 Select Setting Items Page (When IT Security Version 2.0 Is Selected)

b. Select or clear the check boxes of the items you want to change.
Under [Current Value], the value currently set for the applicable setting item is displayed according to the following table.

IMPORTANT

The group policy settings that were distributed from the domain controller are not displayed. Local group policy settings are displayed.

Table B3.6.1-1 Content displayed in Current Value

Content displayed	Description
Actual value	The value actually set is displayed. For example, Enabled, Disabled, 30, 0, etc., is displayed. (*1)
[Not defined]	This is displayed for a setting item relating to security options, for which no value is set.
[Not configured]	This is displayed for a setting item for the group policy management template, for which no value is set.
[Not applied]	This is displayed for a setting item that takes multiple values, for which IT security has never been applied.
[Applied]	This is displayed for a setting item that takes multiple values, for which IT security has been applied at least once.

*1: Even when the set value is a character string in the Security Policy window, it may be managed as a value in the OS, in which case the value is displayed.

TIP It is recommended not to change the settings when the Standard model is selected.

c. Click [Next].
The Confirm Setting Information page appears.

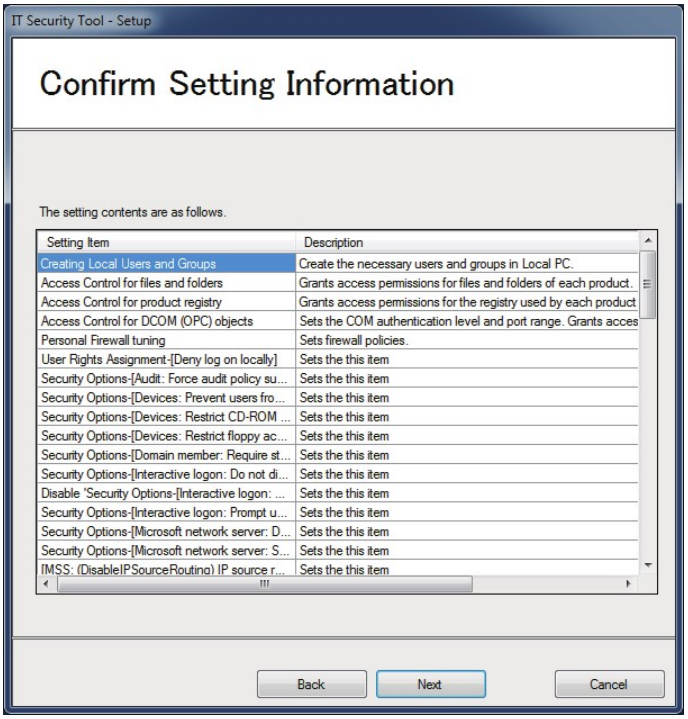


Figure B3.6.1-4 Confirm Setting Information Page (When IT Security Version 2.0 Is Selected)

TIP

If the settings specified are different from the default values of the security model, a warning dialog box appears.

To apply the current settings, click [Yes]. If you click [No], you will return to the Select Setting Items page.

d. Confirm the settings and click [Next].

TIP

If this tool was used in the past to configure security settings without opening the Select Setting Items page, the last configured IT security settings are applied. If these settings and the default settings of the selected security model do not match, a warning dialog box appears.

To apply the current settings, click [Yes]. If you click [No], you will return to the IT Security Settings page.

When the setup is complete, the Setup Completed page appears. If there is any setting items that have failed, the failed items are displayed.

6. Select the [Restart now] check box and click [Finish].
   The IT Security Tool is exited and the computer is restarted automatically.

IMPORTANT

If any setup failures are displayed, contact YOKOGAWA Service.

TIP

The "Program Compatibility Assistant" dialog box may appear after the security settings configuration is completed. Even when this dialog box appears, the settings have been configured successfully, so click [Cancel] to close it.

SEE ALSO For more information about the procedure for importing the IT security settings, refer to:

6.8, “Exporting/Importing the IT Security Setting File” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

For more information about changing the IT security settings, refer to:

6.4, “Changing the IT Security Settings” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

Notes on the Case when NetBIOS over TCP/IP is Disabled

When the Standard model is selected, you can configure to disable NetBIOS over TCP/IP. With domain management, combination management, or linked domain management, NetBIOS over TCP/IP is disabled by default.

If it is disabled, you need to make the following settings for name solution.

- Standalone management
  In the LMHOSTS file of each station, set the computer names of the stations it needs to access.

  Location of the LMHOSTS file: `%Systemroot%\system32\drivers\etc`

  %Systemroot% is the directory where the Windows OS is installed. Usually, it is `C:\Windows`.

  Example script in the LMHOSTS file: The following is an example of accessing HIS0124.

```
########## lmhosts
172.17.1.24 HIS0124 #PRE
```

Table B3.6.1-2 LMHOSTS File Settings

Station type	Stations to be set in the LMHOSTS file
License management station	All license-assigned stations
License-assigned station	• License management station • Computer that holds project files (File server computer; if integrated with CENTUM, computer that holds CENTUM project database) • To use the Forced I/O Viewer function, the computer on which SCS projects are saved and the computer which receives the distribution.

- Domain management, combination management, or linked domain management
  In the DNS server, set the license management station and all the license-assigned stations.

B3.6.2 Precautions for Coexistence with Other Product

Precautions to be heeded when a YOKOGAWA product that supports IT security settings co-exists on a ProSafe-RS computer are explained.

Installing the ProSafe-RS Software After Installing Other Product

When installing the ProSafe-RS software after installing other product that does not support IT security version 2.0, only IT security version 1.0 can be selected.

When installing the ProSafe-RS software after installing other product that supports IT security version 2.0, the IT security version can be kept or changed.

Installing Other Product After Installing the ProSafe-RS Software

If IT security Version 2.0 is set during the installation of the ProSafe-RS software and then IT security settings are configured during the installation of other product that does not support IT security version 2.0, the following warning dialog box will appear.

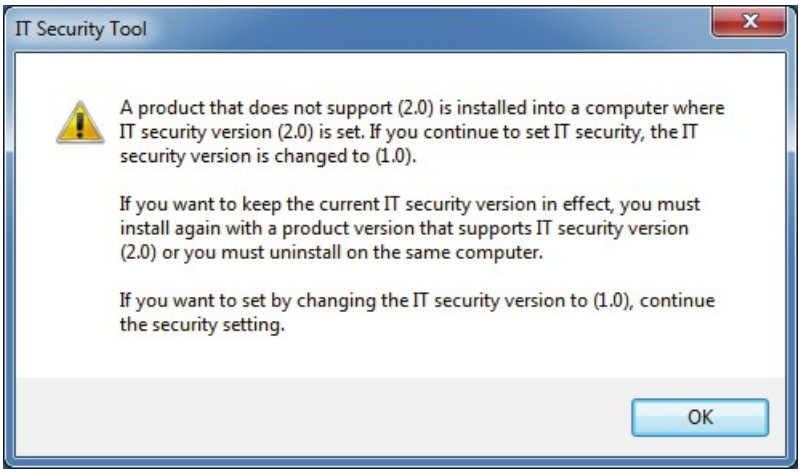


Figure B3.6.2-1 Warning Dialog Box

When changing to IT security version 1.0, continue configuring the IT security settings.

When changing to IT security version 2.0, close the IT security tool and uninstall other products, then re-install other products that are compatible with IT security version 2.0.

B3.6.3 Running Domain Link Management Tool

To configure IT security for linked domain management, use Domain Link Management Tool.

Adding the corresponding domain group to the members of the local group for the product installed on the computer by using the Domain Link Management Tool is called linking the domain. Conversely, deleting the domain group from the members of the local group is called unlinking the domain.

IMPORTANT

- The domain can be linked if the following conditions are met.
  - All of YOKOGAWA system products installed on the computer support the linked domain management.
  - The IT security settings for standalone management are applied to the installed products with IT Security Tool.
  - The computer is added to the Domain.
- You can link or unlink the domain for all of YOKOGAWA system products installed on the computer at once.
- If you install another YOKOGAWA system products after linking domains, you must configure security with IT Security Tool and link the domain. The same applies to upgrading the revision or the version of the installed products.

SEE ALSO

For more information about how to add client computers to the domain, refer to:

B2.5, “Adding Computers to the Domain” on page B2-17

For more information about notes on the case when NetBIOS over TCP/IP is disabled, refer to:

“■ Notes on the Case when NetBIOS over TCP/IP is Disabled” on page B3-50

For more information about IT Security Tool, refer to:

6.1, “IT Security Tool” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

For more information about Domain Link Management Tool, refer to:

6.2, “Domain Link Management Tool” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

■ Linking the domain with Domain Link Management Tool

Follow these steps to link the domain:

1. Sign in as a local user who belongs to both the Administrators group and PSF_MAINTENANCE group of the local computer.
2. Start Domain Link Management Tool.

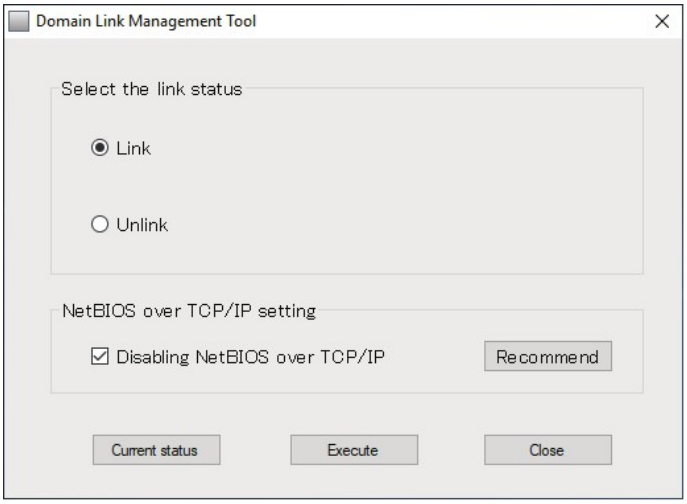


Figure B3.6.3-1 Domain Link Management Tool

3. In Domain Link Management Tool, select [Link] in the Select the link status section.
4. To change the recommended settings of NetBIOS over TCP/IP setting, perform the following step.
   Clear the [Disabling NetBIOS over TCP/IP] check box.

TIP

If the security model is set to Standard model with IT Security Tool, the setting of the Disabling NetBIOS over TCP/IP check box is switched to the recommended settings in conjunction with the settings of the Select the link status.

5. In Domain Link Management Tool, click [Execute].
   The domain user authentication dialog box appears.
6. Enter the user name and password of the domain user and click [OK].
   The corresponding domain group is added to the member of the local groups related to the products installed on your computer. Also, NetBIOS over TCP/IP setting is configured.

TIP

The user name and password that you enter in the domain user authentication dialog box do not have to be those of the domain administrator.

7. In Domain Link Management Tool, click [Close].
   The Domain Link Management Tool closes.

Error messages and countermeasures

When attempting to link the domain, an error message will be displayed and the process will not be performed depending on the conditions. Check the current status of the products installed on the computer and take necessary measures.

The following table describes the error messages and countermeasures when you cannot run the process for linking domain.

Table B3.6.3-1 Error messages and countermeasures

the error messages	Remedy
The computer is not joined to the domain.	Join the computer to the domain.
This account information you entered is incorrect.	Domain user authentication has failed. Enter the correct account information.

Continues on the next page

Table B3.6.3-1 Error messages and countermeasures (Table continued)

the error messages	Remedy
Any products that support linked domain management are not installed. (*1)	All of YOKOGAWA system products installed on the computer must support the linked domain management. Perform either of the following measures: • Change the user management type to domain management or combination management. • Uninstall the products that do not support linked domain management and link the domain.
The products that do not support linked domain management are installed.	
IT security is not configured. (*1)	With IT Security Tool, apply the security settings for standalone management.
Linked domain management is not to be configured for the Legacy model computer.	Change to Standard model with standalone management.
Standalone management is not applied.	Change the user management type to standalone management.
Failed to connect to the domain controller.	Check the network settings and cabling between the computer and domain controller.
The group required for linked domain management does not exist in the domain.	Create necessary domain group.

*1: This error does not occur in Domain Link Management Tool for File Server.

SEE ALSO

For more information about how to add client computers to the domain, refer to:

B2.5, “Adding Computers to the Domain” on page B2-17

For more information about installation of the product, refer to:

B3.5, “Installing the ProSafe-RS Software” on page B3-39

For more information about configuring network settings, refer to:

B3.3, “Configuring Network Settings” on page B3-18

For more information about how to create domain groups, refer to:

- B2.3, “Configuring Security Settings for the Domain Controller” on page B2-6
- B2.4, “Creating Domain Users” on page B2-13

For more information about how to configure IT security settings with IT Security Tool for the first time, refer to:

B3.6.1, “Running the IT Security Tool” on page B3-46

For more information about the procedure for displaying the current status with Domain Link Management Tool, refer to:

6.2, “Domain Link Management Tool” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

For more information about the procedure for changing the IT security settings, refer to:

6.4, “Changing the IT Security Settings” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

B3.7 Distributing and Accepting Licenses

Licenses are the rights to use ProSafe-RS software packages.

To make the installed software packages available for use, you need to distribute the licenses from the license management station to license-assigned stations and accept the licenses on each license-assigned station. This process of making software packages available for use is called “activation of software packages.”

In a ProSafe-RS system, there is always one license management station and other stations are license-assigned stations. The license management station can be set up on a computer where SENG runs.

SEE ALSO For more information about distributing and accepting licenses, refer to:

1., “Overview of license management” in License Management Guide (IM 32P01C60-01EN)

B3.8 Creating User Accounts

Create accounts for ProSafe-RS.

When the Standard model is selected in IT security configuration, rights to access the installation folder, registries, etc. are set by the IT Security Tool, based on the access rights granted to the ProSafe-RS user groups. Therefore, you need to register the created user as a member of the appropriate ProSafe-RS user group according to the user's role, such as engineer and maintenance personnel.

This section describes the procedures for the cases where the security settings of the Standard model with Standalone management or the Legacy model are applied.

When you create local user accounts for Standard model with linked domain management, domain management, and combination management, create them in the same way as for Standard model with standalone management. When you create domain user accounts for Standard model with linked domain management, domain management, and combination management, create them on the domain controller.

SEE ALSO For more information about how to create domain user accounts, refer to:

B2.4, “Creating Domain Users” on page B2-13

■ Limitation on User Account Names

- 20 characters at maximum.
- Space, tabs, and multi-byte characters such as half-width katakana and Chinese characters (kanji) cannot be used.

TIP When the Access Control and Operation History Management Package is used and Windows authentication mode is specified, different limitations are applied.

SEE ALSO For more information about the limitations on user account names when using Windows authentication mode of the Access Control and Operation History Management Package, refer to:

“■ Creating User Accounts in Windows Authentication Mode” on page B4-8

B3.8.1 When the Standard Model with Standalone Management Security Settings are Applied

When the security settings of Standard model with Standalone management are applied, user accounts should be created on each computer.

Follow these steps to create a user account:

1. Logon as an administrative user.
2. Open the Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Computer Management].
   The Computer Management window appears.
4. On the tree view in the left pane of the window, select [System Tools] > [Local Users and Groups] > [Users].
5. Select [Action] > [New User].
   The New User dialog box appears.
6. Add a user account. (The rest of the steps shows an example of adding a new user account, OPERATOR.)
7. Right-click the user you have created and select [Properties], and then click [Add] on the Member of tab.
8. Select an appropriate user group for the created user and click [OK].

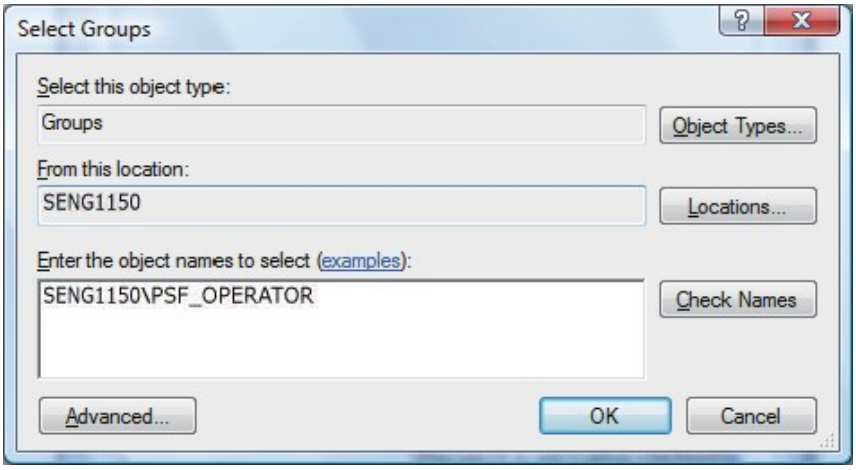


Figure B3.8.1-1 Select Groups

TIP

A user who belongs to the administrative group (PSF_MAINTENANCE) must also be a member of the Administrators group.

9. In the user properties dialog box, confirm that the group you selected has been added to the Member of list.

B3.8.2 When the Legacy Model of Security Settings are Applied

The procedure for creating user accounts is the same as that for creating user accounts on a Standalone management computer. However, with the Legacy model, Windows groups PSF_xxxx are not supported. So, there is no need to add the created users to these groups.

SEE ALSO For more information about creating user accounts, refer to:

B3.8.1, “When the Standard Model with Standalone Management Security Settings are Applied” on page B3-57

B3.9 Configuring Windows Environment Settings for Each User

After creating user accounts, configure the required Windows environment settings for each user.

B3.9.1 Setting of Items Common to Windows 10, Windows Server 2016, Windows Server 2019, and Windows Server 2022

This section describes how to set the items common to Windows 10, Windows Server 2016, Windows Server 2019, and Windows Server 2022.

Showing Icons on the Task Tray

On license-assigned stations, you must set so that the License Agent icon is always shown on the task tray.

1. Sign in using the user account for which the License Agent icon should be displayed.
2. Open the Control Panel.
3. From the menu, select [Appearance and Personalization] > [Taskbar and Navigation]. The Settings window appears.
4. Under [Notification area], select [Select which icons appear on the taskbar].
5. Set [Always show all icons in the notification area] to [Off], and set [License.Agent.Task-Tray] to [On].
6. Click the [×] button to close the window.

Display Properties

The procedure for setting the display properties is explained as follows.

1. Sign in using the user account for which to set display properties.
2. From the Start menu, display the Windows Settings window.
3. Click [Personalization].
4. Click [Themes], and on Apply a theme, select [Windows].
5. Click [Background], select [Solid color] from the Background drop-down list, and select a desired background color.
6. Click [Lock screen] > [Screen saver settings].
   The Screen Saver Settings dialog box appears.
7. From the Screen Saver drop-down list, select [(None)], and then click [OK].
8. Click the [×] button to close the window.

Stopping the Inactive Window Scrolling Function (Windows 10)

Stop the function to scroll the inactive windows with the mouse wheel as it can cause mal-functions.

Follow these steps to stop the inactive window scrolling function:

1. Sign in with the user account for which to disable scrolling of inactive windows.
2. Start the Windows Settings window.
3. Select [Devices].
   The rest of the operation differs depending on the OS.
   - If the OS is Windows 10 Enterprise 2016 LTSB, perform steps 4 through 6.
   - If the OS is Windows 10 Enterprise LTSC 2019, perform steps 7 through 9.
   - If the OS is Windows 10 Enterprise LTSC 2021, perform steps 10 through 12.

4. In the left pane, select [Mouse & touchpad].
   The Mouse page appears.

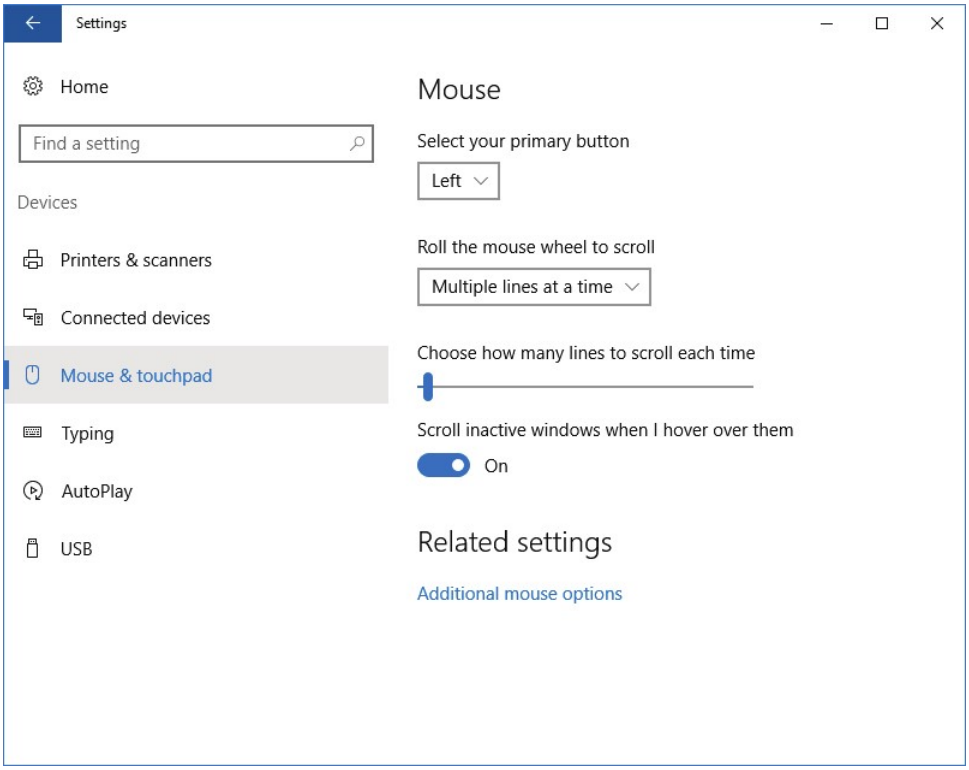


Figure B3.9.1-1 Mouse Page

5. Turn off [Scroll inactive windows when I hover over them].
6. Click the [×] button to close the window.
7. In the left pane, select [Mouse].
   The Mouse page appears.
8. Turn off [Scroll inactive windows when I hover over them].
9. Click the [×] button to close the window.
10. In the left pane, select [Mouse].
    The Mouse page appears.
11. Turn off [Scroll inactive windows when I hover over them].
12. Click the [×] button to close the window.

Stopping the Inactive Window Scrolling Function (Windows Server)

Stop the function to scroll the inactive windows with the mouse wheel as it can cause malfunctions.

Follow these steps to stop the inactive window scrolling function:

1. Sign in with the user account for which to disable scrolling of inactive windows.
2. Start the Windows Settings window.
3. Select [Devices].
   The rest of the operation differs depending on the OS.
   - If the OS is Windows Server 2016 or Windows Server 2019, perform steps 4 through 6.

- If the OS is Windows Server 2022, perform steps 7 through 9.

4. In the left pane, select [Mouse & touchpad].
   The Mouse page appears.

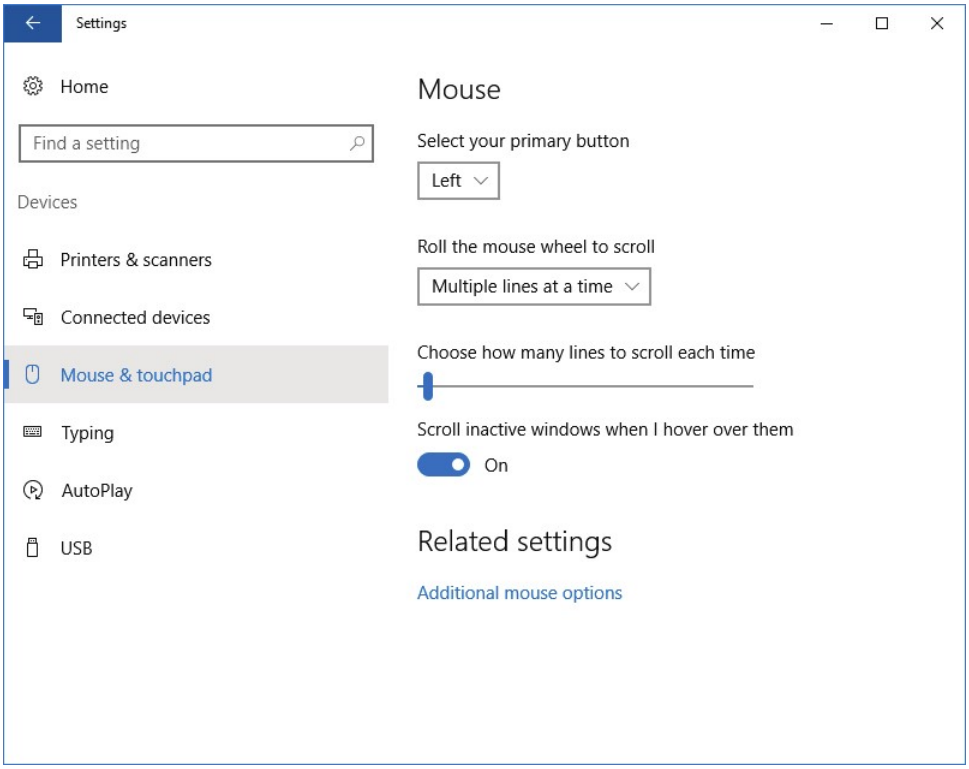


Figure B3.9.1-2 Mouse Page

5. Turn off [Scroll inactive windows when I hover over them].
6. Click the [×] button to close the window.
7. In the left pane, select [Mouse & touchpad].
   The Mouse page appears.
8. Turn off [Scroll inactive windows when I hover over them].
9. Click the [×] button to close the window.

B3.9.2 Setting of Items Specific to Windows 10

This section describes how to set the items specific to Windows 10.

Suppressing Toast Notifications Regarding Windows Firewall

If your OS is Windows 10 Enterprise 2016 LTSB and the IT security model is Legacy model, suppress toast notifications regarding Windows Firewall.

Follow these steps to suppress toast notifications:

TIP

This setting is not required if the OS is Windows 10 Enterprise LTSC 2019 or Windows 10 Enterprise LTSC 2021 and the IT security model is Legacy model.

1. Sign in as an administrative user.
2. Open Control Panel.
3. From the menu, select [System and Security] > [Windows Firewall].
   The Windows Firewall window appears.
4. In the left pane, click [Turn Windows Firewall on or off].
5. Select [Turn off Windows firewall] in the private network settings, public network settings, and domain network settings. However, you need to configure the domain network settings only in domain environments.
6. Click [OK].
7. Sign out and sign in again using the user account for which to turn off toast notifications regarding Windows Firewall.
8. Open Control Panel.
9. From the menu, select [System and Security] > [Security and Maintenance].
   The Security and Maintenance window appears.
10. On the left pane, click [Change Security and Maintenance settings].
11. Clear the [Network firewall] check box under Security messages.
12. Click [OK].

TIP

- If the [Network firewall] check box is grayed out, wait for a few minutes until it is enabled.
- If a toast notification [Turn on Windows firewall] appears, carry out the above procedure without clicking the toast notification.

Precautions when using Windows 10 Enterprise LTSC 2019 or Windows 10 Enterprise LTSC 2021

This section describes precautions when the OS is Windows 10 Enterprise LTSC 2019 or Windows 10 Enterprise LTSC 2021 and the IT security model is Legacy model.

- What to do when a toast notification regarding Windows Firewall appears
  If a toast notification appears, close it. If you click the toast notification to open the Settings window, close it without doing anything.

  You cannot enable or disable Windows Firewall in the Settings window that opens when you click the toast notification.
- How to check the firewall state
  In Legacy model, the firewall is disabled in a proper state. You can check the firewall state in the following ways.

On the left pane of the Local Group Policy Editor, open the properties of [Windows Defender Firewall with Advanced Security], the [Firewall state] is displayed as [Disabled].

Alternatively, in Control Panel, open [Windows Defender Firewall], and [Disabled] and [Some settings are managed by your system administrator] are displayed.

TIP

You can check the firewall state for the Standard model in the following ways.

On the left pane of the Local Group Policy Editor, open the properties of [Windows Defender Firewall with Advanced Security], the [Firewall state] is displayed as [Not Configured].

Alternatively, in Control Panel, open [Windows Defender Firewall], and [Enabled] is displayed.

B3.10 Configuring the Uninterruptible Power Supply (UPS) Service

You can install uninterruptible power supply (hereinafter referred to as UPS) software and make various settings to protect data in the computer at power supply failures.

UPS Software Setting

Specify the UPS battery operation time so that the computer can continue operation with the UPS battery without shutting down even if a power supply error (for example, power interruption) occurs for a short period of time. Use several seconds as a guideline for setting the UPS battery operation time.

TIP

Although the UPS battery operation time can be set longer than several seconds, the computer should be shut down at a power interruption of several seconds for safety reasons.

SEE ALSO

For more information about the UPS software that can coexist with ProSafe-RS, refer to:

"● Software that can coexist with ProSafe-RS" in "■ Software requirements for SENG" in A1.2, "Software requirements" in ProSafe-RS User's Guide (IM 32P01B10-01EN)

B4. Configuring the Functions Specific to SENG

This section describes how to configure the following settings for the functions specific to SENG.

- Setting the manual browsing environment
- Settings of Project Database Folder
- Settings for Message Cache Tool
- Settings Required for OPC Communication
- Setup when Using the Access Control and Operation History Management Package

B4.1 Setting the Manual Browsing Environment

Configure Adobe Acrobat Reader to view the online manuals and the Help files for PROFINET Configurator.

Adobe Acrobat Reader Settings

In the Adobe Acrobat Reader settings, make sure that the [Open cross-document links in same window] check box is selected.

- The [Open cross-document links in same window] check box can be displayed by selecting [Preferences] - [Documents] from the [Edit] menu of Adobe Acrobat Reader. You must set this setting for each logon user.

Copying the Help Files for PROFINET Configurator

The Help files for PROFINET Configurator are stored in the software medium of ProSafe-RS. As the Help files are not installed automatically on the computer, copy them from the software medium as necessary.

- Stored location

  `<Media drive of ProSafe-RS>:\ProSafe-RS\PDFFILE\PROFINET_Configurator\en\`

- Help files

  `SYCONnet netFrame YOKOGAWA S2LP131.pdf`

  `SYCONnet netDevice YOKOGAWA S2LP131.pdf`

  `PROFINET IO Controller YOKOGAWA S2LP131 DTM.pdf`

  `YOKOGAWA PROFINET IO Generic Device DTM.pdf`

B4.2 Settings of Project Database Folder

This section explains the procedure for strengthening the security of project databases.

Strengthening the Security of the Project Database on SENG PC

When ProSafe-RS software is installed, `C:\RS-Projects` folder is automatically created as the default location for saving project data. By running the IT Security Tool after the installation, security reinforcement is done for this default folder.

Shown below is the procedure for reinforcing security when you place the project database in a location other than the default folder on an SENG PC and have it shared with other computers.

1. Create a new folder for storing project data.
2. Log on as an administrative user belonging to the PSF_MAINTENANCE group and assign the share name RS-Projects to a folder to which the project database is to be stored.
3. Grant full control access permissions to Everyone.
4. Launch the IT Security Tool from the Start menu and configure security settings without changing the security model and user management type.

Strengthening the Security of Version Control Tool's Check-in Folder

If you place the Version Control Tool's check-in folder on an SENG PC, follow these steps to strengthen the security of the folder.

1. Create a new folder for use as the check-in folder of Version Control Tool.
2. Log on as an administrative user belonging to the PSF_MAINTENANCE group and assign the share name RS-Share to the check-in folder.
3. If the folder should be shared with other computers, grant full control access permissions to Everyone.
4. Launch the IT Security Tool from the Start menu and configure security settings without changing the security model and user management type.

B4.3 Settings for Message Cache Tool

If you want to check the status of data collection by other stations using the Message Cache Tool, the following setups are required.

On Workgroup Member Computers

1. Create a user account on the station whose status of data collection shall be checked. The user account name and password should be the same as the user account of the computer that uses the Message Cache Tool.
2. Make the created user account created in step 1 belong to the PSF_ENGINEER user group.

On Windows Domain Member Computers

Register users of the Message Cache Tool to the PSF_ENGINEER user group.

B4.4 Settings Required to Use the Forced I/O Viewer Function

To use the Forced I/O Viewer function, settings must be made on the computer where SCS projects are saved and the computer to which to distribute SCS projects.

Setting on the Computer where SCS Projects are Saved

The Forced I/O Viewer Setup Tool acquires the SCS projects to be distributed to Forced I/O Viewer from the computer in which the SCS projects are stored.

Follow these steps to set up the computer where SCS projects are saved:

1. Assign the share name RS-Projects to the upper folder of the RS project folder that contains the SCS projects.
   If the share name RS-Projects is assigned already, no setting is required.
2. Create a user account with the same user name and password as the user account that uses the Forced I/O Viewer Setup Tool. If the IT security model is the Standard model, add the created user account to the PSF_ENGINEER or PSF_MAINTENANCE group.

SEE ALSO For more information about how to assign the share name RS-Projects, refer to:

"■ Strengthening the Security of the Project Database on SENG PC" on page B4-3

Settings on the Computer to which to Distribute SCS Projects

Follow these steps to set up the computers to which to distribute SCS projects, such as a computer where Forced I/O Viewer will be used and SENG that shares the registration file:

1. Assign the share name RS-ForcedIO to the following folder:
   `<ProSafe-RS installation drive>:\Program Files (x86)\ProSafe-RS\YOKOGAWA\hmi\ForcedIO`
2. In the Share Permission of the share name RS-ForcedIO, grant full control access permissions to Everyone.

IMPORTANT

The share name is "RS-ForcedIO" with "RS-" added to the beginning of the folder name. It is different from the folder name.

3. Create a user account with the same user name and password as the user account that uses the Forced I/O Viewer Setup Tool. If the IT security model is the Standard model, add the created user account to the PSF_ENGINEER or PSF_MAINTENANCE group.
4. If the IT security model is the Standard model, add the user account that uses the Forced I/O Viewer to the PSF_OPERATOR group.

B4.5 Settings Required for OPC Communication

This section describes how to make settings required to perform OPC communication when the Standard model of IT security settings are selected on an SENG PC running the SOE OPC Interface Package. If the Standard model of security settings is applied, access to DCOM will be set. By this setting, only users belonging to ProSafe-RS user groups can access the SOE OPC interface.

Setting when Using Packages Performing OPC Communication with SENG PC

When you are using packages (OPC clients) that perform OPC communication with SENG PC (OPC servers), you must make the setting explained here.

In the Case of Standalone Management or When Combination Management is Applied on Some Computers

Perform the following procedure on an SENG PC performing OPC communication.

1. Create a program user of the OPC client package. Set the same user name and password as those on the client computer.
2. Make the created program user belong to the PSF_OPC user group.

In the Case of Domain Management or When Combination Management is Applied on All Computers

- In the case of package that can join the domain
  1. Make a computer that runs the OPC client package join the domain.
  2. Register the package program user to the domain and make it belong to the PSF_OPC user group.
- In the case of package that cannot join the domain
  Perform the following procedure on the SENG PC performing OPC communication.
  1. Create a program user of the OPC client package. Set the same user name and password as those on the computer running the package.
  2. Make the created program user belong to the PSF_OPC_LCL user group.

SEE ALSO

For more information about the settings for a computer where the SOE OPC Interface Package and CENTUM VP ExaOPC Interface Package coexist, refer to:

D1.1.4, “CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS SOE OPC Interface Package” on page D1-8

For more information about the settings for using Exaquantum as an OPC client, refer to:

D1.4.1, “ProSafe-RS SOE OPC Interface Package and Exaquantum PIMS Server” on page D1-27

In the Case of Linked Domain Management

- In the case of package that can join the domain
  1. Make a computer that runs the OPC client package join the domain.
  2. Register the package program user to the domain and make it belong to the PSF_OPC user group.
- In the case of package that cannot join the domain

Perform the following procedure on the SENG PC performing OPC communication.

1. Create a program user of the OPC client package. Set the same user name and password as those on the computer running the package.
2. Make the created program user belong to the PSF_OPC user group.

B4.6 Setup when Using the Access Control and Operation History Management Package

In ProSafe-RS R3.01 or later, it is possible to manage operation histories on SENG by using the Access Control and Operation History Management Package. This section describes the operations required to use this package.

SEE ALSO For more information about the precautions to be followed when setting the access control/operation history management function, refer to:

E., “Access Control/Operation History Management functions” in Engineer's Reference Manual (IM 32P04B10-01EN)

Windows User Groups to which Administrators and Engineers Belong

There are two types of personnel in a system where the access control and operation history management is applied: “administrators of access control and operation history management” (hereinafter referred to as “administrator” in this section) and “engineers.”

After creating user accounts for administrators and engineers, add them to the Windows user groups shown in the following table.

Table B4.6-1 Windows User Groups to which Administrators and Engineers Must Belong

Personnel	Windows user group to belong to	
	Standard or Strengthened model	Legacy model
Administrator	Either of the following: PSF_MAINTENANCE (*1) PSF_MAINTENANCE_LCL (*1)	Group with administrator privilege
Engineer	One of the following: PSF_OPERATOR PSF_ENGINEER PSF_OPERATOR_LCL PSF_ENGINEER_LCL	Any group

*1: Users belonging to these groups must also have the Windows administrator privileges. Make them also belong to the Administrators or Domain Admins group.

Security Model and User Authentication Mode

If you select the Standard model with the IT Security Tool, you can select either ProSafe authentication mode or Windows authentication mode as the user authentication mode of the operation history management function on SENG. By default, ProSafe authentication mode is selected.

If you select the Legacy model with the IT Security Tool, only ProSafe authentication mode is available.

You can configure user authentication modes by using the operation history management setting tool included in the Access Control and Operation History Management Package.

SEE ALSO For more information about security models, refer to:

2., “Security Models” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

Creating User Accounts in Windows Authentication Mode

In Windows authentication mode, Windows user names are used to log on to the SENG functions and authenticate users.

IMPORTANT

When you use Windows authentication mode, create Windows users following the naming convention below, rather than the Windows naming convention. This naming convention is the same as the naming convention for engineers.

The naming convention for users in Windows authentication mode is as follows:

Table B4.6-2 User Naming Convention in Windows Authentication Mode

Number of characters	Up to 16 characters
Character type	Alphanumeric characters and the following symbols can be used: ! # $ % ( ) - . ^ _ { } ~ Double-byte characters cannot be used.
Restriction	Upper-case characters only (*1) For the head character, alphanumeric characters and the following symbols can be used: ^ _ { } ~ Names ending with a period cannot be used.

*1: Only upper-case characters can be used for engineer names to be registered in the Engineers' Account Builder. Although both upper-case and lower-case characters can be used on the Windows side, they are not distinguished; use upper-case characters only.

You can set passwords within 63 characters using alphanumeric characters and symbols.

- Passwords are case-sensitive.
- The following symbols and space character are allowed:
  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ { | } ~

SEE ALSO For more information about how to create Windows user accounts, refer to:

B3.8, "Creating User Accounts" on page B3-56

B4.6.1 Setup Procedure when Using Access Control and Operation History Management Functions

This section describes the setup procedure you should perform after installing the ProSafe-RS software when using the operation history management functions. If you want to introduce the access control and operation history management functions later, perform the procedure at a proper timing.

Perform the following tasks after creating administrator and engineer user accounts on Windows.

1. Add the Windows accounts for administrators and engineers to their respective appropriate user groups.
2. Configure security settings for the operation history database.
3. On a computer granted with the licenses of the Safety System Engineering and Maintenance Function and the Access Control and Operation History Management Package, use the Operation History Management Setup Tool and Engineers' Account Builder to perform required setting.

SEE ALSO

For more information about how to create Windows user accounts, refer to:

B3.8, "Creating User Accounts" on page B3-56

For more information about the explanation of the procedure involved in making security settings for operation history management databases, refer to:

B4.6.2, "Security Settings for the Operation History Database" on page B4-11

For more information about the precautions to be followed when setting the access control/operation history management function, refer to:

E2.2, "Setting up Access Control/Operation History Management" in Engineer's Reference Manual (IM 32P04B10-01EN)

B4.6.2 Security Settings for the Operation History Database

The administrator must specify the folder for storing the operation history database by using the operation history management setting tool. Set the security of the folder for storing the operation history database at proper timing before starting to use the operation history management function.

This section explains the procedures to configure security settings when the operation history database is placed on an SENG PC and when it is placed on a file server. After performing these procedures, the administrator and engineers can access the operation history database folder.

Setting when Operation History Databases are Placed on SENG PC

If you place an operation history database on an SENG PC, perform the following procedure to reinforce the security of the folder for storing the operation history database.

1. Create a new folder for storing the operation history database.
2. Log on to the system as an administrative user who belongs to the PSF_MAINTENANCE group and assign the sharing name “RS-Share” to the folder for storing the operation history database.
3. If the folder needs to be shared with other computers, grant a full control permission to Everyone.
4. Launch the IT Security Tool from the Start menu and execute it again without changing the setting made the last time it was executed.

Setting when Operation History Databases are Placed on a File Server

If you place an operation history database on a computer not installed with the ProSafe-RS software and allow SENG to access the database via a network, perform the procedure to reinforce security of the file server.

SEE ALSO For more information about the procedure for reinforcing the security of the file server, refer to:

B5., “Setting Up a File Server” on page B5-1

B5. Setting Up a File Server

By setting up a file server, you can access the files placed on this server computer from other computers. On a file server, you may place a project database, the check-in destination folder for Version Control Tool, and/or the operation history database of the Access Control and Operation History Management Package, which you can access and operate through the network.

This section describes how to set up a file server computer for the following cases:

- Computer that serves only as a file server
- Computer that serves as both a file server and an SENG
- Computer that serves as both a file server and a license management station

IMPORTANT

- The initial password is set by default for the predefined user accounts in this product. Be sure to change the password because operating with the initial password may increase the security risk.
- When changing the password, ensure that the same password is set in the entire system.

SEE ALSO For more information about user accounts that require password change, refer to:

2.2.3, “User/Group Management” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

Item to be Prepared

Have the following item at hand before you set up a file server.

- ProSafe-RS software medium

File System

Ensure that the file system is in the NTFS format.

B5.1 Setting Up a Computer that Serves Only as a File Server

This section describes how to set up a computer that is used only as a file server.

IMPORTANT

- When sharing a file server between CENTUM VP and ProSafe-RS and operating with other than linked domain management, use the IT Security Tool for file server and domain controller whose revisions are R6.04 or later to set IT security for CENTUM VP.
- When sharing a file server between CENTUM VP and ProSafe-RS and operating with linked domain management, you must build a file server between the products of revisions that support linked domain management. Use the IT Security Tool for file server and domain controller of the product of revisions that support linked domain management and the Domain Link Management Tool for File Server. CENTUM VP supports linked domain management with R6.08 or later software revisions.
- When sharing a file server with a product that does not support linked domain management and using it in a domain environment, operate with domain management or combination management.

Installing Windows Update Programs

Download and apply the Windows update programs for your Windows OS.

SEE ALSO For more information about downloading the Windows Server 2022 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2022)" on page B1-5

For more information about downloading the Windows Server 2019 update programs , refer to:

"■ Downloading the Windows Update Programs (Windows Server 2019)" on page B1-6

For more information about downloading the Windows Server 2016 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2016)" on page B1-6

Disabling the Automatic Cleanup Task

When using Windows Server as a file server, disable Automatic cleanup task.

SEE ALSO For more information about the procedure for disabling the Automatic cleanup task, refer to:

"■ Disabling the Automatic Cleanup Task" on page B3-15

Administrative User who Performs the Setup

A file server must be set up by an administrative user who belongs to the groups shown in the following table.

Table B5.1-1 Groups to Which the Administrative User Who Sets Up a File Server Belongs

Security model and user management type to be applied		
Legacy model	Standard model	
	Standalone management/Linked domain management	Domain/Combination management
Local user who belongs to the Administrators local group	Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group	• Domain user who belongs to the Domain Admins domain group and PSF_MAINTENANCE domain group • Domain user who belongs to the Administrators local group and PSF_MAINTENANCE local group • Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group (*1)

*1: The domain user name and password must be entered during installation.

TIP

If the user management type is Domain or Combination management, install the software after the computer is added to the domain.

■ Procedure 0: Procedure for Placing an SCS Project on Another PC Such as a File Server

If an SCS project is newly placed on a file server PC that is different from the SENG PC, files in the SCS project database may be corrupted while the SCS project is operated on the SENG PC. When you are going to place an SCS project on a PC such as a file server which is different from the SENG PC that operates the SCS project, make sure to implement the avoidance described in SEE ALSO to prevent file corruption in the SCS project database.

SEE ALSO

For more information about avoidance, refer to:

"■ Precautions when Placing the SCS Project on Another PC such as a File Server" in 1.2, "Engineering" in ProSafe-RS Release Information (IM 32P01A50-01EN)

■ Procedure 1: Install Microsoft Visual C++ 2017 Redistributable Package

Before you can run the IT Security Tool, you must install the Microsoft Visual C++ 2017 redistributable package.

SEE ALSO

For more information about the procedure for installing the Microsoft Visual C++ 2017 redistributable package, refer to:

"■ Installation of Microsoft Visual C++ 2017 Redistributable Package" on page B2-6

■ Procedure 2: Create an Administrative User

Perform one of the following procedures according to the security model to be applied.

TIP

In the case of the Legacy model, this operation is not required because the setup can be performed by an existing user.

● Standard Model with Standalone Management/Linked Domain Management

1. Log on as a member of the Administrators group.
2. Create the PSF_MAINTENANCE group.

3. Add the user to be set as the administrator to the Administrators and PSF_MAINTENANCE groups.

TIP

If any other YOKOGAWA product coexists in the computer, the user also needs to be a member of the MAINTENANCE group of the coexisting product. For example, if CENTUM VP coexists, also add the user to the CTM_MAINTENANCE group.

Standard Model with Domain/Combination Management

Follow these steps to designate a local group user as an administrator:

TIP

To use a domain group user as an administrative user, this operation is not required because the user already exists.

1. Log on to Windows as a user with administrative rights.
2. Create the PSF_MAINTENANCE local group.
3. Add the domain user or local user to be set as the administrator to the Administrators local group and PSF_MAINTENANCE local group.

TIP

- After the IT Security Tool is run, the name of the PSF_MAINTENANCE group you have created will change to PSF_MAINTENANCE_LCL.
- If any other product coexists in the computer, the user also needs to be a member of the MAINTENANCE group of the coexisting product. For example, if CENTUM VP coexists, also add the user to the CTM_MAINTENANCE group.

Procedure 3: Create and Set Up Shared Folders

In order to reinforce the security of folders that store databases using the IT Security Tool, you must name the target folders with the following share names:

- Project database
  Share name: RS-Projects
- Operation history database and check-in destination folder of Version Control Tool
  Share name: RS-Share

IMPORTANT

If the share name does not match the name above, the IT Security Tool is not able to reinforce the folder security. Be sure to set the share name above using the following procedure so that you can reinforce security.

Creating a New Folder

1. Log on as an administrative user.
2. Start Windows Explorer and create a folder in which the project folders are to be placed.
3. On the Sharing tab in the properties of the folder that is created, click [Advanced Sharing].
4. Select [Share this folder] and set `RS-Projects` or `RS-Share` as the share name.
5. Click [Permissions], and grant full control to [Everyone] in the Share Permissions tab. This access permission setting will be changed when you run the IT Security Tool.

When a Shared Folder is Already Created on the File Server

Before configuring IT security settings, add a share name, “RS-Projects” or “RS-Share,” to the folder. The folder will be included in the process of IT security setting configuration and access permissions setting will be applied. Share names that were previously set up do not need to be deleted.

IMPORTANT

If a folder with the share name “RS-Projects” or “RS-Share” has already been created for another purpose on an existing file server, change the existing share name to another name. Since the access permissions are granted to folders with the share name “RS-Projects” or “RS-Share” during configuration of IT security settings, unintended settings will be applied if these share names are not assigned to appropriate folders.

If IT security settings have been applied to an unintended folder, delete the permissions set during the configuration of IT security settings and set the original access permissions based on the setting of another folder, such as the `C:\Windows` folder.

Procedure 4: Save the Initial Data of the IT Security Settings

IMPORTANT

- Before you run the IT Security Tool to configure IT security settings for the first time, be sure to save the security settings on the computer.
- On a file server, when changing the IT security settings, you need to use the initial data saved beforehand to restore the security settings, and then apply them again. Therefore, the following saved data of IT security settings is required.
  - When the user management type is standalone management or linked domain management in Standard model:
    Data saved before the first application of IT security settings in the standalone state
  - When the user management type is Domain management or Combination management in Standard model:
    Data saved before applying IT security settings after adding to the domain
- When configuring the security settings for the second time onward, basically the security settings need not be saved. However, to configure the security settings by using the IT Security Tool of R3.01 to R4.02 and change the IT security version to 2.0 by using the IT Security Tool of R4.03 or later, save the initial security setting data again.
- To save the initial security setting data again, restore the security settings that were saved before by using the IT Security Tool. If the file server is a member of the domain, determine which of the two sets of initial data will be recovered based on whether or not to keep the file server as the member of the domain. Then, perform this procedure to save the security settings. From then on, the data you have saved again will be used when the security settings are initialized; accordingly, keep the saved data in a safe place.

Follow these steps to save the security settings:

1. Log on as an administrative user.
2. Insert the ProSafe-RS software medium into the drive.
   - If the AutoPlay dialog box appears, click [Run Launcher.exe].

- If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the software medium.

The installation menu appears.

3. Click [Setting IT Security (File server/domain controller use)].
   The IT Security Tool starts.

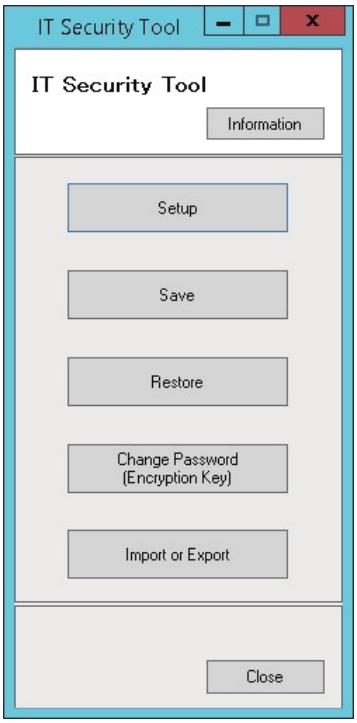


Figure B5.1-1 IT Security Tool Menu

TIP

If the file server is a member of a domain, when restoring the initial security settings on the file server, the initial data should have two types, either the initial data for a standalone computer or the initial data for a member of domain.

If you do not have the initial data for a standalone file server computer, you need to remove the file server from the domain temporarily and then save the security settings as the initial data for the standalone computer.

4. Click [Save].
   The Specify destination page appears.
5. Specify the destination folder and enter following setting items.
   - Distinguished Name
   - Support Product
   - Support OS
   - File Version

TIP

The [Distinguished Name] and [File Version] are omissible.

6. Click [Next].
   The Type default account password page appears.
7. Enter the password for use as the initial account password and click [Next].
   The Type password (Encryption Key) page appears.

TIP

This initial password will be set when the account saved with this tool is recovered. If the saved accounts are not found on the computer when you recover the accounts, new accounts are created. This password will be set as the initial password for the newly created account.

Even when multiple accounts have been created, the same initial password is assigned to all.

If the set password does not meet the password policy in the environment where the account is to be recovered, an error will occur when recovering an account.

This password is set as the initial password for the account. Accordingly, you will be prompted to change the password when you log on for the first time using this account.

8. Enter the password for encrypting the saved data, and click [Next].
   Saving of the security settings starts.

IMPORTANT

- If this password (encryption key) is lost, the saved security settings cannot be restored. The password (encryption key) must be carefully kept by the customer.
- The password (encryption key) must be at least one character.
- The password can consist of upper-case and lower-case alphanumeric characters and the following symbols: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . /
  Double-byte characters cannot be used.

9. When the saving is completed, click [Finish].
   If the saving failed, the details of the failure are displayed.
10. On the IT Security Tool menu, click [Close].

TIP

If any save failures are displayed, contact YOKOGAWA Service.

Procedure 5: Configure with IT Security Tool

IMPORTANT

If you operate with linked domain management, do not add the computer to the domain before you configure the settings with IT Security Tool.

Follow these steps to configure the file server with IT Security Tool:

1. From the IT Security Tool Menu, click [Setup].
   A confirmation dialog box appears
2. If you have saved the above mentioned initial security setting data, click [OK].

TIP

If you have not saved the initial security setting data, click [Cancel] to return to the tool's menu and save the security settings.

The Select Security Model page appears.

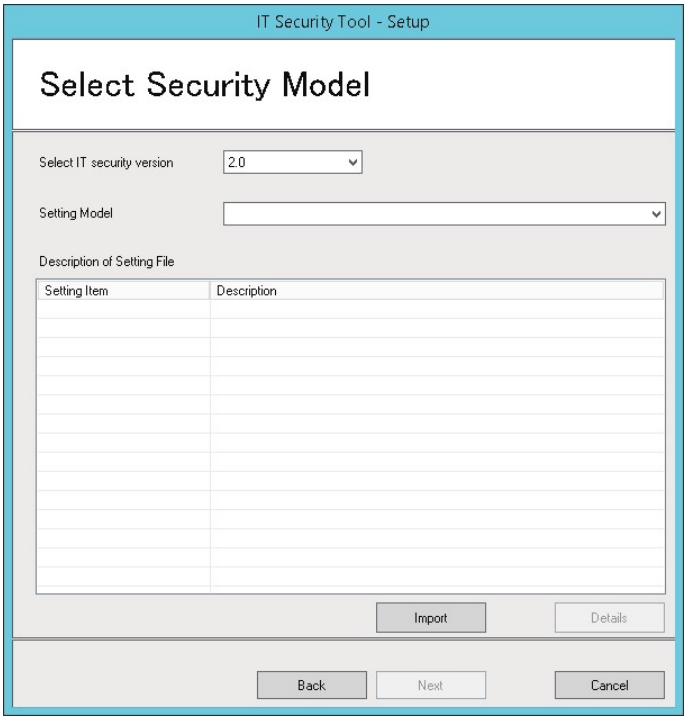


Figure B5.1-2 Select Security Model

3. From the Select IT security version drop-down list, select the IT security version.
4. From the Setting Model drop-down list, select a security model for the file server.
   You can select from the following four models:

Table B5.1-2 Security Models for a File Server

Model	Description
File Server Legacy Model (*1)	Select this model to apply Legacy model to the file server, regardless of the user management type.
File Server Standard Model with Standalone Management	Select this model to apply Standard model to the file server when the user management type is Standalone management or Linked domain management.
File Server Standard Model with Domain Management	Select this model to apply Standard model to the file server when the user management type is Domain management.
File Server Standard Model with Combination Management	Select this model to apply Standard model to the file server when the user management type is Combination management.

*1: If you select [2.0] for Select IT security version, you cannot select the file server legacy model.

5. Click [Next].
   The Confirm Setting Information page appears.

TIP

If you click [Detail] here, the Select Setting Items page appears.

6. The subsequent steps are the same as those for the settings with IT Security Tool after installing the ProSafe-RS software.

TIP

If the file server is shared with CENTUM VP, start the IT Security Tool for file server and domain controller from the installation menu of CENTUM VP software medium and set IT security for CENTUM VP as well. Use the software medium of the following revisions depending on the user management type.

- Linked domain management: R6.08 or later
- Other than Linked domain management: R6.04 or later

SEE ALSO

For more information about operation of IT Security Tool after the ProSafe-RS software is installed, refer to:

B3.6.1, “Running the IT Security Tool” on page B3-46

For more information about the procedure for importing the IT security settings, refer to:

6.8, “Exporting/Importing the IT Security Setting File” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

Procedure 6: Create Accounts on the File Server for Users who Access Project Data

On the file server computer, create accounts for users who access the project data, according to the selected security model and user management type.

● Standard Model with Linked Domain Management/Combination Management

When you create accounts of local users who access project data, create them in the same way as for “● Legacy/Standard Model with Standalone Management.”

On the domain controller, add the accounts for accessing projects. No account needs to be created if already created.

SEE ALSO

For more information about how to create domain user accounts, refer to:

B2.4, “Creating Domain Users” on page B2-13

● Standard Model with Domain Management

On the domain controller, add the accounts for accessing projects. No account needs to be created if already created.

● Legacy/Standard Model with Standalone Management

Perform the following procedure on the file server.

1. Create a user account.
   The user name and the password must be the same as those of the SENG PCs from which the projects are accessed.
2. Register the user you have created to the same group as that on the SENG PCs which access the file server.

TIP

If the Standard model is applied, the following user groups have been created during the procedures so far.

- PSF_MAINTENANCE
- PSF_OPERATOR
- PSF_ENGINEER
- PSF_OPC

Procedure 7: Configure Settings for Operating with Linked Domain Management

When operating with linked domain management, join the computer to the domain and then configure settings using Domain Link Management Tool for File Server.

IMPORTANT

The Domain Link Management Tool for File Server in the ProSafe-RS software medium links/unlinks the domain only for the local group related to ProSafe-RS. If the file server is shared by CENTUM VP and ProSafe-RS, use the Domain Link Management Tool for File Server in the software medium of each product to set each.

Follow these steps to configure settings for operation with linked domain management:

1. Join the computer to the domain.
2. Sign in as a local user who belongs to both the Administrators group and PSF_MAINTENANCE group of the local computer, or a domain user who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain.
3. Use Windows Explorer to open the following folder in the ProSafe-RS installation medium.
   `<Drive of ProSafe-RS software medium>:\ProSafe-RS\SECURITY\`
4. In the folder, double-click `DomainLinkManagementToolForRSFileServer.cmd`.
   The Domain Link Management Tool for File Server starts.
5. The subsequent steps are the same as those for the settings with Domain Link Management Tool after installing the ProSafe-RS software.

TIP

- If you start the Domain Link Management Tool as an administrative user of a local group, the domain user authentication dialog box appears in the procedure for linking the domain. The user name and password that you enter in the dialog box do not have to be those of the domain administrator.
- If the file server is shared with CENTUM VP, use the Domain Link Management Tool for File Server in the software medium of CENTUM VP to configure the settings to link the domain for CENTUM VP as well.

SEE ALSO

For more information about the settings with Domain Link Management Tool after the ProSafe-RS software is installed., refer to:

B3.6.3, “Running Domain Link Management Tool” on page B3-52

Error Messages and Countermeasures

Depending on the conditions when starting Domain Link Management Tool for File Server, an error message may be displayed and the tool cannot be started. Take the necessary measures.

The following table describes the error messages and countermeasures when you cannot start Domain Link Management Tool for File Server.

Table B5.1-3 Error messages and countermeasures

Error messages	Countermeasures
This tool cannot be started simultaneously with the IT security tool.	Exit the IT Security Tool.

Continues on the next page

Table B5.1-3 Error messages and countermeasures (Table continued)

This tool does not support computers without the IT security settings for the file server of R4.06.00 or later.	For a file server dedicated computer, set the IT security for the file server of R4.06.00 or later, and then start Domain Link Management Tool for File Server.
	For computers with ProSafe-RS software or license management software installed, start Domain Link Management Tool from the Start menu.

Procedure 8: Create the Project Folder on the File Server and Start the Operation

- Project database
  From an SENG PC, create an RS project under the shared folder “RS-Projects” created in Procedure 3.
- Check-in folder of Version Control Tool
  On an SENG PC, use the Version Control Tool to specify a folder under the shared folder “RS-Share” created in Procedure 3 as the check-in destination folder, and start project operation.
- Operation history database
  On an SENG PC, use the operation history management setting tool to specify a folder under the shared folder “RS-Share” created in Procedure 3 as the top folder of the operation history database, and start the access control and operation history management function.

B5.2 Setting Up the File Server Function on an SENG or a Computer Installed with Only AD Server

This section describes the required settings when you use a computer that has been set up as an SENG or installed with only AD Server, also as a file server.

TIP

On an SENG, the project database is created under the installation folder by default. The procedure described in this section is for the case when the project database is placed in a location other than the installation folder.

1. Set up the computer as an SENG or as a computer installed with only AD Server.

TIP

- If the user management type of IT security setting is domain or combination management, set up after the computer is added to the domain.
- You do not need to configure IT security settings during this setup.

2. If an SCS project is newly placed on a file server PC that is different from the SENG PC, files in the SCS project database may be corrupted while the SCS project is operated on the SENG PC. When you are going to place an SCS project on a file server, make sure to implement the avoidance described in SEE ALSO to prevent file corruption in the SCS project database.
3. On the computer, create and set up the shared folder.
4. Start the IT Security Tool from the Start menu and configure IT security settings.

TIP

When operating with linked domain management, set the standalone management in the Standard model.

5. Select one of the following depending on the user management type.
   - Go to the step 6 to operate with linked domain management.
   - Go to the step 8 to operate with user management type other than linked domain management.
6. Join the computer to the domain.
7. Start Domain Link Management Tool from the Start menu and link the domain.
8. Create a project folder in a location under the shared folder of the computer.

IMPORTANT

When you set up the file server function on an SENG or a computer with only AD Server installed, you must use the IT Security Tool and Domain Link Management Tool that are started from the Start menu.

SEE ALSO

For more information about how to create the project folder on the file server, refer to:

"■ Procedure 8: Create the Project Folder on the File Server and Start the Operation" on page B5-11

For more information about new setup of SENG, refer to:

B3., "Setup of an SENG or a Computer Installed with Only AD Server" on page B3-1

For more information about the shared folder settings, refer to:

"■ Procedure 3: Create and Set Up Shared Folders" on page B5-4

For more information about creating accounts for users who access the project database, refer to:

"■ Procedure 6: Create Accounts on the File Server for Users who Access Project Data" on page B5-9

For more information about avoidance against file corruption in the SCS project database, refer to:

"■ Precautions when Placing the SCS Project on Another PC such as a File Server" in 1.2, "Engineering" in ProSafe-RS Release Information (IM 32P01A50-01EN)

B5.3 Setting Up the Computer that Serves as Both File Server and License Management Station

This section describes the setup required for the computer that serves as both a file server and a license management station.

Setup Procedure

1. Install the license management software.

TIP

If the user management type of IT security setting is domain or combination management, set up after the computer is added to the domain.

2. If an SCS project is newly placed on a file server PC that is different from the SENG PC, files in the SCS project database may be corrupted while the SCS project is operated on the SENG PC. When you are going to place an SCS project on a file server, make sure to implement the avoidance described in SEE ALSO to prevent file corruption in the SCS project database.
3. On the dialog box that appears on completion of the installation, select [No, I want to install other software products.] and click [Finish].
4. Configure the shared folder settings required for a file server.
5. Start the IT Security Tool from the Start menu and configure IT security settings.

TIP

When operating with linked domain management, set the standalone management in the Standard model.

6. Select one of the following depending on the user management type.
   - Go to the step 7 to operate with linked domain management.
   - The steps are completed if you operate with user management type other than linked domain management.
7. Join the computer to the domain.
8. Start Domain Link Management Tool from the Start menu and link the domain.

IMPORTANT

When you configure a computer for use as both a file server and a license management station, you must use the IT Security Tool and Domain Link Management Tool that are started from the Start menu.

SEE ALSO

For more information about installing only the license management software, refer to:

B6., “Setting Up the Computer Dedicated to License Management” on page B6-1

For more information about the shared folder settings, refer to:

“■ Procedure 3: Create and Set Up Shared Folders” on page B5-4

For more information about avoidance against file corruption in the SCS project database, refer to:

“■ Precautions when Placing the SCS Project on Another PC such as a File Server” in 1.2, “Engineering” in ProSafe-RS Release Information (IM 32P01A50-01EN)

B6. Setting Up the Computer Dedicated to License Management

You can use a computer as the license management station by installing only the license management software on it.

This section describes the procedure for setting up the computer dedicated to license management.

Items to be Prepared

Have the following item at hand before installing the license management software.

- ProSafe-RS software medium

Installing Windows Update Programs

Download and apply the Windows update programs for your Windows OS.

SEE ALSO

For more information about downloading the Windows 10 Enterprise LTSC 2021 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows 10 Enterprise LTSC 2021)" on page B1-4

For more information about downloading the Windows 10 Enterprise LTSC 2019 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows 10 Enterprise LTSC 2019)" on page B1-5

For more information about downloading the Windows 10 Enterprise 2016 LTSB update programs, refer to:

"■ Downloading the Windows Update Programs (Windows 10 Enterprise 2016 LTSB)" on page B1-5

For more information about downloading the Windows Server 2022 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2022)" on page B1-5

For more information about downloading the Windows Server 2019 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2019)" on page B1-6

For more information about downloading the Windows Server 2016 update programs, refer to:

"■ Downloading the Windows Update Programs (Windows Server 2016)" on page B1-6

Administrative User who Performs the Installation

The administrative users shown in the following table should install the license management software:

IMPORTANT

- The initial password is set by default for the predefined user accounts in this product. Be sure to change the password because operating with the initial password may increase the security risk.
- When changing the password, ensure that the same password is set in the entire system.

Table B6-1 Administrative User Who Installs the License Management Software

Security model and user management type to be applied		
Legacy Model	Standard Model	
	Standalone management/Linked domain management	Domain/Combination Management
Local user who belongs to the Administrators local group	Local user who belongs to the Administrators local group	• Domain user who belongs to the Domain Admins domain group • Domain user who belongs to the Administrators local group • Local user who belongs to the Administrators local group(*1)

*1: The domain user name and password must be entered during installation.

TIP

If the user management type is Domain or Combination management, install the software after the computer is added to the domain.

SEE ALSO

For more information about user accounts that require password change, refer to:

2.2.3, “User/Group Management” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

Setting Up a License Management Station

This section describes the procedure for setting up a license management station.

Set Up Windows

The following table shows the Windows setting items. Configure the items that are required for the OS being used.

Table B6-2 Windows Setting Items

Windows setting item	Windows OS (*1)	
	Windows 10	Windows Server 2016, Windows Server 2019, Windows Server 2022
File System	Yes	Yes
Power Options	Yes	Yes
Turning Off Fast Startup	Yes	-
Windows Defender	Yes	Yes
Disk Defragmenter	Yes	Yes
DCOM Settings	Yes	Yes

*1: Yes: Configuration required; -: Not available on the OS.

SEE ALSO

For more information about setting up Windows, refer to:

B3.2, “Setting Up Windows” on page B3-7

Install the License Management Software

Follow these steps to install the license management software.

1. Sign in as an administrative user.
2. Insert the ProSafe-RS software medium into the drive.
   - If the AutoPlay dialog box appears, click [Run Launcher.exe].

- If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the ProSafe-RS software medium.

The installation menu appears.

3. Click [Install License Manager Software].
   The Welcome dialog box appears.

TIP

If the Windows redistributable modules required to run ProSafe-RS are not installed, a dialog box appears, prompting you to install such modules. Follow the instruction of the dialog box.

4. Click [Next].
   The User Information dialog box appears.

TIP

If a different version of control bus driver is already installed, a dialog box appears, prompting you to update the driver. However, you do not need to install the control bus driver on a computer dedicated to license management. Click [OK] to close the dialog box.

5. In the User Information dialog box, enter the name and company name, select the installation folder, and confirm the language for installation, and click [Next].
   The Confirm Settings dialog box appears.
6. Review the installation settings and click [Install].
   A dialog box showing the installation progress appears, and when the license management software installation is complete, the Installation Complete dialog box appears.
7. Select [Yes, I want to set up IT security now.] and click [Finish].
   The IT Security Tool starts.
8. Go on to configure the security settings.

TIP

- When deleting the ProSafe-RS function and installing only the license management software after installing ProSafe-RS, first sign in using an administrative user account and uninstall ProSafe-RS, and then install the license management software.
- When operating with linked domain management, set the standalone management in the Standard model.

9. Select one of the following depending on the user management type.
   - Go to the step 10 to operate with linked domain management.
   - The steps are completed if you operate with user management type other than linked domain management.
10. Join the computer to the domain.
11. Sign in as an administrative user, start Domain Link Management Tool, and link the domain.

IMPORTANT

- If you want to manage other product's licenses on the computer dedicated to license management, you also need to install the license management software from the software medium of that product.
- Settings for using a license management dedicated computer, use IT Security Tool and Domain Link Management Tool started from the Start menu.

SEE ALSO For more information about IT security settings, refer to:

B3.6.1, “Running the IT Security Tool” on page B3-46

For more information about how to uninstall the ProSafe-RS software, refer to:

C5.1.1, “Uninstalling the ProSafe-RS Software” on page C5-3

Create User Accounts

Create accounts for the users who manage licenses.

SEE ALSO For more information about creating user accounts, refer to:

B3.8, “Creating User Accounts” on page B3-56

For more information about the user who manages licenses, refer to:

1.2.2, “User privileges in License Manager” in License Management Guide (IM 32P01C60-01EN)

Configure Windows Environment Settings for Each User

The following table shows the Windows setting items that must be configured for each user. Configure the items that are required for the OS being used.

Table B6-3 Windows Setting Items Required for Each User

Windows setting item	Windows OS (*1)	
	Windows 10	Windows Server 2016, Windows Server 2019, Windows Server 2022
Showing Icons on the Task Tray	Yes	Yes
Stopping the Inactive Window Scrolling Function	Yes	Yes

*1: Yes: Configuration required; -: Not available on the OS.

SEE ALSO For more information about configuring Windows environment settings for each user, refer to:

B3.9, “Configuring Windows Environment Settings for Each User” on page B3-59

B7. Configuring the Hardware of SCS and Devices for Connection between Domains

Configure the hardware of SCS and devices used for connection between domains, such as V net routers and L3 switches.

- On the processor module of SCS, set the V net or Vnet/IP address.
- If a V net router (AVR10D) is used to connect a Vnet/IP domain and a V net domain, the V net router address should be set on the CENTUM side.

CAUTION

When removing and installing the cards to set DIP switches, take measure to prevent the damages caused by static electricity.

SEE ALSO

For more information about antistatic measures, refer to:

Appendix 4., “Antistatic Precautions When Handling Hardware” on page App.4-1

For more information about hardware of SCS, refer to:

B., “Components of SCS” in Hardware User's Guide (IM 32P06C10-01EN)

For more information about setting the processor module of SCS, refer to:

B4.2, “Processor module” in Hardware User's Guide (IM 32P06C10-01EN)

For more information about configurations for N-IO Node Interface Unit, refer to:

F2.1, “Configuring the N-IO node interface unit” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about setting up the hardware when using V net routers, bus converters, and communication gateway, refer to:

CENTUM VP Communication Devices (IM 33J50D10-01EN)

B8. Installing the Functions that Operate with CENTUM VP Licenses

The test function and SOE Viewer of ProSafe-RS operate in coordination with CENTUM VP packages. You can set up a computer so as to use only these functions without using other SENG functions. First, grant the computer licenses (at least one license for the test functions) of the CENTUM VP packages that operate in coordination.

Then, install the ProSafe-RS software from the ProSafe-RS software medium. Licenses for ProSafe-RS software packages are not required.

TIP When you move the CENTUM package from a computer where the function that operates with CENTUM VP licenses is used, fully install the ProSafe-RS software also on the new computer.

Installation on the Computer for Running SCS Simulator

SCS simulator is used in combination with the CENTUM packages listed in the following table. Licenses for ProSafe-RS packages are not required.

Table B8-1 CENTUM Packages Required for SCS Simulator

Model	CENTUM VP package name
VP6E5420	Test Function
VP6E5426	FCS Simulator Package

Perform the following tasks on the computer where the SCS simulator is used. Either task can be performed first.

- Install CENTUM software and grant a license for any of the CENTUM packages in the table.
- Install ProSafe-RS software.

SEE ALSO For more information about installing the CENTUM VP Software, refer to:

CENTUM VP Installation (IM 33J01C10-01EN)

Installation on the Computer for Integration of CENTUM SOE Viewer

In the case of system configurations integrating CENTUM, it is possible to display SOE (Sequence of Events) of SCS on the CENTUM SOE Viewer. This is referred to as integration of CENTUM SOE Viewer. The ProSafe-RS software package licenses are not required.

Perform the following tasks on the computer. Either task can be performed first.

- Install CENTUM software and grant a license for the CENTUM SOE Viewer package (VP6P6920).
- Install ProSafe-RS software.

In order to display SOE of SCS on the CENTUM SOE Viewer, it is necessary to connect the computer and SCS via V net or Vnet/IP.

SEE ALSO For more information about granting a license of CENTUM SOE Viewer Package (VP6P6920), refer to:

License Management (IM 33J01C20-01EN)

C. Maintenance

This section describes the tasks required in the operation and maintenance of stations after they have been newly set up.

C1. Adding Licenses and Changing License Assignments

This section describes how to add licenses, which is required to add new software packages on a station, and how to change the assignments of licenses, which is required to migrate software packages between stations.

C1.1 Adding a License

The procedure for loading an additionally purchased license on the license management station is the same as the procedure for new installation.

SEE ALSO For more information about how to load an additionally purchased license on the license management station, refer to:

3.1, “Reading additional licenses on a license management station” in License Management Guide (IM 32P01C60-01EN)

C1.2 Changing License Assignments

Use the License Manager on the license management station to add the license for the software package additionally required on a license-assigned station.

Also use the License Manager on the license management station to remove the license for the software package no longer required on a license-assigned station.

These operations are called “changing license assignments.”

SEE ALSO For more information about changing license assignments, refer to:

3.2, “Modifying licenses” in License Management Guide (IM 32P01C60-01EN)

C2. Setting Up the Windows Domain Environment Later

This section describes the procedure for the case when you want to change the system that has been built as a Standalone management system to a Domain management system.

Workflow

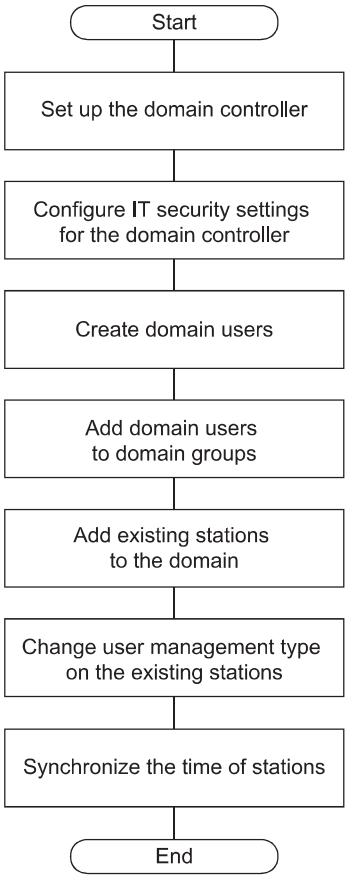


Figure C2-1 Workflow for Setting Up the Windows Domain Environment Later

Setup Procedure

1. Prepare a computer to be used as the domain controller and configure a domain controller on it.
2. Configure IT security settings.
3. Create domain users.
4. Add the domain users to domain groups.
5. Select one of the following depending on which type you want to change the user management type for the existing station.
   - Go to the step 6 to change to linked domain management.
   - Go to the step 9 to change to domain management or combination management.
6. Add the client computer stations to the domain.

7. Link the domain with Domain Link Management Tool.
8. Go to the step 11.
9. Add the client computer stations to the domain.
10. On each station, change the user management type to Domain management or Combination management.
11. Synchronize the time of the stations within the domain.

SEE ALSO

For more information about configuring the domain controller, refer to:

B2.2, “Configuring the domain controller” on page B2-5

For more information about configuring IT security settings on the domain controller, refer to:

B2.3, “Configuring Security Settings for the Domain Controller” on page B2-6

For more information about how to create domain users and add them to domain groups, refer to:

B2.4, “Creating Domain Users” on page B2-13

For more information about how to add client computers to a domain, refer to:

B2.5, “Adding Computers to the Domain” on page B2-17

For more information about how to set up time synchronization within a domain, refer to:

B2.7, “Setting Up Time Synchronization in Windows Domain Environment” on page B2-20

For more information about changing the user management type, refer to:

6.4.2, “For File Server or Domain Controller” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

C3. Backing Up the System

To be prepared for system failures, it is recommended to back up the system periodically. The files in the folders listed in the following table should be regularly backed up:

Table C3-1 Folder Backups

Contents	Folder	Registry	When to back up
Backup of entire Windows	All hard disk	Entire registry	• When changes have been made to the system; for example, after program installation or completion of setup. • After closing all applications
Automation Design Master Database (ADMDB)	-	-	-
ProSafe-RS engineering data	SCS project folders	-	After closing the SENG software

When you back up a system where the Standard model of IT security settings is applied, log on to Windows as an administrative user who has the right to access ProSafe-RS-related folders.

C3.1 Backing Up the Entire Windows

This section describes how to back up the entire Windows.

Backing Up Entire Windows

Back up Windows using a commercially available software program in preparation against disk trouble.

Creating Windows Repair Disk

Installing various application programs on a computer can cause troubles: for example, Windows does not start up, or you cannot log on to Windows. In such cases, if you have a system repair disk and boot disk, you can restore the system to the state at the time you created these disks.

To be prepared for Windows troubles, create a system repair disk and boot disk when you have changed the state of the system by installing a program, changing hardware configuration, etc.

SEE ALSO For more information about how to create a repair disk, refer to:

Windows-related manual or the web site of Microsoft Corporation

C3.2 Backing Up the ProSafe-RS Engineering Data

After performing engineering operations, be sure to back up the engineering data.

Backing Up Projects

You can copy the ProSafe-RS folders to a backup medium using Windows Explorer. It is also possible to use commercially available backup software to back up the folders.

The SCS project folders should be backed up using Version Control Tool.

SEE ALSO For more information about Version Control Tool, refer to:

F5., “Version control” in Engineer's Reference Manual (IM 32P04B10-01EN)

Backing Up to AD Project

Be sure to back up the RS project to AD project before backing up ADMDB or exporting the AD project.

SEE ALSO For more information about how to back up projects to an AD project, refer to:

C1.1, “Tools for management of AD Server and AD projects” in Engineer's Reference Manual (IM 32P04B10-01EN)

C4. Upgrading the ProSafe-RS Software

This section explains the procedure to follow when upgrading the ProSafe-RS software and tasks to be performed after upgrading.

To upgrade the software from the current version to the latest version, perform the tasks in ”Installation for Upgrading”.

To use the added or modified features, read the all cautionary notes including from the current version to the latest version, and perform the tasks in “Settings after Upgrading ProSafe-RS Software”.

IMPORTANT

- When you install for upgrading the version or the revision of this product, the password for the predefined user accounts in this product is reset to the default initial password. Be sure to change the password because operating with the initial password may increase the security risk.
- If SOE OPC Interface Package is used, be sure to change the PSF_PROCESS password after configuring IT security settings. If you changed the password before configuring IT security settings, reset the password that you set.
- If you are going to change the initial password of PSF_PROCESS in an environment that AD Suite is used, activate the system project backup function with ADS Administration Tool before you change the password. If you change the password before activating the system project backup function, the [Backup System Projects prior to AD Project Export] check box in the ADS Administration Tool appears dimmed and you cannot select it. In that case, change the initial password of PSF_PROCESS after activating the system project backup function.
- When changing the password, ensure that the same password is set in the entire system.

SEE ALSO For more information about user accounts that require password change, refer to:

2.2.3, “User/Group Management” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

C4.1 Installation for Upgrading

This section explains the procedure to upgrade the ProSafe-RS software already installed on a computer to a newer version or revision.

TIP

For example, as when upgrading from R3.02 to R4.01, an upgrade where the number next to R is incremented by 1 or more is referred to as a version upgrade. On the other hand, as when upgrading from R4.02 to R4.03, an upgrade where the number immediately next to R remains the same is referred to as a revision upgrade.

The procedure is different between an upgrade of the version and an upgrade of the revision of ProSafe-RS software and some steps are separately explained. Refer to descriptions appropriate to respective cases.

SEE ALSO

For more information about the procedure for upgrading the version of ProSafe-RS Software, refer to:

C4.1.1, “Upgrading the Version of ProSafe-RS Software” on page C4-5

For more information about the procedure for upgrading the revision of ProSafe-RS Software, refer to:

C4.1.2, “Upgrading the Revision of ProSafe-RS Software” on page C4-9

Precautions for Revision Upgrade

Observe the following precautions when you upgrade the ProSafe-RS software.

- If the revision of ProSafe-RS prior to the revision upgrade is R4.03 or later, distribute and accept the upgrade license. If the installation is performed without distributing and accepting the upgrade license, an error dialog will appear and you will not be able to complete the installation.

  This is not necessary if the upgrade license has already been accepted.

- When you upgrade the ProSafe-RS software, install a new revision of software without uninstalling the earlier revision.

  If you uninstall R4.03 or later revision of ProSafe-RS software, a new revision of ProSafe-RS software cannot be installed. In that case, reinstall the uninstalled ProSafe-RS software again and then install the new revision.

IMPORTANT

The software release number must be the same between all the SENGs which is for engineering SCS projects in the RS project, and SENGs which is for engineering SCSs that perform inter-SCS safety communication each other. Also, you must upgrade the revision of SCS projects that perform inter-SCS safety communication.

- Once opening an existing SCS project or creating a new SCS project using newer revision software in SENG, the SCS project cannot be opened using older revision software.
- The SCS system program release number of SCSs in a system should basically be the same, but mixture of different release numbers is allowed.

SEE ALSO

For more information about upgrading the revision of an SCS project, refer to:

C4.2.2, “Upgrading an SCS project” on page C4-18

Upgrading the Revision of Products When Two or More Upgrade License Support Products are Installed

When CENTUM VP R6.04 or later and ProSafe-RS R4.03 or later, both of which support upgrade licenses, are installed on the same computer, follow these steps to upgrade them:

1. Distribute the upgrade licenses of the respective coexisting products.
2. Upgrade the revision of each product.

Items to be Prepared

Prepare the following items so that they are at hand before upgrading the ProSafe-RS software.

- ProSafe-RS software medium
- ProSafe-RS license medium
- ProSafe-RS license sheet (with project ID)

User Who Performs Update Installation

When update installation is performed, IT security settings are configured following the installation of the ProSafe-RS software. Update installation must be performed by a user who belongs to the groups shown in the following table.

Table C4.1-1 Groups to Which the User Who Performs Update Installation Belongs

Currently applied security model and user management type	Security model and user management type to be applied			
	Legacy model	Standard model		
		Standalone type	Linked domain management	Domain/Combination type
Legacy model	Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group		Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group	• Domain user who belongs to the Domain Admins domain group and PSF_MAINTENANCE domain group (*1) • Domain user who belongs to the Administrators local group and PSF_MAINTENANCE local group (*1) • Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group (*1) (*2) (*3)

Continues on the next page

Table C4.1-1 Groups to Which the User Who Performs Update Installation Belongs (Table continued)

Currently applied security model and user management type		Security model and user management type to be applied			
		Legacy model	Standard model		
			Standalone type	Linked domain management	Domain/Combination type
Standard model	Standalone type	Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group		Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group (*4)	• Domain user who belongs to the Administrators local group and PSF_MAINTENANCE local group (*1) • Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group (*1) (*2) (*3)
	Linked domain management	Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group	• Domain user who belongs to the Domain Admins domain group and PSF_MAINTENANCE domain group (*4) • Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group (*4)	• Domain user who belongs to the Domain Admins domain group and PSF_MAINTENANCE domain group (*1) • Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group (*1)	• Domain user who belongs to the Domain Admins domain group and PSF_MAINTENANCE domain group (*1) • Local user who belongs to the Administrators local group and PSF_MAINTENANCE local group (*1)
	Domain/Combination type	Local user who belongs to the Administrators local group and PSF_MAINTENANCE_LCL local group (*5)		Local user who belongs to the Administrators local group and PSF_MAINTENANCE_LCL local group (*1) (*2)	• Domain user who belongs to the Domain Admins domain group and PSF_MAINTENANCE domain group (*1) • Domain user who belongs to the Administrators local group and PSF_MAINTENANCE_LCL local group (*1) • Local user who belongs to the Administrators local group and PSF_MAINTENANCE_LCL local group (*1) (*2) (*3)

*1: Log on while the computer is added to the domain.
*2: The domain user name and password must be entered during installation.
*3: When this user applies IT security and uses iDefine interface package, the following steps must be performed as a domain user who belongs to the Domain Admins domain group or as a domain user who belongs to the Administrators local group.
1. Run the 32 bit Command Prompt (%SystemDrive%\Windows\SysWOW64\cmd.exe) as Administrator.
2. Run either of the following batch files appropriate to the user management type.
%ProgramFiles(x86)%\YOKOGAWA\IA\iPCS\Platform\Security\Program
For Domain management: PSF_SetupSMSvcHostConfigDOM.cmd
For Combination management: PSF_SetupSMSvcHostConfigCMB.cmd
*4: No need to reconfigure the IT Security Tool as the settings are made in Domain Link Management Tool.
*5: Remove the computer from the domain before you change the IT security setting.

C4.1.1 Upgrading the Version of ProSafe-RS Software

The following flowchart illustrates the flow of installation for upgrading the version of ProSafe-RS software.

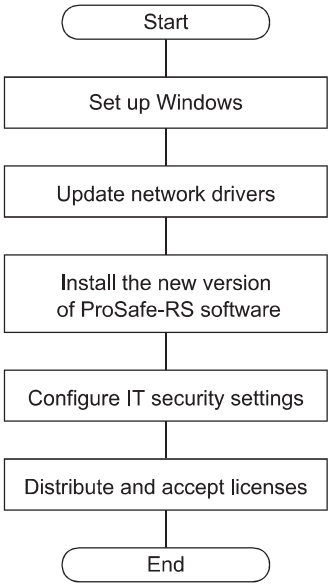


Figure C4.1.1-1 Flow of installation for upgrading the version

■ Set Up Windows

Configure Windows settings.

SEE ALSO For more information about procedures for setting up Windows, refer to:

B3.2, “Setting Up Windows” on page B3-7

■ Installing Latest Network Driver

Before upgrading the software, install the latest network driver (included in the new ProSafe-RS software version to be installed).

This section explains how to update the control bus driver, Vnet/IP open communication driver, and the Vnet/IP Interface Package.

● Updating the Control Bus Driver

Follow these steps to update the control bus driver:

1. Uninstall the control bus driver.
2. Install the latest version of the control bus driver.
3. Configure Windows network settings.

SEE ALSO For more information about the uninstallation procedure of control bus driver, refer to:

“■ Uninstalling Control Bus Driver” on page C5-5

For more information about installing the control bus driver, refer to:

B3.3.1, “Installing the Control Bus Driver” on page B3-19

For more information about the procedure for configuring Windows network settings, refer to:

B3.3.5, “Configuring Windows Network Settings” on page B3-27

Updating the Vnet/IP Open Communication Driver

The procedure to update the Vnet/IP open communication driver is the same as the procedure to install the Vnet/IP open communication driver. If it is necessary to update the Vnet/IP open communication driver, you can select [INSTALL] in the Setup dialog box.

Follow these steps to update the Vnet/IP open communication driver:

1. Install the latest version of the Vnet/IP open communication driver.
2. Be sure to restart the computer after updating the Vnet/IP open communication driver.
3. Configure Windows network settings.

SEE ALSO For more information about installing the Vnet/IP open communication driver, refer to:

B3.3.3, “Installing the Vnet/IP Open Communication Driver” on page B3-22

For more information about the procedure for configuring Windows network settings, refer to:

B3.3.5, “Configuring Windows Network Settings” on page B3-27

Updating the Vnet/IP Interface Package

If a virtual machine is used, update the Vnet/IP Interface Package.

Follow these steps to update the Vnet/IP Interface Package:

1. Uninstall the Vnet/IP Interface Package.
2. Install the latest Vnet/IP Interface Package.
3. Configure Windows network settings.

SEE ALSO For more information about the procedure to uninstall the Vnet/IP Interface Package, refer to:

“■ Uninstalling the Vnet/IP Interface Package on a Virtual Machine” on page C5-7

For more information about the procedure to install the Vnet/IP Interface Package, refer to:

B3.3.4, “Installing the Vnet/IP Interface Package on a Virtual Machine” on page B3-24

For more information about the procedure for configuring Windows network settings, refer to:

B3.3.5, “Configuring Windows Network Settings” on page B3-27

Checking Inconsistency in TCP/IP Settings

After updating the network driver, run the TCP/IP Inconsistency Detection Tool. If any inconsistency is detected in the settings, use the TCP/IP Inconsistency Repair Tool and then configure the TCP/IP settings again.

SEE ALSO For more information about the TCP/IP Inconsistency Detect Tool and TCP/IP Inconsistency Repair Tool, refer to:

“■ Procedure 5: Repair TCP/IP Settings” on page B3-35

Procedure for Update Installation

Follow these steps below to upgrade the ProSafe-RS software.

1. Log on as an administrative user.
2. Terminate all running applications, including resident programs such as anti-virus software.

3. Insert the ProSafe-RS software medium to the drive. The ProSafe-RS installation menu appears.
   If the installation menu does not appears, double-click Launcher.exe in the top folder of the software medium using Explorer.
4. Click [ProSafe-RS software].
   The Welcome dialog box appears if all the Windows redistribution modules required for ProSafe-RS have been installed. Proceed to step 6.
   The dialog box for confirming module installation appears if any of Windows redistribution modules required for ProSafe-RS have not been installed.
5. Click [Install] in the module installation confirmation dialog box. Module installation starts.
6. After the installation is completed, click [Close].
   The window closes.

IMPORTANT

If the installation fails, reinstall referring to the installation procedure for the new setup.

7. If the dialog box for confirming the privilege setting appears, reboot the computer and log on again.
   a. Click [OK] and reboot the computer.
   b. After rebooting the computer, log on again as the same user. The Welcome dialog box appears automatically.
8. Click [Next] in the welcome dialog box.
   The Confirm Settings dialog box appears.

TIP

- If a different version of control bus driver or Vnet/IP open communication driver is already installed, a dialog box appears, prompting you to update the driver. Confirm the message and click [OK]. To update the control bus driver, uninstall the existing driver and then install the new one after you install the ProSafe-RS software. To update the Vnet/IP open communication driver, install the new driver after you install the ProSafe-RS software.
- After updating the Vnet/IP open communication driver, disable the driver if the computer is to be connected to Ethernet.

9. Check the installation settings in the Confirm Settings dialog box and click [Install]. The installation of ProSafe-RS starts and the dialog box showing installation progress status appears.
10. When you have completed the installation of the ProSafe-RS software, the installation complete dialog box appears.
    If there are no products to be installed subsequently, select [Yes, I want to set up IT security now.] and click [Finish].

TIP

If you intend to continue to install other YOKOGAWA products, select [No, I want to install other software products.] and click [Finish].

IMPORTANT

If you select [No, I want to install other software products.] here, you must perform IT security settings when you install the last product.

SEE ALSO For more information about the installation procedure for new setup, refer to:

"■ Installation Procedure" on page B3-40

For more information about configuring the IT security settings, refer to:

B3.6, "Configuring IT Security Settings" on page B3-44

When Upgrading the Version during Linked Domain Management Operation

Follow these steps to upgrade the version during linked domain management operation:

1. If you have performed a version upgrade installation, sign in as a local administrator or domain administrator.
2. Start the IT Security Tool and apply the IT security for standalone management.
3. Start Domain Link Management Tool as a local administrator or domain administrator, and apply the domain link management.

SEE ALSO For more information about running the IT Security Tool, refer to:

B3.6.1, "Running the IT Security Tool" on page B3-46

For more information about running the Domain Link Management Tool, refer to:

B3.6.3, "Running Domain Link Management Tool" on page B3-52

Additional Execution of IT Security Configuration

If you are upgrading from R2 where the standard model of security settings are applied, you must configure IT security settings again in this way: after configuring the IT security settings following the installation of the product, reboot the computer and then start the IT Security Tool from the Start menu to configure the IT security settings.

Tasks Related to Licenses

In the case of a version upgrade, perform the tasks related to licenses after configuring IT security.

SEE ALSO For more information about tasks related to licenses, refer to:

B3.7, "Distributing and Accepting Licenses" on page B3-55

C4.1.2 Upgrading the Revision of ProSafe-RS Software

The following flowchart illustrates the flow of installation for upgrading the revision of ProSafe-RS software.

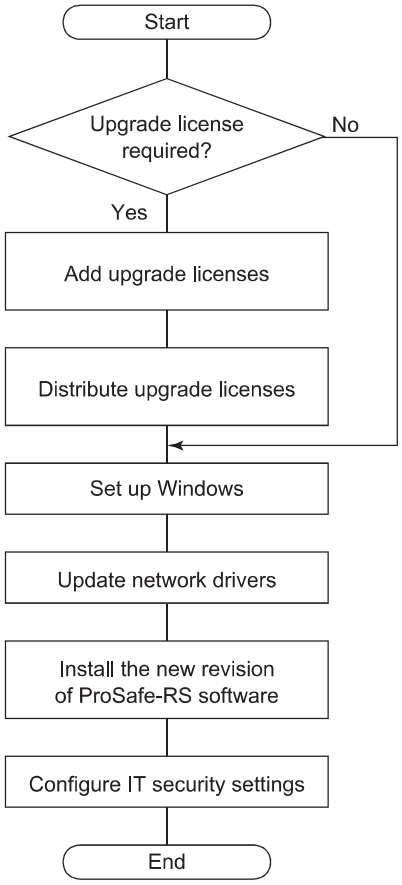


Figure C4.1.2-1 Flow of installation for upgrading the revision

SEE ALSO For more information about details of the upgrade license, refer to:

1., “Overview of license management” in License Management Guide (IM 32P01C60-01EN)

Adding an Upgrade License

Adding an upgrade license enables you to distribute the upgrade license. If an upgrade license is necessary, add the upgrade license by using License Manager on the license management station.

Distributing an Upgrade License

Distributing an upgrade license enables you to install upgrades of the ProSafe-RS software on a license-assigned station. If an upgrade license is necessary, distribute the upgrade license to the license-assigned station from the license management station.

TIP

- If an upgrade license is distributed alone, the license will be accepted automatically.
- The upgrade license can be distributed simultaneously with a software license. In such case, by accepting the license on the license-assigned station, the upgrade license and software license will both be accepted.

SEE ALSO For more information about how to add and distribute an upgrade license, refer to:

5., “Working with upgrade licenses” in License Management Guide (IM 32P01C60-01EN)

Setting Up Windows

Configure Windows settings.

SEE ALSO For more information about procedures for setting up Windows, refer to:

B3.2, “Setting Up Windows” on page B3-7

Installing Latest Network Driver

Before upgrading the software, install the latest network driver (included in the new ProSafe-RS software version to be installed).

This section explains how to update the control bus driver, Vnet/IP open communication driver, and the Vnet/IP Interface Package.

Updating the Control Bus Driver

Follow these steps to update the control bus driver:

1. Uninstall the control bus driver.
2. Install the latest version of the control bus driver.
3. Configure Windows network settings.

SEE ALSO For more information about the uninstallation procedure of control bus driver, refer to:

“■ Uninstalling Control Bus Driver” on page C5-5

For more information about installing the control bus driver, refer to:

B3.3.1, “Installing the Control Bus Driver” on page B3-19

For more information about the procedure for configuring Windows network settings, refer to:

B3.3.5, “Configuring Windows Network Settings” on page B3-27

Updating the Vnet/IP Open Communication Driver

The procedure to update the Vnet/IP open communication driver is the same as the procedure to install the Vnet/IP open communication driver. If it is necessary to update the Vnet/IP open communication driver, you can select [INSTALL] in the Setup dialog box.

Follow these steps to update the Vnet/IP open communication driver:

1. Install the latest version of the Vnet/IP open communication driver.
2. Be sure to restart the computer after updating the Vnet/IP open communication driver.
3. Configure Windows network settings.

SEE ALSO For more information about installing the Vnet/IP open communication driver, refer to:

B3.3.3, “Installing the Vnet/IP Open Communication Driver” on page B3-22

For more information about the procedure for configuring Windows network settings, refer to:

B3.3.5, “Configuring Windows Network Settings” on page B3-27

Updating the Vnet/IP Interface Package

If a virtual machine is used, update the Vnet/IP Interface Package.

Follow these steps to update the Vnet/IP Interface Package:

1. Uninstall the Vnet/IP Interface Package.
2. Install the latest Vnet/IP Interface Package.
3. Configure Windows network settings.

SEE ALSO For more information about the procedure to uninstall the Vnet/IP Interface Package, refer to:

"■ Uninstalling the Vnet/IP Interface Package on a Virtual Machine" on page C5-7

For more information about the procedure to install the Vnet/IP Interface Package, refer to:

B3.3.4, "Installing the Vnet/IP Interface Package on a Virtual Machine" on page B3-24

For more information about the procedure for configuring Windows network settings, refer to:

B3.3.5, "Configuring Windows Network Settings" on page B3-27

Checking Inconsistency in TCP/IP Settings

After updating the network driver, run the TCP/IP Inconsistency Detection Tool. If any inconsistency is detected in the settings, use the TCP/IP Inconsistency Repair Tool and then configure the TCP/IP settings again.

SEE ALSO For more information about the TCP/IP Inconsistency Detect Tool and TCP/IP Inconsistency Repair Tool, refer to:

"■ Procedure 5: Repair TCP/IP Settings" on page B3-35

Procedure for Update Installation

Follow these steps below to upgrade the ProSafe-RS software.

1. Log on as an administrative user.
2. Terminate all running applications, including resident programs such as anti-virus software.
3. Insert the ProSafe-RS software medium into the drive. The ProSafe-RS installation menu appears.
   If the installation menu does not appear, double-click Launcher.exe in the top folder of the software medium using Explorer.
4. Click [ProSafe-RS software].
   The Welcome dialog box appears if all the Windows redistribution modules required for ProSafe-RS have been installed. Proceed to step 6.
   The dialog box for confirming module installation appears if any of Windows redistribution modules required for ProSafe-RS have not been installed.
5. Click [Install] in the module installation confirmation dialog box. Module installation starts.
6. After the installation is completed, click [Close].
   The window closes.

IMPORTANT

If the installation fails, reinstall referring to the installation procedure for the new setup.

7. If the dialog box for confirming the privilege setting appears, reboot the computer and log on again.
   a. Click [OK] and reboot the computer.
   b. After rebooting the computer, log on again as the same user. The Welcome dialog box appears automatically.
8. Click [Next] in the welcome dialog box.
   The Confirm Settings dialog box appears.

TIP

- If a different version of control bus driver or Vnet/IP open communication driver is already installed, a dialog box appears, prompting you to update the driver. Confirm the message and click [OK]. To update the control bus driver, uninstall the existing driver and then install the new one after you install the ProSafe-RS software. To update the Vnet/IP open communication driver, install the new driver after you install the ProSafe-RS software.
- After updating the Vnet/IP open communication driver, disable the driver if the computer is to be connected to Ethernet.

9. Check the installation settings in the Confirm Settings dialog box and click [Install]. The installation of ProSafe-RS starts and the dialog box showing installation progress status appears.
10. When you have completed the installation of the ProSafe-RS software, the installation complete dialog box appears.
    If there are no products to be installed subsequently, select [Yes, I want to set up IT security now.] and click [Finish].

TIP

If you intend to continue to install other YOKOGAWA products, select [No, I want to install other software products.] and click [Finish].

IMPORTANT

If you select [No, I want to install other software products.] here, you must perform IT security settings when you install the last product.

SEE ALSO

For more information about the installation procedure for new setup, refer to:

"■ Installation Procedure" on page B3-40

For more information about configuring the IT security settings, refer to:

B3.6, "Configuring IT Security Settings" on page B3-44

■ When Upgrading the Revision during Linked Domain Management Operation

Follow these steps to upgrade the revision to R4.07 or later during linked domain management operation:

1. If you have performed a revision upgrade installation, sign in as a local administrator or domain administrator.
2. Start the IT Security Tool and apply the IT security for standalone management.
3. Start Domain Link Management Tool as a local administrator or domain administrator, and apply the domain link management.

SEE ALSO For more information about running the IT Security Tool, refer to:

B3.6.1, “Running the IT Security Tool” on page B3-46

For more information about running the Domain Link Management Tool, refer to:

B3.6.3, “Running Domain Link Management Tool” on page B3-52

C4.2 Settings after Upgrading ProSafe-RS Software

This section describes the tasks and precautions required after upgrading the SENG software.

Because the SCS databases and SCS system programs that SENG manages are basically upward compatible, there is no need to modify the engineering data created with earlier version software. However, in order to use the new features supported by the newer SCS system program, re-creation of the SCS project or offline downloading of database to SCS may be required after upgrading the SENG.

TIP

For computers that do not have Adobe Acrobat installed, we recommend that you upgrade the software for viewing online manuals to the recommended version of Adobe Acrobat Reader described in this manual.

SEE ALSO

For more information about configuration of Adobe Acrobat Reader, refer to:

B4.1, “Setting the Manual Browsing Environment” on page B4-2

For more information about release numbers of the SENG software in each software release and compatibility in inter-SCS safety communication between different revisions, refer to:

Appendix 6., “Compatibility between Revisions and Cautionary Notes for Upgrading” on page App.6-1

C4.2.1 Updating the engineering data after an upgrade

To maintain the use of existing engineering data after you upgrade the ProSafe-RS software, you must upgrade the AD Server data, and upgrade the revision of the AD project data and the RS project data before you start the engineering.

Procedure for starting engineering

The following figure shows the procedure for starting engineering.

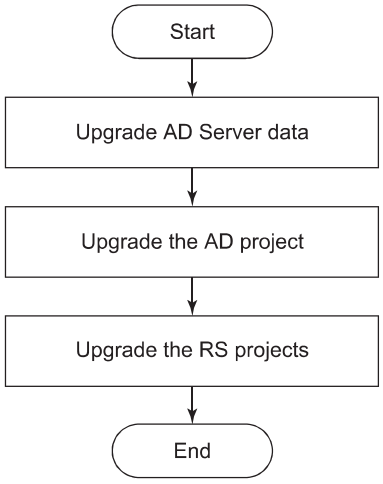


Figure C4.2.1-1 Procedure for starting engineering

TIP

For some steps in this procedure, upgrading may not be required. In this case, do not quit the engineering at such a step and proceed to the next step.

Upgrading the AD Server data

The following AD Server data should be upgraded:

- Back-up and restore history of the ADMDB
- Export and import history information of AD projects
- Option settings

To perform this task, use the ADS Administration Tool on the computer with AD Server.

Upgrading the AD Server data

Follow these steps to upgrade the AD Server data:

1. Log on to the computer with AD Server. If the IT security model is the Standard model or Strengthened model, log on as a member of the ADS_MANAGER or ADS_MANAGER_LCL group.
2. Start the ADS Administration Tool.
   If upgrading of the AD server data is required, the AD Server Data Upgrade Dialog Box appears.
3. Click [OK].
   Data upgrade starts. When the upgrade is complete, the Upgrade Complete Dialog Box appears.
4. Click [Close AD Server Administration Tool].
   The AD Server restarts to complete the data upgrade.

TIP

Performing this task does not upgrade AD project data.

Upgrading an AD project

You must upgrade the AD project data.

To perform this task, use AD Organizer on a computer with the safety system generation function.

If there are multiple computers with the safety system generation function, you can use any of these computers.

Upgrading an AD project

IMPORTANT

Before you upgrade an AD project, you must exit AD Organizer on all computers except for the computer that you are about to upgrade.

Follow these steps to upgrade an AD project:

1. Log on to the computer with the safety system generation function as a user having rights to modify all data in the AD project.

TIP

During upgrade of an AD project, AD project files are checked out, updated, and checked in. If you log on as a user who does not have modifying access rights, upgrade of the AD project fails with an error.

You must log on as a user whose user role is RS Lead Engineer and whose access scope is All Scope.

2. Start AD Organizer.
   If upgrading of an AD project is required, the Upgrade dialog box appears.
3. Click [Yes].
   The upgrade for the AD project starts. When the upgrade is complete, the Update Complete dialog box appears.

IMPORTANT

While revision upgrade of the AD project proceeds, make sure that communication between AD Server and AD Organizer is not interrupted. If the communication is interrupted, upgrade of the AD project fails with an error.

When upgrading the AD project fails with an error due to an interruption, check to see if there are any checked-out files in the AD project. If there are any, forcibly cancel the checked-out status by using the ADS Administration Tool and start AD project upgrade again.

4. Click [OK].

SEE ALSO

For more information about how to check the Checked-out Status of AD project files, refer to:

C1.2.5, “Forcibly canceling the checked-out status of currently checked-out files” in Engineer's Reference Manual (IM 32P04B10-01EN)

Upgrading an RS project

You can upgrade an RS project on a computer with the safety system generation function.

If there are multiple computers with the safety system generation function, perform the tasks on any one of the computers.

Upgrading an RS project

Follow these steps to upgrade an RS project:

1. Log on as a user with rights to modify the RS project.
   For example, log on with the rights of a user whose user role is RS Lead Engineer or RS Engineer.
2. Start AD Organizer.
3. Upgrade all SCS projects under the RS project.
4. In System Structure Navigator, select the RS project.
5. From the sub menu of System Structure Navigator, select [Back up].
   A confirmation dialog box appears.
6. Click [Yes].
   The upgraded RS project is backed up.

C4.2.2 Upgrading an SCS project

After you install the latest revision on SENG or AD Server and upgrade an AD project and an RS project, open SCS projects. The SCS projects are upgraded. Steps are described in the following procedure A.

Procedure A: Opening SCS Projects

Use SCS Manager to open an SCS project in an earlier revision. The SCS project is upgraded.

You can upgrade the SCS project without interrupting SCS operation. The scope of online changes is the same as the earlier revision.

IMPORTANT

- If you upgrade an SCS project, you must upgrade the SCS projects of all the SCSs that perform inter-SCS safety communication with this SCS. Otherwise, an error may occur during build.
- When opening a project of R4.05 or later, specify PRJlibrary.accdb. When opening a project before R4.05, specify PRJlibrary.mdb. PRJlibrary.mdb is converted to PRJlibrary.accdb by upgrading the revision.
- The SCS project created by an earlier revision cannot be opened in Read-Only mode.

  Such SCS projects must be opened in Read-Write mode. To open the project with password, the password needs to be entered and then open the project in the Read-Write status.
- It is necessary to use the newer revision SCS Manager at least once to open the library created by older revision SCS Manager.

Follow these steps to call SCS Manager from AD Organizer:

1. In System Structure Navigator, select the SCS project you want to upgrade and select [SCS Manager] from the context menu.
   If upgrading of the SCS project is required, a dialog box appears, asking you whether to upgrade the SCS project.
2. Click [Yes].
   Upgrading of the SCS project starts. When the upgrade is complete, the Upgrade Complete dialog box appears.
3. Click [OK].
   SCS Manager starts, and the steps are completed.

C4.2.3 Cautionary notes for upgrading to R4.10

This section provides cautionary notes and actions required for a revision upgrade from R4.09 to R4.10. When you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.

IMPORTANT

When integrating ProSafe-RS with CENTUM VP, use the R6.11 or a later version of CENTUM VP for the installation on the same computer.

In R4.01 or later, be sure to register the RS project in an AD project regardless of the engineering method.

SEE ALSO

For more information about creating an AD project, refer to:

"■ Creating AD projects" in C1.2.1, "Creating and deleting AD projects" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects in an AD project, refer to:

C1.2.3, "Registering RS projects in the AD project" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about cautionary notes when upgrading the revision to ProSafe-RS R4.09, refer to:

Appendix 6.10, "Cautionary notes for upgrading to R4.09" on page App.6-28

For more information about the detailed operation procedure required after the revision upgrade, refer to:

C4.2.4, "Procedures for using new functions" on page C4-22

■ Software revisions

The respective software release numbers of R4.10 are as follows:

Software release number R4.10.xx (*1)

- SENG software release number: R4.10.xx(*1)
- SCS system program release number: R4.10.xx(*1)

*1: The last two digits of the revision number will be changed in accordance with the software revisions after the release of R4.10.00.

The database revision of an SCS project that is created by SENG with software release number R4.10.xx will be R4.10.00.

● Control bus drivers

The control bus drivers that are installed on the computer must be upgraded to the version supplied in R4.10.

● Inter-SCS safety communication

This section describes the SCS system program release numbers that support inter-SCS safety communication.

SEE ALSO For more information about compatibility in inter-SCS safety communication between different revisions, refer to:

"● Important issues to consider" in "■ Precaution for engineering" in A7., "Inter-SCS safety communication" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

For more information about the SCS system program release numbers that support inter-SCS safety communication, refer to:

Appendix 4.2, "Inter-SCS safety communication in a V net domain" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Basic procedure for upgrading

To use the added or modified features, install the ProSafe-RS software R4.10 or later and open the existing SCS projects ("Procedure A").

SEE ALSO For more information about operations of "Procedure A", refer to:

"■ Procedure A: Opening SCS Projects" on page C4-18

■ Procedures for using added and modified features

The basic upgrading procedures are not enough to use the following features that have been added or modified in R4.10. After you upgrade the SENG software to R4.10, you must perform offline download to the SCS and other operations. The following procedures are required to use the new features.

SEE ALSO For more information about operation "Procedure B" to "Procedure F" for using new functions, refer to:

C4.2.4, "Procedures for using new functions" on page C4-22

● Diagnostic information indicator system function blocks

To use the diagnostic information indicator system function blocks added in R4.10 (SYS_CPUDSP, SYS_NODEPSU, SYS_N_NODEPSU), you need to perform "Procedure C" on an SENG of R4.10. SYS_CPUDSP and SYS_NODEPSU can be used on SSC50, S2SC70, SSC57, and L1SC70. SYS_N_NODEPSU can be used only on S2SC70.

■ Precautions Regarding the Policy Distributed from GPO

If the following policy is distributed from the domain controller by the settings in the GPO file, it is necessary to change the setting of the domain controller and each computer after upgrading the version in order to deal with the problem of Windows.

- For IT security version 1.0 and strengthened model:

  The setting item is [Computer Configuration] > [Policy] > [Windows Settings] > [Security Settings] > [Local Policies] > [Audit Policy] > [Audit Object Access].

- For IT security version 2.0 and standard or strengthened model:

  The setting item is [Computer Configuration] > [Policy] > [Windows Settings] > [Security Settings] > [Advanced Audit Policy Configuration] > [Audit Policy] > [Object Access] > [Audit Removable Storage].

This setting is applied to each computer from the domain controller by the settings in the GPO file of the following versions:

- R4.03.00 to R4.09.00

TIP After changing the setting, the above item will no longer be subject to consolidated management by the GPO file, so set it with the IT Security Tool.

Changing Group Policy on Domain Controller

Follow these steps to change the group policy on the domain controller:

1. Sign in to the domain controller as a user with administrative rights.
2. Open the Control Panel and select [Administrative Tools] > [Group Policy Management]. The Group Policy Management dialog box appears.
3. Right-click the group policy object that applies to each computer and select [Edit...]. Group Policy Management Editor appears.
4. For IT security version 1.0 and strengthened model, select [Audit Object Access] and select [Not defined]. For IT security version 2.0 and standard or strengthened model, select [Audit Removable Storage] and select [Not Configured].

Setting the Registry on Each Computer

After changing the group policy on the domain controller, set the registry on each computer. Follow these steps to set the registry on each computer:

1. Sign in as a user with administrative rights on each computer.
2. Run the command from the Command Prompt by either of the following operations.
   - When using the ProSafe-RS software medium, insert the medium into the drive

     ```
     <Software medium drive>:\ProSafe-RS\Security\RepairRemovableStoragePolicies.cmd
     ```

   - If there is no medium, access the installation directory

     ```
     <ProSafe-RS installation folder>\Program Files (x86)\YOKOGAWA\IA\iPCS\Platform\Security\Program\RepairRemovableStoragePolicies.cmd
     ```

   The correct value is set in the corresponding registry.

Steps when an SCS project is already placed on another computer such as a file server

If an SCS project is already placed on a file server PC that is different from the SENG PC, files in the SCS project database may be corrupted while the SCS project is operated on the SENG PC. When an SCS project is already placed on a PC such as a file server which is different from the SENG PC that operates the SCS project, make sure to implement the avoidance described in SEE ALSO to prevent file corruption in the SCS project database.

SEE ALSO For more information about avoidance, refer to:

"■ Precautions when Placing the SCS Project on Another PC such as a File Server" in 1.2, "Engineering" in ProSafe-RS Release Information (IM 32P01A50-01EN)

Cautionary notes for upgrading when ALE111 is used

You must be careful when upgrading the system if ALE111 is used for Modbus slave or DNP3 communication.

SEE ALSO For more information about the precautions when upgrading a system where ALE111 is used for Modbus slaveor DNP3communication, refer to:

"■ Cautionary Notes for Upgrading When ALE111 is Used" on page App.6-5

C4.2.4 Procedures for using new functions

This section describes the detailed operation procedures required after the revision upgrade, which is described in the precautions for upgrade of each revision.

After upgrading the ProSafe-RS software, the following procedures need to be performed.

What procedure needs to be performed depends on what new features to be used. User needs to run the following procedures in accordance with each guideline of the revision upgrade procedure.

- Procedure B: Master Database Offline Download
- Procedure C: Creating New SCS Project and Offline Download
- Procedure D: Setting Definition Items for New Features and Offline Download
- Procedure E: Clean Project, Build, and Offline Download
- Procedure F: Setting Definition Items for New Features, Clean Project, Build, and Offline Download

SEE ALSO For more information about procedure A: opening SCS projects, refer to:

"■ Procedure A: Opening SCS Projects" on page C4-18

For more information about the procedures to use new features in each revision, refer to:

Appendix 6.5, "Cautionary Notes for Revision Upgrade to R4.04" on page App.6-15

For more information about procedure of upgrading the system while maintaining the existing engineering data, refer to:

C4.2.1, "Updating the engineering data after an upgrade" on page C4-15

■ Procedure B: Master Database Offline Download

For using the new features, this procedure may be necessary.

After upgrading the SENG, perform Master Database Offline Download to the SCS. Re-testing of SCS application is not required.

The outline of the procedure is as follows:

1. Run Procedure A.
2. Offline download to the SCS using Master Database Offline Download.

SEE ALSO For more information about the procedure of Master Database Offline Download, refer to:

I4.4, "Master database offline download" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Procedure C: Creating New SCS Project and Offline Download

For using the new features, this procedure may be necessary.

After upgrading SENG, create a new SCS project and remake the existing SCS project and then offline download the SCS project.

The procedure is the same as creating a new SCS project. And it is roughly as follows:

1. Create a new project and enter all the project settings.
   The existing SCS project can be upgraded to a later revision by using Import/Export functions. Upgrading the SENG to a newer revision and creating a new SCS project, the whole existing project data can be transferred to the new SCS project.

TIP

If the new SCS project uses a library, the library must be opened by a new-revision SCS Manager. However, if the library POU uses FB/FU supported only by a new revision, create a new library.

When you have upgraded an SENG, you must ensure that all SCS projects and library are of the same revision as the upgraded SENG.

Follow these steps to upgrade the revision of SCS and library:

1. Open each original library projects to upgrade. Then, copy the library to the predetermined folder, LIBRARIES, of the SCS project that uses the library.
2. Open each SCS project to upgrade.

If a project-level password is set for the SCS project or library, you have to enter the password and open it in ReadWrite mode in order to upgrade. If you do not know the password, contact the creator of the SCS project and library.

2. Run build, and check the project data using Integrity Analyzer/Cross Reference Analyzer.
3. Offline download the project.

IMPORTANT

The SCS project and library created by an SENG in a revision later than the currently used revision cannot be used.

- The SCS project created or opened by a new revision of SENG cannot be opened by an SENG in an earlier revision.
- The library created or opened by a new revision of SENG cannot be added to the SCS project of an earlier revision.

SEE ALSO

For more information about the procedures for transferring the existing SCS project using Import/Export functions, refer to:

E2., “Import/Export function” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about the procedure for migrating existing SCS projects engineered by I/O list engineering, refer to:

“■ Regenerating an SCS project with the new revision” in E3.3, “Data transfer procedure during SCS project regeneration” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about areas in which re-testing is required after using the Import/Export function, refer to:

“■ Confirming a regenerated project” in E3.3, “Data transfer procedure during SCS project regeneration” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about procedures for offline download, refer to:

“● Offline download process in I/O list engineering” in “■ Procedure for offline download” in C7., “Offline download to the target SCS” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Procedure D: Setting Definition Items for New Features and Offline Download

Some new features require this procedure.

Install the new revision of SENG software, set the definition items for the new features, and offline download the project.

The procedure is as follows:

1. Using SCS Manager, open the old-revision project.
2. Set the definition items for the new features.

The items to be set are described in the section of upgrading procedures for each software release number.

3. Run Build. Then use Integrity Analyzer and Cross Reference Analyzer for approval check.

IMPORTANT

Even if all POUs are displayed in green in the result of checking by Cross Reference Analyzer, further check is required if Cross Reference Analyzer is unable to detect differences related to the definition items of the new features.

4. Offline download the project.

SEE ALSO For more information about the items that cannot be detected by Cross Reference Analyzer, refer to:

"■ Other changes not detectable by Cross Reference Analyzer" in C5.2.5, "Precautions on Cross Reference Analyzer" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Procedure E: Clean Project, Build, and Offline Download

Some new features require this procedure.

After upgrading the SENG, run Clean Project and Build for the existing project, and offline download the project.

The procedure is as follows:

1. Using SCS Manager, open the old-revision project.
2. Run Clean Project.
3. Run Build. Then use Integrity Analyzer and Cross Reference Analyzer for approval check. In the check using Cross Reference Analyzer, make sure that all POUs are displayed in green.
4. Offline download the project.

■ Procedure F: Setting Definition Items for New Features, Clean Project, Build, and Offline Download

Some new features require this procedure.

This procedure consists of "Procedure D" plus Clean Project.

The procedure is as follows:

1. Using SCS Manager, open the old-revision project.
2. Set the definition items for the new features.
   The items to be set are described in the section of upgrading procedures for each software release number.
3. Run Clean Project.
4. Run Build. Then use Integrity Analyzer and Cross Reference Analyzer for approval check.

IMPORTANT

Even if all POUs are displayed in green in the result of checking by Cross Reference Analyzer, further check is required if Cross Reference Analyzer is unable to detect differences related to the definition items of the new features.

5. Offline download the project.

SEE ALSO

For more information about the items that cannot be detected by Cross Reference Analyzer, refer to:

"■ Other changes not detectable by Cross Reference Analyzer" in C5.2.5, "Precautions on Cross Reference Analyzer" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

C4.3 Upgrading the Computer Dedicated to License Management

This section describes how to upgrade the computer dedicated to license management.

Upgrade Procedure

1. When upgrading from R4.02 or earlier, set up Windows.
2. Install only the license management software from the ProSafe-RS software medium.

TIP

When upgrading the computer dedicated to license management, you can install the license management software in the same way as when it is installed for the first time. However, you are not required to enter the following items because the data already set are applied.

- Name
- Company name
- Installation folder

3. Configure IT security settings.
4. When upgrading from R4.02 or earlier, configure Windows environment settings for each user.

SEE ALSO

For more information about configuring the IT security settings, refer to:

B3.6.1, “Running the IT Security Tool” on page B3-46

For more information about setting up Windows, refer to:

B3.2, “Setting Up Windows” on page B3-7

For more information about installing the license management software, refer to:

B6., “Setting Up the Computer Dedicated to License Management” on page B6-1

For more information about configuring Windows environment settings for each user, refer to:

B3.9, “Configuring Windows Environment Settings for Each User” on page B3-59

C5. Uninstalling the ProSafe-RS Software

This section describes how to uninstall the ProSafe-RS software and network drivers. Procedures are provided for the following two cases:

- Uninstallation on SENG
- Uninstallation on the computer dedicated to license management

Note, however, that uninstalling the ProSafe-RS software does not remove the project database, user settings, registries, and so on. If you need to remove ProSafe-RS software completely, reinstall your operating system.

C5.1 Uninstallation on SENG

This section describes the procedures for uninstallation on SENG.

C5.1.1 Uninstalling the ProSafe-RS Software

If you uninstall the ProSafe-RS software, the license management software is also uninstalled. However, the license management data, IT Security Tool, and project data will not be deleted.

TIP

The IT Security Tool is also used by YOKOGAWA products other than ProSafe-RS. Therefore, even if you uninstall the ProSafe-RS software, the Start menu setting, programs and files of the IT Security Tool will not be removed. To completely uninstall the IT Security Tool, you need to uninstall all the products that use the IT Security Tool and then run the command for uninstalling the IT Security Tool.

■ Deleting and Deactivating the Licenses

If there are any active licenses distributed on the SENG PC, delete the licenses to deactivate the software packages before uninstalling the ProSafe-RS software.

SEE ALSO

For more information about how to deactivate software packages on a computer, refer to:

"■ Deleting a license from a license-assigned station" in 3.2.1, "Modifying license assignments" in License Management Guide (IM 32P01C60-01EN)

■ Uninstallation Procedure

After deactivating the packages (deleting the licenses), follow these steps to uninstall the ProSafe-RS software:

1. Open the Control Panel.
2. Select [Programs] > [Programs and Features].
   The Programs and Features window appears.

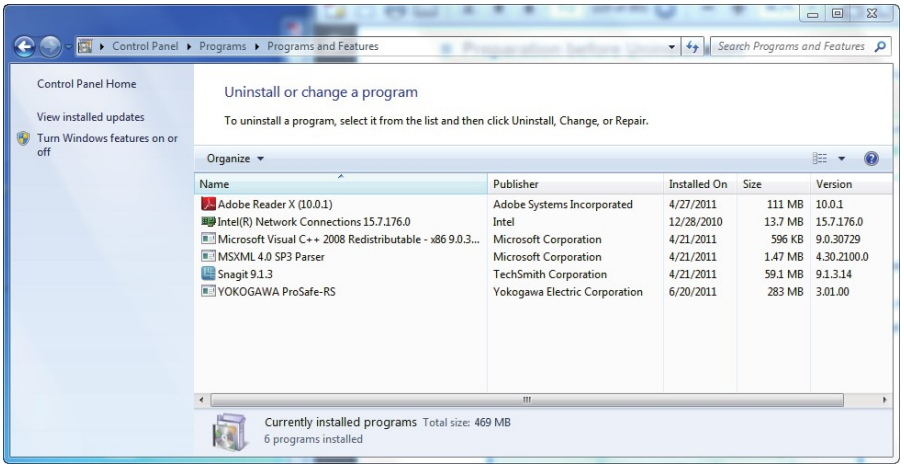


Figure C5.1.1-1 Programs and Features

3. Select [YOKOGAWA ProSafe-RS] and click [Change].
   The Welcome dialog box appears.
4. Click [Next].
   A dialog box for confirming the uninstallation appears.
5. Click [Remove].
   Uninstallation starts and a dialog box showing the progress of uninstallation appears.

TIP

If any active license is found, a dialog box appears confirming the continuation of the uninstallation process. Select [Yes] to continue the uninstallation. The active licenses are deactivated at this point.

However, the license information on the license management station remains unchanged. Update the license information on the license management station as necessary.

6. If a User Account Control dialog box appears, click [Yes] or [Allow].

TIP

If you leave the User Account Control dialog box without clicking [Yes] or [Allow], the dialog box closes automatically. Then, a dialog box indicating failure of uninstallation appears, and the uninstallation is discontinued. In this case, run the uninstallation again.

7. In the uninstallation complete dialog box that appears upon completion of the uninstallation, do either of the following operations.:
   - To restart the computer now, select [Yes, I want to restart my computer now.] and click [Finish].
   - To restart the computer later, select [No, I will restart my computer later.] and click [Finish].

C5.1.2 Uninstalling the Network Drivers

This section describes how to uninstall the network drivers.

Disabling the Control Bus Driver (Windows 10)

In Windows 10, before you uninstall the control bus driver, be sure to disable the control bus driver.

Follow these steps to disable the control bus driver:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [Network and Internet] > [Network and Sharing Center].
   The Network and Sharing Center window appears.
4. Select [Change adapter settings].
   The Network Connections window appears.
5. Right-click [Yokogawa Vnet Adapter] and select [Disable].
   An error dialog box regarding disabling connection appears.
6. Click [OK].
7. Restart the computer.
8. Perform steps 1 to 4.
9. In the Network Connections window, confirm that the Vnet driver is disabled.

TIP If the control bus driver is not disabled, perform the procedure from step 2 again.

Uninstalling Control Bus Driver

Follow these steps to uninstall the control bus driver:

1. Log on as an administrative user.
2. Terminate all applications that are running.
3. Set the ProSafe-RS software medium in the drive.
   - If the AutoPlay dialog box appears, click [Run Launcher.exe].
   - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the software medium.

   The installation menu appears.
4. Click [Control Bus Driver].
   The following dialog box appears.

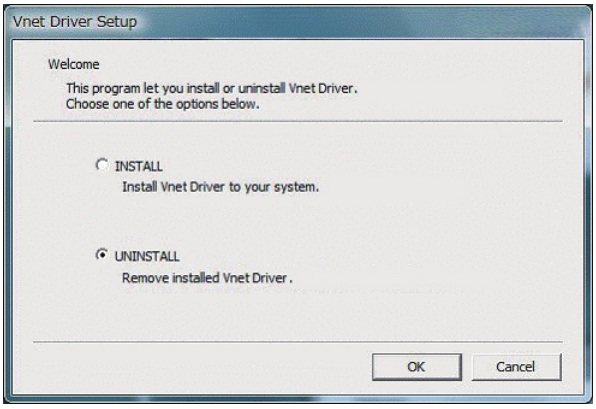


Figure C5.1.2-1 Setup Selection Dialog Box

5. Select [UNINSTALL] and then click [OK].
   A dialog box appears, confirming the uninstallation.
6. Click [OK].
   The uninstallation starts.
7. In the uninstallation complete dialog box that appears upon completion of the uninstallation, click [OK].
8. Restart the computer.

IMPORTANT

After uninstalling the driver, run the TCP/IP Inconsistency Detection Tool.

If any inconsistency is detected, use the TCP/IP Inconsistency Repair Tool and then configure the TCP/IP settings again.

SEE ALSO For more information about the TCP/IP Inconsistency Detect Tool and TCP/IP Inconsistency Repair Tool, refer to:

"■ Procedure 5: Repair TCP/IP Settings" on page B3-35

■ Uninstalling the Vnet/IP Open Communication Driver

Follow these steps to uninstall the Vnet/IP open communication driver:

1. Log on as an administrative user.
2. Terminate all applications that are running.
3. Set the ProSafe-RS software medium in the drive.
   - If the AutoPlay dialog box appears, click [Run Launcher.exe].
   - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the software medium.

   The installation menu appears.
4. Click [Vnet/IP Open com driver].
   The following dialog box appears.



Figure C5.1.2-2 Setup Selection Dialog Box

5. Select [UNINSTALL] and then click [OK].
   A dialog box appears, confirming the uninstallation.
6. Click [OK].
   The uninstallation starts.
7. In the uninstallation complete dialog box that appears upon completion of the uninstallation, click [OK].
8. Restart the computer.

IMPORTANT

After uninstalling the driver, run the TCP/IP Inconsistency Detection Tool.

If any inconsistency is detected, use the TCP/IP Inconsistency Repair Tool and then configure the TCP/IP settings again.

SEE ALSO For more information about the TCP/IP Inconsistency Detect Tool and TCP/IP Inconsistency Repair Tool, refer to:

"■ Procedure 5: Repair TCP/IP Settings" on page B3-35

■ Uninstalling the Vnet/IP Interface Package on a Virtual Machine

Follow these steps to uninstall the Vnet/IP Interface Package:

The procedures explained here should be performed on the guest OS of the virtual machine.

IMPORTANT

- If multiple products coexist in the virtual machine, if you uninstall the license product with the Vnet/IP Interface Package enabled, after restarting the virtual machine, Vnet/IP communication cannot be performed from other products.
- Unlike computers with a Vnet/IP interface card installed, if you uninstall the Vnet/IP Interface Package from a virtual machine, the virtual machine results in a Station Fail status immediately.

Procedure 1: Uninstall the Vnet/IP Interface Package

Follow these steps to uninstall the Vnet/IP Interface Package:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Terminate all applications that are running.
3. Sign out from the guest OS on the virtual machine.
4. Sign in to the host OS of virtualization host computer as an administrative user.
5. Copy an ISO format file of the ProSafe-RS software medium and paste it into a folder on the host OS.
6. Select [Start] > [Server Manager].
   Server Manager starts.
7. Select [Tools] > [Hyper-V Manager].
   Hyper-V Manager starts.
8. On the left pane, select the virtualization host computer.
   Virtual machines on the virtualization host computer are displayed on the middle pane.
9. Right-click on the virtual machine that the ISO format file is mounted and select [Connect].
   The virtual machine connection window appears.

TIP

The virtual machine connection window may appear full-screen. If it appears full-screen, click [Undo] to exit full-screen.

10. Click [Media] > [DVD Drive] > [Insert Disk].
    A file opening dialog box appears.
11. Select the copied ISO format file of the ProSafe-RS software medium and click [Open].
    The selected ISO format file is mounted on the virtual machine.
    - If the AutoPlay dialog box appears, click [Run Launcher.exe].
    - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the folder where the ISO format file of the ProSafe-RS software is stored.

    The installation menu appears.
12. On the installation menu, click [Control Bus Driver].
    A setup selection dialog box appears.
13. Select [UNINSTALL] and click [OK].
    A dialog box appears, confirming the uninstallation.
14. Click [OK].
    The uninstallation starts.
15. In the uninstallation complete dialog box that appears upon completion of the uninstallation, click [OK].
16. Restart the virtual machine.

IMPORTANT

After uninstalling the driver, run the TCP/IP Inconsistency Detection Tool.

If any inconsistency is detected, use the TCP/IP Inconsistency Repair Tool and then configure the TCP/IP settings again.

SEE ALSO For more information about the TCP/IP Inconsistency Detect Tool and TCP/IP Inconsistency Repair Tool, refer to:

"■ Procedure 5: Repair TCP/IP Settings" on page B3-35

Procedure 2: Disable the RIP Listener Service

This section describes how to disable the RIP Listener service.

IMPORTANT

Disabling of the RIP Listener service may fail when the Default Authentication Level of DCOM is configured to [None]. In this case, change to [connection].

Follow these steps to disable the RIP Listener service on Windows Server 2016:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Run the Command Prompt as Administrator.
3. Run the following command:
   ```
   dism /online /disable-feature /featurename:rasrip
   ```
4. Confirm that the message, "The operation completed successfully." appears.

SEE ALSO For more information about how to change the default authentication level of DCOM to "Connect", refer to:

"■ DCOM Settings" on page B3-15

C5.2 Uninstallation on the computer Dedicated to License Management

This section describes the procedure for uninstalling the license management software on the computer dedicated to license management.

Running the Uninstallation

Follow these steps to uninstall the license management software:

1. Log on as an administrative user.
2. Open the Control Panel.
3. Select [Programs] > [Programs and Features].
   The Programs and Features window appears.
4. From the program list, select [YOKOGAWA ProSafe-RS] and click [Change].
   The Welcome dialog box appears.
5. Click [Next].
   A dialog box for confirming the uninstallation appears.
6. Click [Delete].
   Uninstallation starts and a dialog box showing the progress of uninstallation appears.
7. In the uninstallation complete dialog box that appears upon completion of the uninstallation, do either of the following operations.:
   - To restart the computer now, select [Yes, I want to restart my computer now.] and click [Finish].
   - To restart the computer later, select [No, I will restart my computer later.] and click [Finish].

C6. Reinstalling the ProSafe-RS Software

This section describes how to reinstall the ProSafe-RS Software. The procedures are explained for the cases when changing and not changing the computer to be used. For each case, the reinstallation procedure is explained for license-assigned stations and for the license management station.

C6.1 When the Computer Used is the Same

This section describes the procedure for reinstalling the ProSafe-RS software to restore the software when the installed file gets damaged or deleted accidentally. The assumption is that the computer on which the software is to be installed is the same as before.

The software cannot be reinstalled by overwriting the software already installed. You must first uninstall the ProSafe-RS software and install the ProSafe-RS software again.

Reinstallation for a License-Assigned Station

This section describes the reinstallation procedure for a license-assigned station.

The flow of reinstallation is as follows.

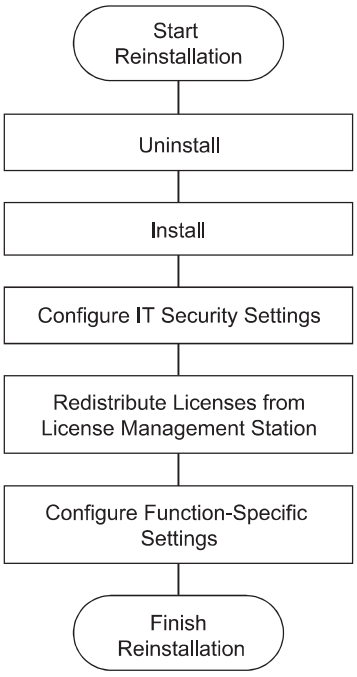


Figure C6.1-1 Flow of Reinstallation for a License-Assigned Station

Uninstall the ProSafe-RS Software

Uninstall the ProSafe-RS software.

SEE ALSO For more information about uninstallation procedure, refer to:

C5.1.1, “Uninstalling the ProSafe-RS Software” on page C5-3

Install the ProSafe-RS Software

Install the ProSafe-RS software.

SEE ALSO For more information about installing the ProSafe-RS software, refer to:

B3.5, “Installing the ProSafe-RS Software” on page B3-39

Configure IT Security Settings

Configure IT security settings in the same way as that for a new installation of the ProSafe-RS software.

SEE ALSO For more information about configuring the IT security settings, refer to:

B3.6, “Configuring IT Security Settings” on page B3-44

Redistribute Licenses from the License Management Station

Redistribute the licenses from the license management station.

SEE ALSO For more information about redistributing licenses from the license management station, refer to:

3.4, “Redistributing licenses to license-assigned stations” in License Management Guide (IM 32P01C60-01EN)

Configure Function-Specific Settings

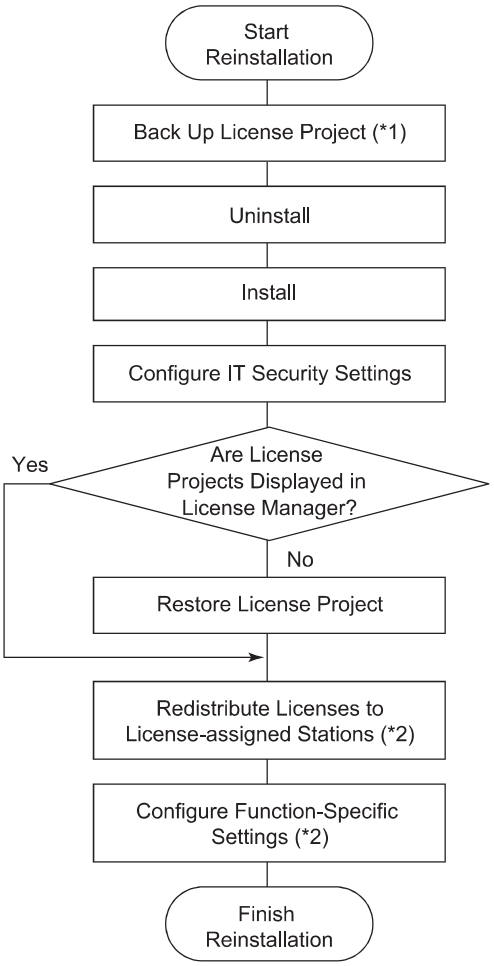
Configure the settings specific to the functions that run on the SENG.

SEE ALSO For more information about configuring the settings specific to each function of SENG, refer to:

B4., “Configuring the Functions Specific to SENG” on page B4-1

Reinstallation for the License Management Station

This section describes the reinstallation procedure for the license management station. The license management station can be a computer installed with the ProSafe-RS software or a computer dedicated to license management, where only the license management software is installed. You need to perform reinstallation according to the type of the license management station.



*1: If the license project backup is already created, this task is not required.
*2: These tasks are not required for the computer dedicated to license management.

Figure C6.1-2 Flow of Reinstallation for the License Management Station

Back Up the License Projects

Back up the license projects managed on the computer.

SEE ALSO For more information about the procedure for backing up license projects, refer to:

3.6, “Backing up and restoring a license project” in License Management Guide (IM 32P01C60-01EN)

Uninstall the ProSafe-RS Software

Uninstall the ProSafe-RS software. For a computer dedicated to license management, uninstall the license management software.

SEE ALSO For more information about the procedure for uninstallation on an SENG PC, refer to:

C5.1, “Uninstallation on SENG” on page C5-2

For more information about the procedure for uninstallation on the computer dedicated to license management, refer to:

C5.2, “Uninstallation on the computer Dedicated to License Management” on page C5-10

Install the ProSafe-RS Software

Install the ProSafe-RS software. For a computer dedicated to license management, install the license management software.

SEE ALSO For more information about installing the ProSafe-RS software, refer to:

B3.5, “Installing the ProSafe-RS Software” on page B3-39

For more information about how to install the license management software, refer to:

B6., “Setting Up the Computer Dedicated to License Management” on page B6-1

Configure IT Security Settings

Configure IT security settings in the same way as that for a new installation of the ProSafe-RS software.

SEE ALSO For more information about configuring the IT security settings, refer to:

B3.6, “Configuring IT Security Settings” on page B3-44

Restore the License Projects

Start the License Manager and then check if license projects are displayed. If not displayed, you need to restore the license projects from the backup.

SEE ALSO For more information about the procedure for restoring license projects, refer to:

“■ Restoring a license project on another license management station” in 3.6, “Backing up and restoring a license project” in License Management Guide (IM 32P01C60-01EN)

Redistribute Licenses to License-Assigned Stations

Redistribute the licenses to the license-assigned stations.

SEE ALSO For more information about redistributing licenses from the license management station, refer to:

3.4, “Redistributing licenses to license-assigned stations” in License Management Guide (IM 32P01C60-01EN)

Configure Function-Specific Settings

Configure the settings specific to the functions that run on the SENG.

SEE ALSO For more information about configuring the settings specific to each function of SENG, refer to:

B4., “Configuring the Functions Specific to SENG” on page B4-1

C6.2 When the Computer Used is Not the Same

This section describes the procedure for reinstallation on a different computer when the computer installed with the ProSafe-RS software can no longer be used due to damage or other reasons.

Reinstallation for a License-Assigned Station

This section describes the reinstallation procedure for a license-assigned station.

The procedure is the same as that for a new setup of SENG except that you need to restore the data that were backed up.

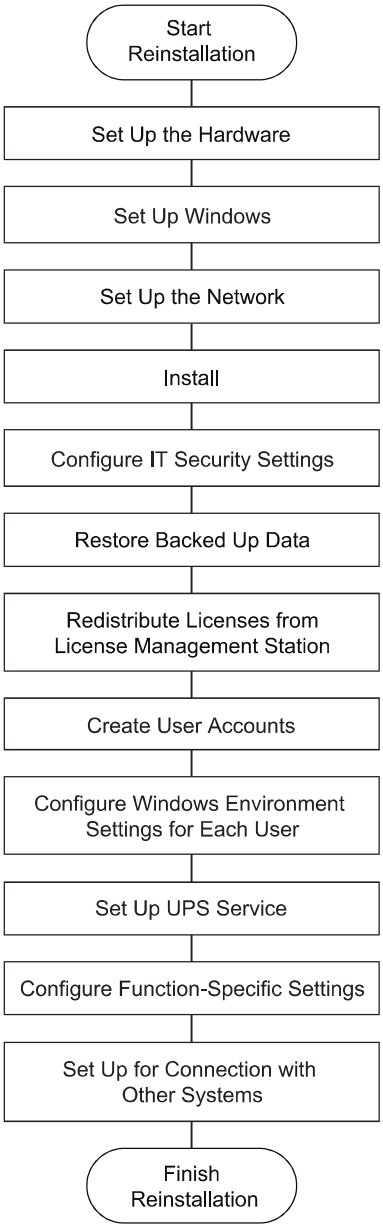


Figure C6.2-1 Flow of Reinstallation for a License-Assigned Station

IMPORTANT

For the station name of the new computer, specify the same name as that set on the previous computer.

SEE ALSO For more information about the procedures for a new setup of SENG, refer to:

- B3., “Setup of an SENG or a Computer Installed with Only AD Server” on page B3-1
- B4., “Configuring the Functions Specific to SENG” on page B4-1
- D1., “Connecting YOKOGAWA products” on page D1-1

Restore the Backed Up Data

Restore the backed up data on the new computer.

SEE ALSO For more information about the backed up data, refer to:

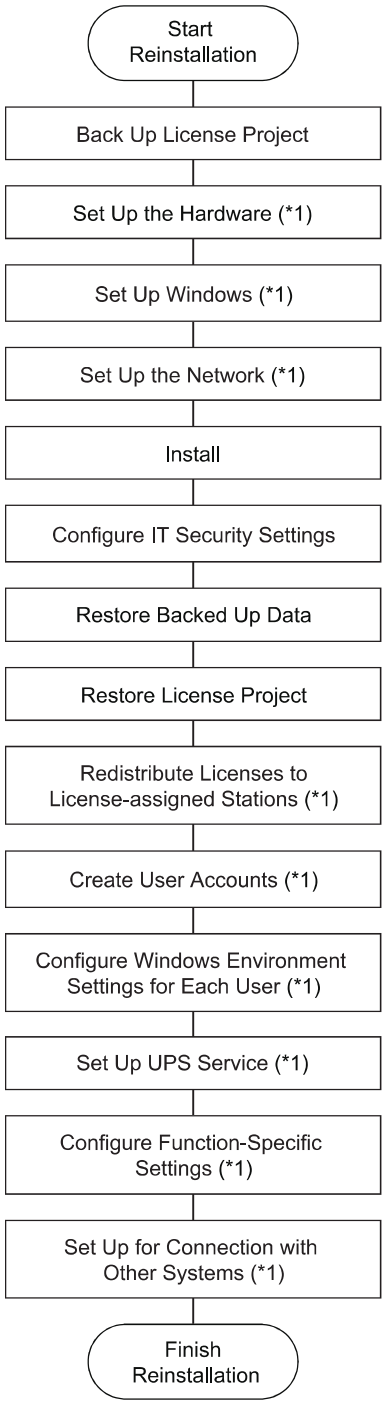
C3., “Backing Up the System” on page C3-1

Reinstallation for the License Management Station

The license management station can be a computer installed with the ProSafe-RS software or a computer dedicated to license management. You need to perform reinstallation according to the type of the license management station.

The procedure is the same as that for a new setup except that the following tasks are involved:

- Back up license projects
- Restore the backed up data
- Restore the license projects
- Redistribute licenses to the license-assigned stations



*1: For the computer dedicated to license management, these tasks are not required or may be omitted according to the circumstances.

Figure C6.2-2 Flow of Reinstallation for the License Management Station

IMPORTANT

For the station name of the new computer, specify the same name as that set on the previous computer.

SEE ALSO For more information about the procedures for a new setup of SENG, refer to:

- B3., “Setup of an SENG or a Computer Installed with Only AD Server” on page B3-1
- B4., “Configuring the Functions Specific to SENG” on page B4-1
- D1., “Connecting YOKOGAWA products” on page D1-1

For more information about the procedure for a new setup of a computer dedicated to license management, refer to:

B6., “Setting Up the Computer Dedicated to License Management” on page B6-1

Back Up the License Projects

Back up the license projects managed on the previous computer.

SEE ALSO For more information about procedures for backing up license projects, refer to:

3.6, “Backing up and restoring a license project” in License Management Guide (IM 32P01C60-01EN)

Restore the Backed Up Data

Restore the backed up data on the new computer.

SEE ALSO For more information about the backed up data, refer to:

C3., “Backing Up the System” on page C3-1

Restore the License Projects

Restore the license projects from the backup.

SEE ALSO For more information about the procedure for restoring license projects, refer to:

“■ Restoring a license project on another license management station” in 3.6, “Backing up and restoring a license project” in License Management Guide (IM 32P01C60-01EN)

Redistribute Licenses to License-Assigned Stations

Redistribute licenses to the license-assigned stations.

SEE ALSO For more information about redistributing licenses from the license management station, refer to:

3.4, “Redistributing licenses to license-assigned stations” in License Management Guide (IM 32P01C60-01EN)

C7. Troubleshooting

This section describes the causes of and remedies for problems that may occur.

C7.1 Windows Related Troubleshooting

This section describes how to handle problems related to Windows.

Note on User Account Control

If you log on as a non-administrative user and try to start the installer, the User Account Control dialog box appears. Click [No] and log on again as an administrative user, and then start the installer again.

The System Locks Up

Contact YOKOGAWA service.

Computer Operation Becomes Unstable

If the operation of the computer that was working normally has become unstable, do the task described below.

Cause

Incompatible software was installed.

Remedy

Uninstall the incompatible software you have installed.

SEE ALSO For more information about software that can coexist with ProSafe-RS, refer to:

"● Software that can coexist with ProSafe-RS" in "■ Software requirements for SENG" in A1.2, "Software requirements" in ProSafe-RS User's Guide (IM 32P01B10-01EN)

Cannot Change the Time Zone (Windows Server 2019, Windows Server 2022)

You cannot change the time zone in the Date and Time window.

Condition for Occurrence

- When the OS is Windows Server 2019 or Windows Server 2022 and User Account Control is enabled:
  Administrators other than the built-in Administrator cannot change the time zone.
- In addition, if "User Account Control: Admin Approval Mode for the Built-in Administrator account" is enabled in IT security settings:
  The time zone cannot be changed even if you are a built-in Administrator.

Problem

When you start the Control Panel and click the [Date and Time] > [Change the time zone] button, the following error message appears.

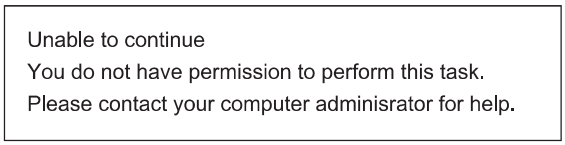


Figure C7.1-1 Error message

Also, if you click [Settings] > [Time & Language] from the Start menu to display the Date & Time window, the behavior will be as follows.

- For Windows Server 2019
  Even if you select any time from the [Time zone] drop-down list, the setting will return to the previous setting when you redisplay the window.
- For Windows Server 2022
  The [Time zone] drop-down list is grayed out and cannot be selected.

Workaround

Follow these steps:

1. Sign in as an administrative user.
2. Right-click the Start menu, select [Search], and search for the keyword timedate.cpl.
3. From the search results, right-click [timedate.cpl], and select [Run as administrator].
4. Change the time zone.

C7.2 Troubleshooting Related to Network

This section describes how to handle problems related to the network.

C7.2.1 Precaution on Network Cable Connection

A network charm bar may appear from the right side of the desktop when the cable is wired. If it appears, select [No].

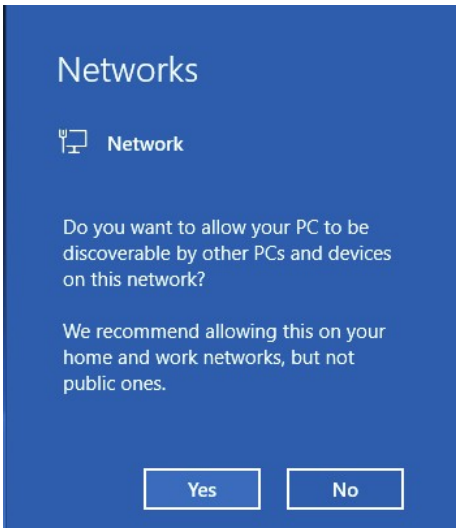


Figure C7.2.1-1 Network Charm Bar

C7.2.2 Problems Related to Installation and Deletion of Drivers

This section provides troubleshooting related to the installation and deletion of network drivers.

IMPORTANT

Some operations require administrative rights, and a User Account Control dialog box may appear when you try to do such operations. You can continue with the operation by clicking [Yes], [Continue], or [Allow] (if the user has administrator rights).

Confirming Installation Result

Check if the network driver is properly installed. If the driver is not operating property, install it again.

Adapter Driver for Control Bus Driver

When the control bus driver is added, the adapter driver “Yokogawa Vnet Adapter” appears under Network Adapters on Device Manager.

If the adapter driver does not start properly, "!" appears on the adapter driver icon.

Follow these steps to display Device Manger:

1. Log on as an administrative user.
2. Open the Control Panel.
3. Select [System and Security] > [System] > [Device Manager].

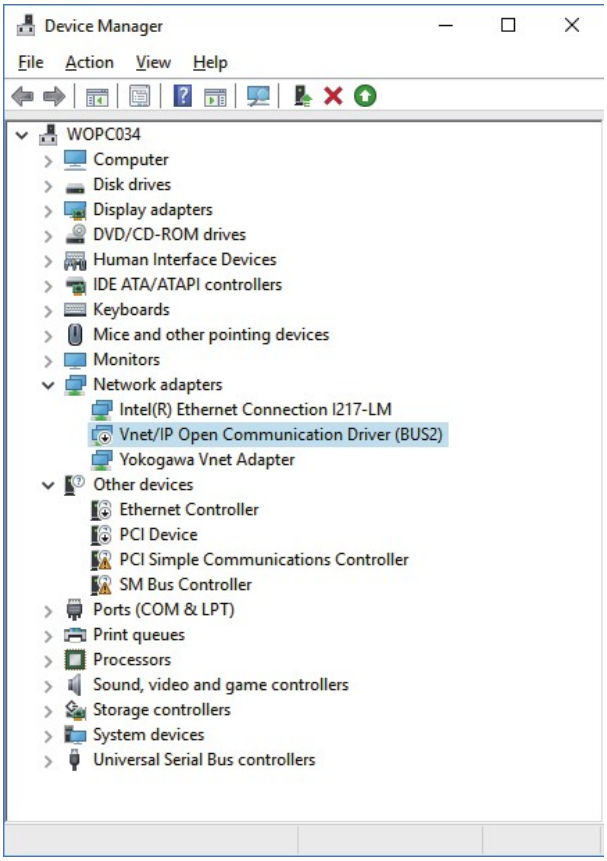


Figure C7.2.2-1 Adapter Driver Added Properly

Protocol Driver for Control Bus Driver

When the control bus driver is added, the protocol driver is installed together with the adapter driver.

The operating condition of the protocol driver can be checked in Command Prompt.

Follow these steps to check the operating condition of the protocol driver:

1. Sign in as a general user or administrative user.
2. Open Command Prompt.
3. Enter `sc query VLTDI`.
   The condition of the protocol driver is shown. If RUNNING is shown under STATE, the driver is operating properly.

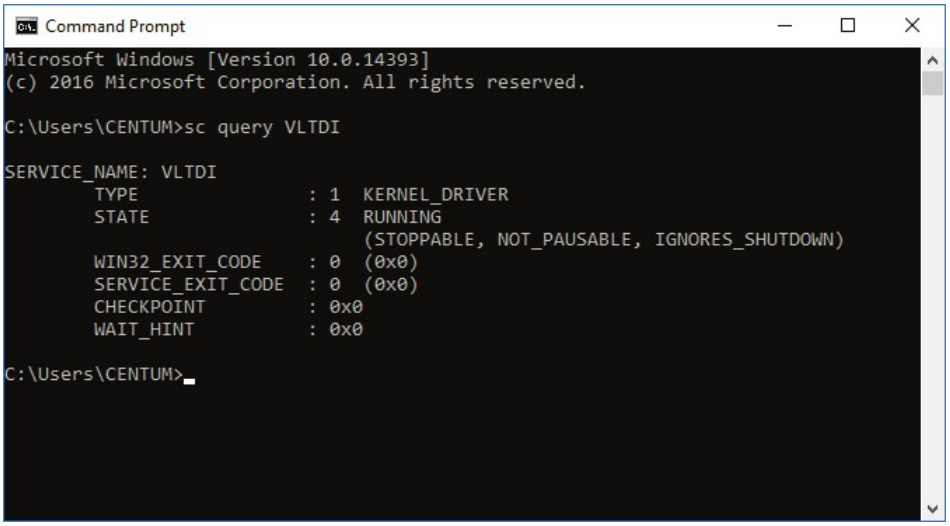


Figure C7.2.2-2 Protocol Driver Operating Properly

Vnet/IP Open Communication Driver

When the driver is added, “Vnet/IP Open Communication Driver (BUS2)” appears in Network Adapters in Device Manager.

If the driver does not start successfully, the “!” symbol appears next to the network adapter icon.

Follow these steps to display Device Manger:

1. Log on as an administrative user.
2. Open the Control Panel.
3. Select [System and Security] > [System] > [Device Manager].

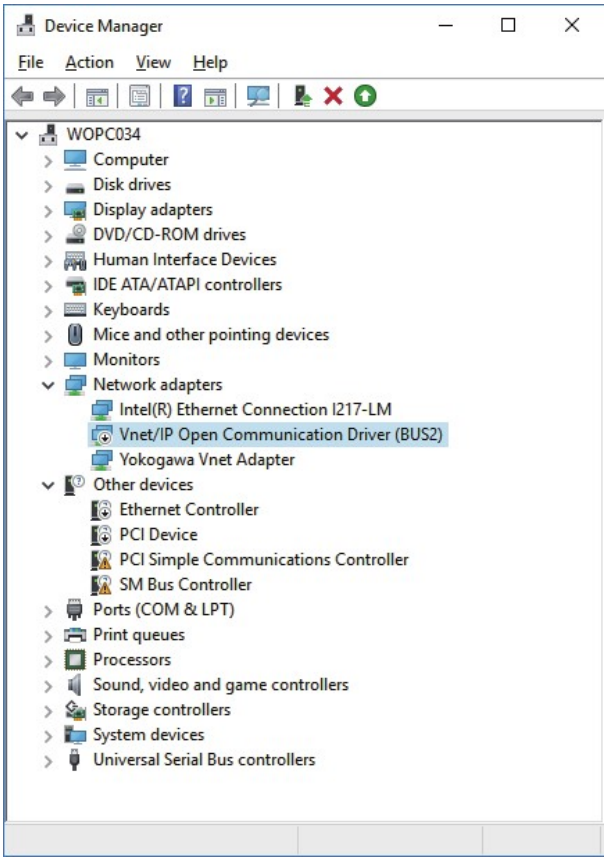


Figure C7.2.2-3 Adapter Driver Added Properly

Control Bus Driver is Successfully Installed but Does Not Start

The control bus driver may not start normally due to wrong connection of the bus cables or mistakes in address setting. In this case, VLNIC errors are recorded in the System log of Event Viewer.

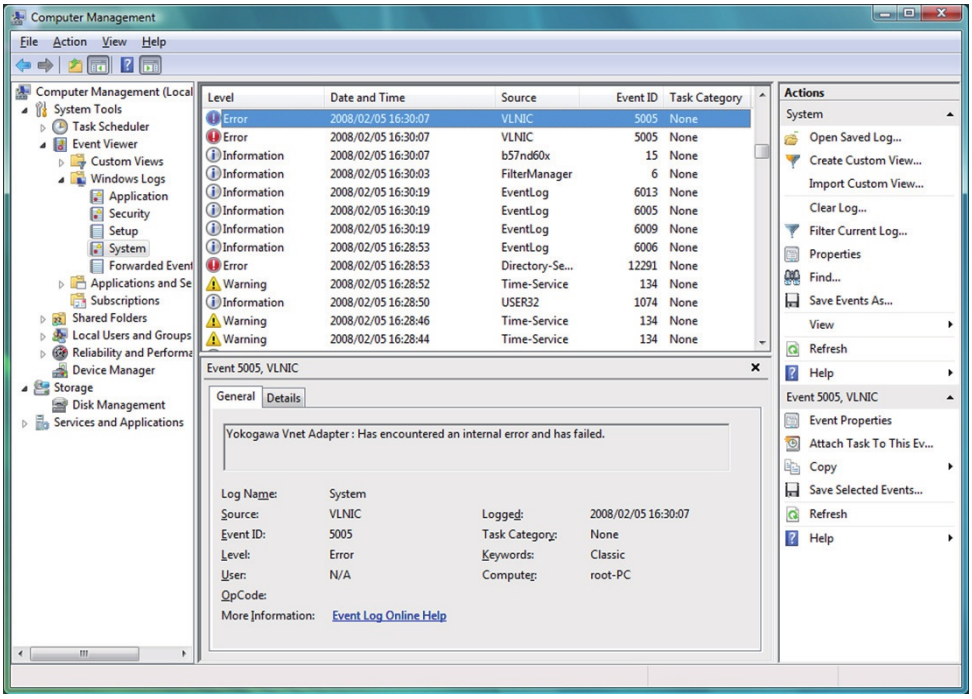


Figure C7.2.2-4 Event Viewer Recording VLNIC Errors (System)

1. Double-click a VLNIC error.
   The Event Properties dialog box appears.

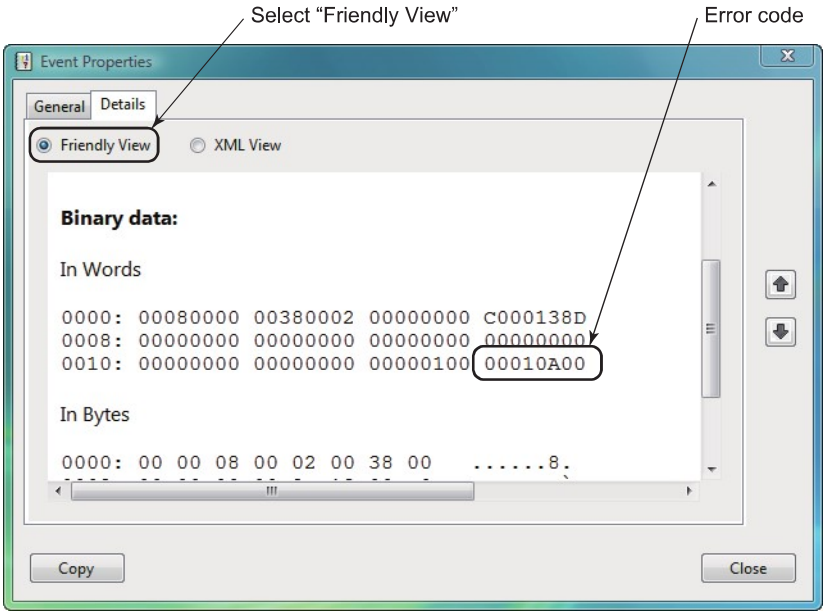


Figure C7.2.2-5 Event Properties

2. Look up the error code in the following table. If the problem is caused by the bus configuration and/or address setting, make sure that the settings are correctly made and shut down the computer. Then start up the computer again.

Table C7.2.2-1 Error Codes Generated when Starting the Driver

Code (*1)	Meaning
000101**	RAM parity error (failure of VF702/VF701/VI702/VI701 card)

Continues on the next page

Table C7.2.2-1 Error Codes Generated when Starting the Driver (Table continued)

Code (*1)	Meaning
000102**	RAM read/write error (failure of VF702/VF701/VI702/VI701 card)
000109**	Address overlap error
00010a**	Bus configuration error (wrong bus connector connection)
00010b**	Dip switch station number parity error
00010c**	Dip switch domain number parity error
00010d**	Inappropriate dip switch station number setting
00020013	Illegal station number (may be detected in the case of bus connector connection mistakes)

*1: In the code, a 2-digit number 00 is displayed at the position of ** for VF702/VF701 while others for VI702/VI701.

If the driver still does not start, other possible causes may be a failure of the control bus interface card or Vnet/IP interface card, or conflicts with other devices.

Replace the control bus interface card or Vnet/IP interface card, or remove the other devices from the computer.

Duplicate Instances of the Installer

You cannot start two instances of the installer. If you start a second instance, a warning message appears. Click [OK] and terminate the installer you started later.

The processing of the installer started first continues.

Error Message is Displayed during Network Driver Installation – 1

If an error message is displayed when you click [Don't Install] in the Windows Security dialog box that appears during installation of a network driver, perform the following tasks.



Figure C7.2.2-6 Windows Security Dialog Box (for Network Adapter)

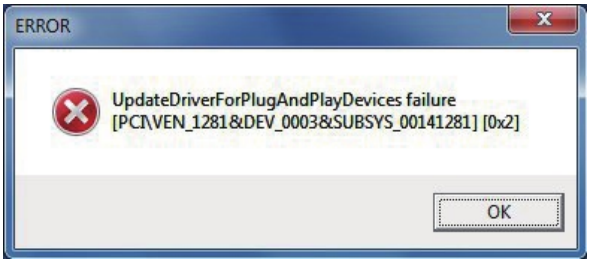


Figure C7.2.2-7 Error Message (for Network Adapter)

Control Bus Driver

1. After restarting the computer, click [Control Bus Drier] on the installation menu.
2. If the control bus driver can be deleted, delete it and then restart the computer.
3. Install the control bus driver again.

Vnet/IP Open Communication Driver

Start the installer again.

Error Message is Displayed during Network Driver Installation – 2

If an error message is displayed when you did not click [Do not install] in the Windows Security dialog box (for confirming installation of the network protocol or network adapter) that appears during installation of a network driver, perform the following tasks.

Control Bus Driver

1. After restarting the computer, click [Control Bus Driver] on the installation menu.
2. Perform either of the following operations:
   - If the control bus driver can be deleted, delete it and restart the computer. Then, install the driver again.
   - If the control bus driver cannot be deleted, restart the computer and install the driver again.

Vnet/IP Open Communication Driver

1. Start the installation menu again and click [Vnet/IP Open Communication Driver].
2. Perform either of the following operations:
   - If the driver can be deleted, delete it and restart the computer. Then, install the driver again.
   - If the driver cannot be deleted, restart the computer and install the driver again.

Error Message is Displayed during Network Driver Installation – 3

Previously functioning Ethernet communications may fail, generating an error message.

Cause

- Hardware, such as the Ethernet adapter card and Ethernet cable, is not connected properly.
- The network binding is not correctly set.
- The TCP/IP communication settings are not correct (IP address, subnet mask, etc.)

Remedy

- Check the hardware, Ethernet adapter card, and the Ethernet cable.
- In Control Panel, check the “Network and Sharing Center” settings.

Restarted the Computer After Deleting the Driver without Removing the Control Bus Interface Card or Vnet/IP Open Interface Card from the Computer

The actions you should take are described for the control bus driver and for the Vnet/IP open communication driver.

Control Bus Driver

If you restart the computer after deleting the control bus driver without removing the control bus interface card from the computer, Windows judges that the control bus interface card is a newly added device and displays the following dialog box.



Figure C7.2.2-8 Found New Hardware Dialog Box

Click [Ask me again later] here. Then, if you do not install the control bus driver, shut down the computer and remove the control bus interface card.

Vnet/IP Open Communication Driver

If you restart the computer after deleting the Vnet/IP open communication driver without removing the Vnet/IP interface card from the computer, Windows judges that the Vnet/IP interface card is a newly added device and prompts you to install the driver for it.

In this case, ignore the prompting message and do not install the driver.

D. Connection with Other Products

ProSafe-RS can be connected with YOKOGAWA products, such as CENTUM VP, PRM, and Exaquantum.

When connecting to these products, you may need to change the IT security settings.

This section describes the information and procedures on how to connect various products after installation.

D1. Connecting YOKOGAWA products

This section describes the settings that are required to connect YOKOGAWA products.

For each connection case, an integration code is assigned. You must perform the tasks that are required for the corresponding integration code of your connection case.

IMPORTANT

- Ensure that the security model and the user management type of the products that you are connecting are the same.
- If the Strengthened model is applied to the products that you want to connect, contact YOKOGAWA.

SEE ALSO For more information about security models, user management types, users and groups, and security settings, refer to:

1., “Overview” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

Integration code

The format of the integration code is as follows:

(Package code 1) - (Package code 2) - (Integration type) - (Revision number)

The following table describes the elements of an integration code.

Table D1-1 Integration code elements

Element	Description
Package code	The code that is assigned to a software package that can be installed independently on a computer. First package code is the package code of product 1, and Second package code is the package code of product 2.
Integration type	The connection setup of various products. The possible values are: • 01: When products are installed and operated on the same computer, and they cannot communicate or share files with each other. • 02: When products are installed and operated on separate computers, and they can communicate or share files with each other. • 03: When products are installed and operated either on the same computer or on separate computers, and they can function together by communicating or sharing files with each other.
Revision number	The version or revision number of the products that you want to connect. When the required connection procedures change on release of new versions or revisions, this revision number is incremented. The revision number can be from 01 to 99.

IMPORTANT

- You cannot install two products that have integration type 02 on the same computer.
- In the user's manuals of a product, the settings that are required to connect with other products are explained. However, information about the settings for connection that is provided in the user's manuals may be inconsistent between the connected products. The reason is that different products are released at different timings. To get the latest information, refer to the user's manuals of both products to check the product version number and the revision number of the integration code for their combination, and use the most recent setting procedure.

Package codes

The following table describes the package codes of various YOKOGAWA products.

Table D1-2 Package codes

Package code	Product	Package
0101	CENTUM VP	CENTUM VP Standard Operation and Monitoring Function (*1)
0102	CENTUM VP	System Builder Function
0108	CENTUM VP	Report Package
0121	CENTUM VP	Engineering Server Function
0153	CENTUM VP	SOE Viewer Package
0196	CENTUM VP	Project Database
0201	ProSafe-RS	Safety System Engineering and Maintenance Function
0202	ProSafe-RS	SOE OPC Interface Package
0203	ProSafe-RS	CENTUM VP Integration Package
0204	ProSafe-RS	CI Server Integration Package
0205	ProSafe-RS	Engineering Server Function
0251	ProSafe-RS	SOE Viewer Package
0252	ProSafe-RS	iDefine for ProSafe-RS
0253	ProSafe-RS	Forced I/O Viewer Package
0296	ProSafe-RS	Project Database
0299	ProSafe-RS	License Manager
0301	PRM	Plant Resource Manager Field Communications Server
0302	PRM	Plant Resource Manager Server
0351	PRM	Plant Resource Manager DeviceViewer
0352	PRM	PRM Client
0401	Exaopc	Exaopc OPC Interface Package
0801	Exaquantum	PIMS Server
0851	Exaquantum	Explorer Client
1202	STARDOM	STARDOM FCN/FCJ OPC Server

*1: As an optional function for this package, Exaopc OPC Interface Package (for HIS) is available. Consolidated Alarm Management Function (CAMS for HIS) is included in Standard Operation and Monitoring Function.

D1.1 CENTUM VP and ProSafe-RS

This section describes the settings when connecting CENTUM VP and ProSafe-RS.

IMPORTANT

- When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
- Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

D1.1.1 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS Safety System Engineering and Maintenance Function

By connecting CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS Safety System Engineering and Maintenance Function, you can use CENTUM integration function of ProSafe-RS.

Using CENTUM integration function of ProSafe-RS

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.1-1 Connection information

Integration code	0101-0201-03-05		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later (*1)		
Product 2	Safety System Engineering and Maintenance Function of ProSafe-RS R3.01 or later (*1)		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination/Linked domain management (*2)
Required procedures	None	Refer to "● When the Standard model is applied."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
*2: Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

When the Standard model is applied

For Standalone management, perform this setting on the computer where the ProSafe-RS safety system engineering and maintenance function is used and the computer where the CENTUM VP standard operation and monitoring function is used. For Domain, Combination, or Linked domain management, perform this setting on the domain controller.

1. Add the ProSafe-RS user account to CENTUM VP groups according to the following table.

Table D1.1.1-2 ProSafe-RS groups and their corresponding CENTUM VP groups

ProSafe-RS group	CENTUM VP group
PSF_MAINTENANCE	CTM_MAINTENANCE or CTM_MAINTENANCE_LCL
PSF_MAINTENANCE_LCL	CTM_MAINTENANCE or CTM_MAINTENANCE_LCL
PSF_ENGINEER	CTM_ENGINEER and CTM_ENGINEER_ADM
PSF_OPERATOR	CTM_OPERATOR
PSF_OPC	CTM_OPC or CTM_OPC_LCL
PSF_OPC_LCL	CTM_OPC or CTM_OPC_LCL
PSF_UTL	None

2. Add the CENTUM VP user account to ProSafeRS groups according to the following table.

Table D1.1.1-3 CENTUM VP groups and their corresponding ProSafe-RS groups

CENTUM VP group	ProSafe-RS group
CTM_MAINTENANCE	PSF_MAINTENANCE or PSF_MAINTENANCE_LCL
CTM_MAINTENANCE_LCL	PSF_MAINTENANCE or PSF_MAINTENANCE_LCL
CTM_ENGINEER	PSF_ENGINEER
CTM_ENGINEER_ADM	PSF_ENGINEER
CTM_OPC	PSF_OPC or PSF_OPC_LCL
CTM_OPC_LCL	PSF_OPC or PSF_OPC_LCL

SEE ALSO

For more information about how to create user accounts and add them to groups in Domain, Combination, or Linked domain management, refer to:

B2.4, “Creating Domain Users” on page B2-13

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B3.8.1, “When the Standard Model with Standalone Management Security Settings are Applied” on page B3-57

D1.1.2 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS SOE Viewer Package

By connecting CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS SOE Viewer Package, you can view historical information of CENTUM VP HIS on ProSafe-RS SOE Viewer.

Viewing Historical Information of CENTUM VP on ProSafe-RS SOE Viewer

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.2-1 Connection information

Integration code	0101-0251-03-05		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later (*1)		
Product 2	SOE Viewer Package of ProSafe-RS R3.01 or later (*1)		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination/Linked domain management (*2)
Required procedures	None	Refer to "● When the Standard model is applied."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
*2: Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

When the Standard model is applied

For Standalone management, perform this setting on the computer where ProSafe-RS SOE Viewer is used. For Domain, Combination, or Linked domain management, perform this setting on the domain controller.

- When enabling collaboration with products installed on the same computer
  Add the user account for using ProSafe-RS SOE Viewer to the CTM_OPERATOR group.
- When enabling collaboration with products installed on different computers
  Register the user account for using ProSafe-RS SOE Viewer to the computer where CENTUM VP HIS runs. The user name and password of the user account to be registered must be the same as those of the user account that uses ProSafe-RS SOE Viewer. Add the registered user account to CTM_OPERATOR group.

SEE ALSO

For more information about how to create user accounts and add them to groups in Domain, Combination, or Linked domain management, refer to:

B2.4, “Creating Domain Users” on page B2-13

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B3.8.1, “When the Standard Model with Standalone Management Security Settings are Applied” on page B3-57

D1.1.3 CENTUM VP SOE Viewer Package and ProSafe-RS Safety System Engineering and Maintenance Function

By connecting CENTUM VP SOE Viewer Package and ProSafe-RS Safety System Engineering and Maintenance Function, you can view SOE events of ProSafe-RS on CENTUM VP SOE Viewer.

Viewing SOE events of ProSafe-RS on CENTUM VP SOE Viewer

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.3-1 Connection information

Integration code	0153-0201-03-05		
Product 1	SOE Viewer Package of CENTUM VP R5.01 or later (*1)		
Product 2	Safety System Engineering and Maintenance Function of ProSafe-RS R3.01 or later (*1) (*2)		
Security model	Legacy model	Standard model	
User management type	N/A	Standalone management	Domain/Combination/Linked domain management (*3)
Required procedures	None	Refer to "● When the Standard model is applied."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
*2: The ProSafe-RS software package licenses are not required.
*3: Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

When the Standard model is applied

Add the user account for using CENTUM VP SOE Viewer to the PSF_OPERATOR group.

For Standalone management, perform this setting on the computer where CENTUM VP SOE Viewer is used. For Domain, Combination, or Linked domain management, perform this setting on the domain controller.

SEE ALSO

For more information about how to create user accounts and add them to groups in Domain, Combination, or Linked domain management, refer to:

B2.4, “Creating Domain Users” on page B2-13

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B3.8.1, “When the Standard Model with Standalone Management Security Settings are Applied” on page B3-57

D1.1.4 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS SOE OPC Interface Package

This section explains the required settings when Exaopc OPC Interface Package (for HIS) of CENTUM VP and SOE OPC Interface Package of ProSafe-RS are installed on the same computer.

If the computer installed with both packages comes under either of the following cases, perform all the procedures explained for each case.

- The computer installed with both packages is designated as the OPC server for OPC communication.
- The computer installed with both packages uses OPC client services.
- In a Domain, Combination, or Linked domain management system, the computer installed with both packages is designated as the OPC server on an OPC client computer that is not a member of the domain.

When the computer installed with both packages is designated as the OPC server to communicate with

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.4-1 Connection information

Integration code	0101-0202-01-02		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later (*1)		
Product 2	ProSafe-RS SOE OPC Interface Package of ProSafe-RS R3.01 or later (*1)		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination/Linked domain management (*2)
Required procedures	None	Refer to "● When the Standard model is applied."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
*2: Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

When the Standard model is applied

On the OPC server computer, add the user account for using OPC client services on OPC client computers to the CTM_OPC and PSF_OPC groups.

For Domain, Combination, or Linked domain management, perform this setting task on the domain controller. For Standalone management, create on the OPC server computer a user account with the same name as the local user who uses OPC client services on the OPC client computer, and add the user account to the CTM_OPC and PSF_OPC groups.

SEE ALSO

For more information about how to create user accounts and add them to groups in Domain, Combination, or Linked domain management, refer to:

B2.4, “Creating Domain Users” on page B2-13

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B3.8.1, “When the Standard Model with Standalone Management Security Settings are Applied” on page B3-57

● Users who use OPC client services

The following table shows the users who use OPC client services:

Table D1.1.4-2 Users who use OPC client services

OPC client service	User
Report Package	User who logged on to Windows
Access Administrator Package (FDA:21 CFR Part 11 compliant)	User who logged on to Windows
OPC client other than CENTUM VP product.(*1)	Users who use OPC client services

*1: Functions created using CENTUM Data Access Library are also included.

When the computer installed with both packages uses OPC client services

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.4-3 Connection information

Integration code	0101-0202-01-02		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later (*1)		
Product 2	ProSafe-RS SOE OPC Interface Package of ProSafe-RS R3.01 or later (*1)		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination/Linked domain management (*2)
Required procedures	None	Refer to "● When the Standard model is applied."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
*2: Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

● When the Standard model is applied

Add the user account for using OPC client services to the CTM_OPC and PSF_OPC groups.

For Standalone management, perform this setting on OPC client computers. For Domain, Combination, or Linked domain management, perform this setting on the domain controller.

SEE ALSO

For more information about how to create user accounts and add them to groups in Domain, Combination, or Linked domain management, refer to:

B2.4, “Creating Domain Users” on page B2-13

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B3.8.1, “When the Standard Model with Standalone Management Security Settings are Applied” on page B3-57

● Users who use OPC client services

The following table shows the users who use OPC client services:

Table D1.1.4-4 Users who use OPC client services

OPC client service	User
Report Package	User who logged on to Windows
Access Administrator Package (FDA:21 CFR Part 11 compliant)	User who logged on to Windows
FCS Data Setting/Acquisition Package (PICOT)	User who logged on to Windows
Consolidated Alarm Management Function (CAMS for HIS)	User that was specified when setting up the OPC A&E server connection
OPC client other than CENTUM VP product (*1)	Users who use OPC client services

*1: Functions created using CENTUM Data Access Library are also included.

● When FCS Data Setting/Acquisition Package (PICOT) is used

If FCS Data Setting/Acquisition Package (PICOT) (LHS6710) and HIS type single sign on are used, also perform the following setting:

For Standalone or Linked domain management:	On the computer running the package, add OFFUSER to the PSF_OPC group.
For Domain or Combination management:	On the computer running the package, add OFFUSER to the PSF_OPC_LCL group.

■ When the computer installed with both packages is designated as the OPC server to communicate with on the OPC client computer that is not a member of the domain

The following table shows the connection information for the case where Domain or Combination management is applied and the computer installed with both packages is designated as the OPC server on the OPC client computer that is not a member of the domain. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.4-5 Connection information

Integration code	0101-0202-01-04
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later (*1)
Product 2	ProSafe-RS SOE OPC Interface Package of ProSafe-RS R3.01 or later (*1)
Security model	Standard model
User management type	Domain/Combination/Linked domain management (*2)
Required procedures	Refer to "● Required procedures for connection."

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
*2: Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

● Required procedures for connection

On the OPC server computer, create a user account with the same name as the local user who performs OPC communication on the OPC client computer, and then add the user account to the following groups.

For Domain or Combination management:	CTM_OPC_LCL and PSF_OPC_LCL groups
For Linked domain management:	CTM_OPC and PSF_OPC groups

SEE ALSO For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B3.8.1, “When the Standard Model with Standalone Management Security Settings are Applied” on page B3-57

For more information about how to create user accounts and add them to groups in Domain, Combination, or Linked domain management, refer to:

B2.4, “Creating Domain Users” on page B2-13

Local Users Who Use OPC Client Service

The following table shows the local users who use OPC client services:

Table D1.1.4-6 Local Users Who Use OPC Client Service

OPC client service	User
Report Package	User who logged on to Windows
OPC client other than CENTUM VP product (*1)	Users who use OPC client services

*1: Functions created using CENTUM Data Access Library are also included.

D1.1.5 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS Forced I/O Viewer Package

You can use ProSafe-RS Forced I/O Viewer Package on a computer where CENTUM VP Standard Operation and Monitoring Function is installed.

TIP

You cannot install ProSafe-RS Forced I/O Viewer Package on a computer where ProSafe-RS Safety System Engineering and Maintenance Function is installed.

Viewing the ProSafe-RS forced-I/O information

The following table describes the connection information. This table also describes the information for connecting with other CENTUM VP packages.

Table D1.1.5-1 Connection information

Integration code	0101-0253-01-02 The same applies to the following combinations: 0102-0253-01-02, 0108-0253-01-02, 0109-0253-01-02, 0110-0253-01-02, 0111-0253-01-02, 0112-0253-01-02, 0113-0253-01-02, 0114-0253-01-02, 0118-0253-01-02, 0119-0253-01-02, 0120-0253-01-02, 0121-0253-01-02, 0152-0253-01-02, 0153-0253-01-02, 0199-0253-01-02		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R6.06 or later (*1)		
Product 2	Forced I/O Viewer Package of ProSafe-RS R4.05 or later (*1)		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination/ Linked domain management (*2)
Required procedures	Read the reference that follows the table.		

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
*2: Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

SEE ALSO

For more information about the settings required to use Forced I/O Viewer Package, refer to:

B4.4, “Settings Required to Use the Forced I/O Viewer Function” on page B4-5

D1.1.6 CENTUM VP System Builder Function and ProSafe-RS CENTUM VP Integration Package

By using ProSafe-RS CENTUM VP Integration Package, you can build an integrated system of CENTUM VP and ProSafe-RS.

Building a system by integrating CENTUM VP and ProSafe-RS

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.6-1 Connection information

Integration code	0102-0203-03-05		
Product 1	System Builder Function of CENTUM VP R5.01 or later (*1)		
Product 2	CENTUM VP Integration Package of ProSafe-RS R3.01 or later (*1)		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination/Linked domain management (*2)
Required procedures	None	Refer to "● When the Standard model is applied."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
*2: Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

When the Standard model is applied

- When CENTUM VP project is placed on a computer where SCS Manager is used:

  Add the user account for using SCS Manager of ProSafe-RS to the CTM_ENGINEER and PSF_ENGINEER groups.

  For Standalone management, perform this setting on the computer where SCS Manager is used. For Domain, Combination, or Linked domain management, perform this setting on the domain controller.

- When CENTUM VP project is placed on a computer where SCS Manager is not used:

  For Standalone management, create a user account with the same name as the user who uses SCS Manager on the computer where the CENTUM VP project is placed and then add the user account to the CTM_ENGINEER group.

  For Domain, Combination, or Linked domain management, add the user account for using SCS Manager to the CTM_ENGINEER group on the domain controller.

SEE ALSO

For more information about how to create user accounts and add them to groups in Domain, Combination, or Linked domain management, refer to:

B2.4, “Creating Domain Users” on page B2-13

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B3.8.1, “When the Standard Model with Standalone Management Security Settings are Applied” on page B3-57

D1.1.7 CENTUM VP System Builder Function and ProSafe-RS Safety System Engineering and Maintenance Function

By connecting CENTUM VP System Builder Function and ProSafe-RS Safety System Engineering and Maintenance Function, you can perform simulation tests of SCS using SCS simulator of ProSafe-RS.

Enabling SCS simulation tests using SCS simulator

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.7-1 Connection information

Integration code	0102-0201-03-05		
Product 1	System Builder Function of CENTUM VP R5.01 or later (*1)		
Product 2	Safety System Engineering and Maintenance Function of ProSafe-RS R3.01 or later (*1)		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination/Linked domain management (*2)
Required procedures	None	Refer to "● When the Standard model is applied."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
*2: Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

When the Standard model is applied

Add all the user accounts for using SCS Manager of ProSafe-RS or System View of CENTUM VP to the CTM_ENGINEER and PSF_ENGINEER groups.

For Standalone management, perform this setting on the computer where SCS Manager of ProSafe-RS and System View are used. For Domain, Combination, or Linked domain management, perform this setting on the domain controller.

SEE ALSO

For more information about how to create user accounts and add them to groups in Domain, Combination, or Linked domain management, refer to:

B2.4, “Creating Domain Users” on page B2-13

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B3.8.1, “When the Standard Model with Standalone Management Security Settings are Applied” on page B3-57

D1.1.8 CENTUM VP Engineering Server Function and ProSafe-RS Safety System Engineering and Maintenance Function

When the CENTUM VP engineering server function and ProSafe-RS safety system engineering and maintenance function are connected, the AD Suite client function and server function work in collaboration so that I/O list engineering and change management function can be used.

Performing engineering and maintenance of a ProSafe-RS safety system by using a CENTUM VP engineering server

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.8-1 Connection information

Integration code	0121-0201-03-03		
Product 1	Engineering Server Function of CENTUM VP R6.02 or later (*1)		
Product 2	Safety System Engineering and Maintenance Function of ProSafe-RS R4.01 or later (*1)		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination/Linked domain management (*2)
Required procedures	Refer to "● When the Legacy model is applied."	Refer to "● When the Standard model is applied."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
*2: Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

When the Legacy model is applied

On the AD Suite client computer and AD Suite server computer, create Windows users who use this function.

Use the ADS Administration Tool to register the Windows users to the engineering server.

When the Standard model is applied

On the AD Suite client computer and AD Suite server computer, create Windows users who use this function.

Add the user accounts to the CTM_ENGINEER and PSF_ENGINEER groups. For Standalone management, perform this setting task on the computer where the CENTUM VP engineering server is used and also on the computer where the ProSafe-RS safety system engineering and maintenance function is used.

For Domain, Combination, or Linked domain management, perform this setting on the domain controller.

Use the ADS Administration Tool to register the Windows users to the engineering server.

SEE ALSO For more information about how to create user accounts and add them to groups, refer to:

C1.2, “Management of AD projects” in Engineer's Reference Manual (IM 32P04B10-01EN)

D1.1.9 CENTUM VP System Builder Function and ProSafe-RS Engineering Server Function

When the CENTUM VP system generation function and ProSafe-RS engineering server function are connected, the AD Suite client function and server function work in collaboration so that the module-based engineering and change management function can be used.

Generating a CENTUM VP system using a ProSafe-RS engineering server

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.9-1 Connection information

Integration code	0205-0102-03-03		
Product 1	Engineering Server Function of ProSafe-RS R4.01 or later (*1)		
Product 2	System Builder Function of CENTUM VP R6.02 or later (*1)		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination/Linked domain management (*2)
Required procedures	Refer to "● When the Legacy model is applied."	Refer to "● When the Standard model is applied."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.11.00 or later and the software revision of ProSafe-RS is R4.10.00 or later.
*2: Linked domain management is supported by CENTUM VP R6.08.00 or later and ProSafe-RS R4.06.00 or later software revisions.

When the Legacy model is applied

On the AD Suite client computer and AD Suite server computer, create Windows users who use this function.

Use the ADS Administration Tool to register the Windows users to the engineering server.

When the Standard model is applied

On the AD Suite client computer and AD Suite server computer, create Windows users who use this function.

Add the user accounts to the CTM_ENGINEER and PSF_ENGINEER groups. For Standalone management, perform this setting task on the computer where the CENTUM VP system builder function is used and also on the computer where the ProSafe-RS engineering server function is used.

For Domain, Combination, or Linked domain management, perform this setting on the domain controller.

Use the ADS Administration Tool to register the Windows users to the engineering server.

SEE ALSO For more information about how to create user accounts and add them to groups, refer to:

C1.2, “Management of AD projects” in Engineer's Reference Manual (IM 32P04B10-01EN)

D1.2 ProSafe-RS and iDefine

This section describes the settings when connecting ProSafe-RS and iDefine.

IMPORTANT

- When using ProSafe-RS and iDefine for ProSafe-RS, use ProSafe-RS R4.02 to R4.08.

  If you want to use SENG to edit engineering data created with iDefine for ProSafe-RS, contact YOKOGAWA.

- iDefine for ProSafe-RS can be installed on the same computer as ProSafe-RS software packages and collaborates with the Safety System Engineering and Maintenance Function.

  In ProSafe-RS R4.05 or later, you can install the combination of iDefine for ProSafe-RS, ProSafe-RS, and CENTUM VP on a same computer.

  You cannot install iDefine for ProSafe-RS on a computer where CENTUM VP SOE Server Package is installed.

- When you install ProSafe-RS and iDefine for ProSafe-RS on the same computer, install ProSafe-RS first and then iDefine for ProSafe-RS in succession. After installing iDefine for ProSafe-RS, configure IT security settings.

- The combination of versions between ProSafe-RS and iDefine for ProSafe-RS is fixed. For example, ProSafe-RS R4.06 can collaborate only with iDefine for ProSafe-RS 1.16.6.

SEE ALSO For more information about the available combination of versions between ProSafe-RS and iDefine for ProSefe-RS, refer to:

“■ Use of iDefine” in A1.2, “Software requirements” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

D1.2.1 ProSafe-RS Safety System Engineering and Maintenance Function and iDefine for ProSafe-RS

Connecting the ProSafe-RS Safety System Engineering and Maintenance Function and iDefine for ProSafe-RS enables exchange of engineering data between ProSafe-RS and iDefine. It also enables execution of ProSafe-RS logic simulation test, SCS simulation test, and target test from iDefine by using iDefine Test Manager.

Exchanging engineering data between ProSafe-RS and iDefine, and using iDefine Test Manger

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.2.1-1 Connection information

Integration code	0201-0252-03-05			
Product 1	Safety System Engineering and Maintenance Function of ProSafe-RS R4.06 or later			
Product 2	iDefine for ProSafe-RS 1.16.6 or later			
Security model	Legacy model	Standard model		
User management type	-	Standalone management	Domain/Combination management	Linked domain management (*1)
Required procedures	Refer to "● When the Legacy model is applied."	Refer to "● When the Standard model is applied with Standalone management."	Refer to "● When the Standard model is applied with Domain or Combination management."	Refer to "● When the Standard model is applied with Linked domain management."

*1: Linked domain management is supported by ProSafe-RS R4.06.00 or later software.

When the Legacy model is applied

- When installing on the same computer
  No procedure is requited.
- When installing on separate computers
  On the computer where you run the ProSafe-RS Safety System Engineering and Maintenance Function, create the logon users of the computer where you run iDefine. For the users that you create, use the same user names and passwords as those of the users on the computer where you run iDefine.

When the Standard model is applied with Standalone management

- When installing on the same computer
  Add the users who use iDefine to one of the following groups:
  - PSF_OPERATOR
  - PSF_ENGINEER
  - PSF_MAINTENANCE

  In addition, add the users who perform communication with iDefine Test Manager through iDefine to the PSF_ENGINEER group.
- When installing on separate computers
  1. On the computer where you run the ProSafe-RS Safety System Engineering and Maintenance Function, create the logon users of the computer where you run iDefine. For the users that you create, use the same user names and passwords as those of the users on the computer where you run iDefine.

2. Add the created users to the PSF_ENGINEER group on the computer where you run the ProSafe-RS Safety System Engineering and Maintenance Function.

SEE ALSO For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B3.8.1, “When the Standard Model with Standalone Management Security Settings are Applied” on page B3-57

When the Standard model is applied with Domain or Combination management

- When installing on the same computer
  Add the users who use iDefine to one of the following groups:
  - PSF_OPERATOR
  - PSF_OPERATOR_LCL
  - PSF_ENGINEER
  - PSF_ENGINEER_LCL
  - PSF_MAINTENANCE
  - PSF_MAINTENANCE_LCL

  In addition, add the users who perform communication with iDefine Test Manager through iDefine to the PSF_ENGINEER or PSF_ENGINEER_LCL group.
- When installing on separate computers
  1. On the domain controller, add the computer that you run iDefine to the domain and create the logon users of the computer where you run iDefine.
  2. Add the created users to the PSF_ENGINEER group.

SEE ALSO For more information about how to create user accounts and add them to groups in Domain or Combination management, refer to:

B2.4, “Creating Domain Users” on page B2-13

When the Standard model is applied with Linked domain management

- When installing on the same computer
  Add the users who use iDefine to one of the following groups:
  - PSF_OPERATOR
  - PSF_ENGINEER
  - PSF_MAINTENANCE

  In addition, add the users who perform communication with iDefine Test Manager through iDefine to the PSF_ENGINEER group.
- When installing on separate computers
  1. On the domain controller, add the computer that you run iDefine to the domain and create the logon users of the computer where you run iDefine.
  2. Add the created users to the PSF_ENGINEER group.

SEE ALSO For more information about how to create user accounts and add them to groups in Linked domain management, refer to:

B2.4, “Creating Domain Users” on page B2-13

D1.2.2 ProSafe-RS functions other than Safety System Engineering and Maintenance Function and iDefine for ProSafe-RS

This section describes the settings when installing ProSafe-RS functions other than Safety System Engineering and Maintenance Function and iDefine for ProSafe-RS on the same computer.

Installing ProSafe-RS SOE OPC Interface Package and iDefine for ProSafe-RS on the same computer

The following table describes the connection information. This table also describes the information for connecting with other ProSafe-RS packages. For required procedures for connection, read the descriptions that follow the table.

Table D1.2.2-1 Connection information

Integration code	0202-0252-01-04 The same applies to the following combinations: 0203-0252-01-04, 0204-0252-01-04, 0205-0252-01-04, 0251-0252-01-04, 0296-0252-01-04, 0299-0252-01-04, 0253-0252-01-02			
Product 1	SOE OPC Interface Package of ProSafe-RS R4.06 or later			
Product 2	iDefine for ProSafe-RS 1.16.6 or later			
Security model	Legacy model	Standard model		
User management type	-	Standalone management	Domain/Combination management	Linked domain management (*1)
Required procedures	None	Refer to "● When the Standard model is applied with Standalone management."	Refer to "● When the Standard model is applied with Domain or Combination management."	Refer to "● When the Standard model is applied with Linked domain management."

*1: Linked domain management is supported by ProSafe-RS R4.06.00 or later software.

When the Standard model is applied with Standalone management

Add the users who use iDefine to one of the following groups:

- PSF_OPERATOR
- PSF_ENGINEER
- PSF_MAINTENANCE

In addition, add the users who perform communication with iDefine Test Manager through iDefine to the PSF_ENGINEER group.

SEE ALSO For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B3.8.1, “When the Standard Model with Standalone Management Security Settings are Applied” on page B3-57

When the Standard model is applied with Domain or Combination management

Add the users who use iDefine to one of the following groups:

- PSF_OPERATOR
- PSF_OPERATOR_LCL

- PSF_ENGINEER
- PSF_ENGINEER_LCL
- PSF_MAINTENANCE
- PSF_MAINTENANCE_LCL

In addition, add the users who perform communication with iDefine Test Manager through iDefine to the PSF_ENGINEER or PSF_ENGINEER_LCL group.

SEE ALSO For more information about how to create user accounts and add them to groups in Domain or Combination management, refer to:

B2.4, “Creating Domain Users” on page B2-13

When the Standard model is applied with Linked domain management

Add the users who use iDefine to one of the following groups:

- PSF_OPERATOR
- PSF_ENGINEER
- PSF_MAINTENANCE

In addition, add the users who perform communication with iDefine Test Manager through iDefine to the PSF_ENGINEER group.

SEE ALSO For more information about how to create user accounts and add them to groups in Linked domain management, refer to:

B2.4, “Creating Domain Users” on page B2-13

D1.3 ProSafe-RS and PRM

This section describes the settings when connecting ProSafe-RS and PRM.

IMPORTANT

- Linked domain management is supported by ProSafe-RS R4.06.00 or later and PRM R4.04.00 or later software revisions.
- When you install ProSafe-RS and PRM client on the same computer, ensure that the software revision of ProSafe-RS is R4.04.00 or later and PRM is R4.02.00 or later. When you install ProSafe-RS and PRM on the same computer with linked domain management, ensure that the software revision of ProSafe-RS is R4.06.00 or later and the software revision of PRM is R4.04.00 or later.

D1.3.1 ProSafe-RS SOE OPC Interface Package and PRM Server

Connecting the ProSafe-RS and PRM Server enables PRM to retrieve ProSafe-RS messages. To perform OPC communication with PRM, the SOE OPC Interface Package is required. No setting is required on the PRM Server.

IMPORTANT

PRM Server and ProSafe-RS software cannot be installed on the same computer.

Enabling PRM to retrieve messages from ProSafe-RS

The following table shows the connection information. The required procedures of connecting the products are provided after the table.

Table D1.3.1-1 Connection information

Integration code	0202-0302-02-04			
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later			
Product 2	Plant Resource Manager Server of PRM R3.20 or later			
Security model	Legacy model	Standard model		
User management type	-	Standalone management	Domain/Combination management	Linked domain management (*1)
Required procedures	Refer to "● When the Legacy model is applied."	Refer to "● Setting the logon type with Standard model", "● Creating internal user accounts with Standard model".		

*1: Linked domain management is supported by ProSafe-RS R4.06.00 or later and PRM R4.04.00 or later software revisions.

When the Legacy model is applied

Follow these steps to set the logon type:

1. Log on as a user with administrative rights.
2. Start SOE OPC Parameter Setting.
   The SOE OPC Interface Settings dialog box appears.
3. In the OPC Security Settings section, click [Edit].
   The Select Logon Type dialog box appears.
4. Select [Automatically logon the designated user for connecting OPC server].
5. Select [Default user of R2.03 and earlier versions].
6. Click [OK].

Setting the logon type with Standard model

Follow these steps to set the logon type:

1. Log on to the SENG as a member of the PSF_ENGINEER or PSF_ENGINEER_LCL group.
2. Start SOE OPC Parameter Setting.
   The SOE OPC Interface Settings dialog box appears.
3. In the OPC Security Settings section, click [Edit].
   The Select Logon Type dialog box appears.

4. Select [Automatically logon the designated user for connecting OPC server].
5. Select [Default user of R2.03 and earlier versions].
6. Click [OK].

Creating internal user accounts with Standard model

Follow these steps to create PRM and ProSafe-RS user accounts:

1. On the SENG, create the PRM_PROCESS and PRM_PROCESS2 user accounts by performing these steps:
   a. Log on to the SENG as a user with administrative rights.
   b. Insert the PRM installation media Disc 1 into the DVD drive, and navigate to the following folder:
      `<DVD drive>:\PRM\SecuritySettingUtility`
   c. Double-click [CreateInternalUserAccount.exe].
      The PRM_PROCESS and PRM_PROCESS2 user accounts are created and automatically added to one of the following groups:

Standalone management:	PSF_OPC
Domain management:	PSF_OPC_LCL
Combination management:	PSF_OPC or PSF_OPC_LCL
Linked domain management:	PSF_OPC

2. On the PRM Server computer, create the PSF_PROCESS user account by performing these steps:
   a. Log on as a user with administrative rights.
   b. Insert the ProSafe-RS software medium into the DVD drive, and navigate to the following folder:
      `<DVD drive>:\ProSafe-RS\SECURITY`
   c. Double-click [ProSafe.Security.CreateProSafeProcess.exe].
      The PSF_PROCESS user account is created.

D1.3.2 PRM Client and Forced I/O Viewer Package

You can use ProSafe-RS Forced I/O Viewer Package on a computer where PRM Client is installed.

TIP

You cannot install ProSafe-RS Forced I/O Viewer Package on a computer where ProSafe-RS Safety System Engineering and Maintenance Function is installed.

Viewing the ProSafe-RS forced-I/O information

The following table describes the connection information.

Table D1.3.2-1 Connection information

Integration code	0352-0253-01-02			
Product 1	PRM Client of PRM R4.02 or later(*1)			
Product 2	Forced I/O Viewer Package of ProSafe-RS R4.05 or later (*1)			
Security model	Legacy model	Standard model		
User management type	-	Standalone management	Domain management or Combination management	Linked domain management (*2)
Required procedures	Read the reference that follows the table.			

*1: When you install ProSafe-RS and PRM on the same computer with linked domain management, ensure that the software revision of ProSafe-RS is R4.06.00 or later and the software revision of PRM is R4.04.00 or later.
*2: Linked domain management is supported by ProSafe-RS R4.06.00 or later and PRM R4.04.00 or later software revisions.

SEE ALSO

For more information about the settings required to use Forced I/O Viewer Package, refer to:

B4.4, “Settings Required to Use the Forced I/O Viewer Function” on page B4-5

D1.4 ProSafe-RS and Exaquantum

This section describes the settings when connecting ProSafe-RS and Exaquantum.

D1.4.1 ProSafe-RS SOE OPC Interface Package and Exaquantum PIMS Server

Connecting the SOE OPC Interface Package and Exaquantum PIMS Server enables the Exaquantum PIMS Server to collect SOE data from SCS through the OPC interface.

Enabling Exaquantum to collect SOE data from SCS

To use Exaquantum PIMS Server as an OPC client and perform OPC communication with an SENG running the SOE OPC Interface Package, you need to perform the settings described below.

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table. The logon type setting on the SENG and the setting to use Exaquantum as an OPC client are mandatory in all cases.

IMPORTANT

As a basic rule, the security model and user management type must be consistent in the products to be connected. However, ProSafe-RS and Exaquantum can be connected even if different security model or user management type is applied.

Table D1.4.1-1 Connection information: ProSafe-RS SOE OPC Interface Package and Exaquantum R2.60 or later

Integration code	0202-0801-02-01		
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later		
Product 2	PIMS server of Exaquantum R2.60 or later		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination management
Required procedures	Refer to "● Setting the logon type" and "● When the Legacy model is applied to both products."	Refer to "● Setting the logon type" and "● When the Standard model is applied to both products."	

Table D1.4.1-2 Connection information: Different security model - Case 1

Integration code	0202-0801-02-01	
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later	
Product 2	PIMS server of Exaquantum R2.60 or later	
Security model	Standard model (ProSafe-RS) Legacy model (Exaquantum)	
User management type of ProSafe-RS	Standalone management	Domain/Combination management
Required procedures	Refer to "● Setting the logon type" and "● When the Standard model is applied to ProSafe-RS and the Legacy model to Exaquantum."	

Table D1.4.1-3 Connection information: Different security model - Case 2

Integration code	0202-0801-02-01
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later

Continues on the next page

Table D1.4.1-3 Connection information: Different security model - Case 2 (Table continued)

Product 2	PIMS server of Exaquantum R2.60 or later	
Security model	Legacy model (ProSafe-RS) Standard model (Exaquantum)	
User management type of Exaquantum	Standalone management	Domain/Combination management
Required procedures	Refer to "● Setting the logon type" and "● When the Legacy model is applied to ProSafe-RS and the Standard model to Exaquantum."	

Table D1.4.1-4 Connection information: Legacy model applied ProSafe-RS and Exaquantum version earlier than R2.60

Integration code	0202-0801-02-02
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later
Product 2	PIMS server of Exaquantum R2.20 or later but earlier than R2.60
Security model	Legacy model (ProSafe-RS) - (Exaquantum)
User management type	-
Required procedures	Refer to "● Setting the logon type" and "● When the Legacy model is applied to both products."

Table D1.4.1-5 Connection information: Standard model applied ProSafe-RS and Exaquantum version earlier than R2.60

Integration code	0202-0801-02-02	
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later	
Product 2	PIMS server of Exaquantum R2.20 or later but earlier than R2.60	
Security model	Standard model (ProSafe-RS) - (Exaquantum)	
User management type of ProSafe-RS	Standalone management	Domain/Combination management
Required procedures	Refer to "● Setting the logon type" and "● When the Standard model is applied to ProSafe-RS and the Legacy model to Exaquantum."	

SEE ALSO For more information about the details on setting up an OPC client, refer to:

C3., “Setup for using the OPC client” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

● Setting the Logon Type

To connect Exaquantum with an SENG (OPC server) running the SOE OPC interface package of ProSafe-RS R3.01.00 or later, you need to set the logon type on the SENG beforehand. After performing this setting, perform the required setting on Exaquantum.

1. Log in to the system as a user belonging to PSF_ENGINEER or PSF_ENGINEER_LCL.
2. Start SOE OPC Parameter Setting.
   The SOE OPC Interface Settings dialog box appears.
3. Click the [Edit] in [OPC Security Settings].
   A dialog box where you can select a type of logon to the OPC server appears.

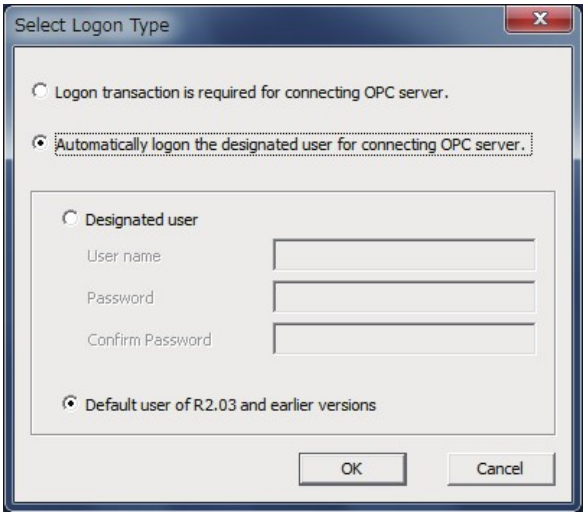


Figure D1.4.1-1 Select Logon Dialog Box

4. Select [Automatically logon the designated user for connecting OPC server.] and then [Default user of R2.03 and earlier versions], and click [OK].

When the Legacy model is applied to both products

1. Set the logon type on the SENG.
2. Add an Exaquantum program user on the SENG.

TIP

The user name and password of the Exaquantum program user should be as follows:

User name: Quantumuser (default user name, changeable with a supplied tool)

Password: quantumuser (default password, changeable with a supplied tool)

3. On the SENG, create the same user account as the logon user account for running Exaquantum.
4. On the SENG and the computer installed with Exaquantum, perform the setting for using Exaquantum as an OPC client.

When the Standard model is applied to both products

1. Set the logon type on the SENG.
2. Configure the DCOM settings on the SENG. For procedures, refer to the user's manual "Engineering Guide Vol.2".
3. On the SENG, create QTM_PROCESS, which is the Exaquantum program user account.
   a. Insert the Exaquantum software medium and start the command prompt window, then move to the following folder.
   (Drive):\Tools
   b. Run the following command.
   `CreateQTMProcess.exe`

   The QTM_PROCESS user account is created.
4. Add the QTM_PROCESS user you have created to the following user group on the SENG.
   - In the case of standalone management or when combination management is applied on some computers: PSF_OPC
   - In the case of domain management or when combination management is applied on all computers: PSF_OPC_LCL

5. On the SENG, create the same user account as the logon user account for running Exaquantum and add the created user account to the PSF_OPC group.
6. On the computer installed with Exaquantum, create the PSF_PROCESS user account.
   a. Insert the ProSafe-RS software medium and start the command prompt window, then move to the following folder.
   (Drive):\ProSafe-RS\SECURITY
   b. Run the following command.
   `ProSafe.Security.CreateProSafeProcess.exe`
   The PSF_PROCESS user account is created.
7. Add the PSF_PROCESS user you have created to the following user group on the computer installed with Exaquantum.
   - In the case of standalone management or when combination management is applied on some computers: QTM_OPC
   - In the case of domain management or when combination management is applied on all computers: QTM_OPC_LCL
8. On the SENG and the computer installed with Exaquantum, perform the setting for using Exaquantum as an OPC client.

SEE ALSO For more information about configuring the DCOM settings, refer to:

"■ DCOM settings" in C2.2, "Overview of product security settings" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

When the Standard model is applied to ProSafe-RS and the Legacy model to Exaquantum

1. Set the logon type on the SENG.
2. Configure the DCOM settings on the SENG. For procedures, refer to the user's manual "Engineering Guide Vol.2".
3. Add an Exaquantum program user on the SENG.

TIP The user name and password of the Exaquantum program user should be as follows:

User name: Quantumuser (default user name, changeable with a supplied tool)

Password: quantumuser (default password, changeable with a supplied tool)

4. Add the Quantumuser user you have created to the following user group on the SENG.
   - In the case of standalone management or when combination management is applied on some computers: PSF_OPC
   - In the case of domain management or when combination management is applied on all computers: PSF_OPC_LCL
5. On the SENG, create the same user account as the logon user account for running Exaquantum and add the created user account to the PSF_OPC group.
6. On the computer installed with Exaquantum, create the PSF_PROCESS user account.
   a. Insert the ProSafe-RS software medium and start the command prompt window, then move to the following folder.
   (Drive):\ProSafe-RS\SECURITY
   b. Run the following command.
   `ProSafe.Security.CreateProSafeProcess.exe`
   The PSF_PROCESS user account is created.

7. On the SENG and the computer installed with Exaquantum, perform the setting for using Exaquantum as an OPC client.

SEE ALSO For more information about configuring the DCOM settings, refer to:

"■ DCOM settings" in C2.2, "Overview of product security settings" in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

When the Legacy model is applied to ProSafe-RS and the Standard model to Exaquantum

1. Set the logon type on the SENG.
2. On the SENG, create QTM_PROCESS, which is the Exaquantum program user account.
   a. Insert the Exaquantum software medium and start the command prompt window, then move to the following folder.
   (Drive):\Tools
   b. Run the following command.
   `CreateQTMProcess.exe`

   The QTM_PROCESS user account is created.
3. On the SENG, create the same user account as the logon user account for running Exaquantum.
4. On the computer installed with Exaquantum, create the EXAUSER user account. The password should also be EXAUSER.
5. Add the EXAUSER user you have created to the following user group on the computer installed with Exaquantum.
   - In the case of standalone management or when combination management is applied on some computers: QTM_OPC
   - In the case of domain management or when combination management is applied on all computers: QTM_OPC_LCL
6. On the SENG and the computer installed with Exaquantum, perform the setting for using Exaquantum as an OPC client.

Appendix 1. Setting Switches

You can set the domain number and station number by configuring the setting switches on the printed circuit board of the control bus interface card and Vnet/IP interface card.

Domain Numbers and DIP Switch Positions

The following table lists the domain numbers and corresponding setting switch positions for the control bus interface card and Vnet/IP interface card. Set the DIP switches as shown in the table to adjust to the required domain number.

Table Appendix 1-1 Domain Numbers and DIP Switch Positions

Domain number	DIP switch bit number(*1)							
	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	1	0
3	1	0	0	0	0	0	1	1
4	0	0	0	0	0	1	0	0
5	1	0	0	0	0	1	0	1
6	1	0	0	0	0	1	1	0
7	0	0	0	0	0	1	1	1
8	0	0	0	0	1	0	0	0
9	1	0	0	0	1	0	0	1
10	1	0	0	0	1	0	1	0
11	0	0	0	0	1	0	1	1
12	1	0	0	0	1	1	0	0
13	0	0	0	0	1	1	0	1
14	0	0	0	0	1	1	1	0
15	1	0	0	0	1	1	1	1
16	0	0	0	1	0	0	0	0
17	1	0	0	1	0	0	0	1
18	1	0	0	1	0	0	1	0
19	0	0	0	1	0	0	1	1
20	1	0	0	1	0	1	0	0
21	0	0	0	1	0	1	0	1
22	0	0	0	1	0	1	1	0
23	1	0	0	1	0	1	1	1
24	1	0	0	1	1	0	0	0
25	0	0	0	1	1	0	0	1
26	0	0	0	1	1	0	1	0
27	1	0	0	1	1	0	1	1
28	0	0	0	1	1	1	0	0
29	1	0	0	1	1	1	0	1
30	1	0	0	1	1	1	1	0
31	0	0	0	1	1	1	1	1

*1: Bit 1: Odd parity, Bits 2, 3: Fixed to 0, Bits 4 to 8: Domain number

Station Numbers and DIP Switch Positions

The following table lists the station numbers and corresponding setting switch positions for the control bus interface card and Vnet/IP interface card. Set the DIP switches as shown in the table to adjust to the required station number.

Table Appendix 1-2 Station Numbers and DIP Switch Positions

Station number	DIP switch bit numbers (*1)							
	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	1	0
3	1	0	0	0	0	0	1	1
4	0	0	0	0	0	1	0	0
5	1	0	0	0	0	1	0	1
6	1	0	0	0	0	1	1	0
7	0	0	0	0	0	1	1	1
8	0	0	0	0	1	0	0	0
9	1	0	0	0	1	0	0	1
10	1	0	0	0	1	0	1	0
11	0	0	0	0	1	0	1	1
12	1	0	0	0	1	1	0	0
13	0	0	0	0	1	1	0	1
14	0	0	0	0	1	1	1	0
15	1	0	0	0	1	1	1	1
16	0	0	0	1	0	0	0	0
17	1	0	0	1	0	0	0	1
18	1	0	0	1	0	0	1	0
19	0	0	0	1	0	0	1	1
20	1	0	0	1	0	1	0	0
21	0	0	0	1	0	1	0	1
22	0	0	0	1	0	1	1	0
23	1	0	0	1	0	1	1	1
24	1	0	0	1	1	0	0	0
25	0	0	0	1	1	0	0	1
26	0	0	0	1	1	0	1	0
27	1	0	0	1	1	0	1	1
28	0	0	0	1	1	1	0	0
29	1	0	0	1	1	1	0	1
30	1	0	0	1	1	1	1	0
31	0	0	0	1	1	1	1	1
32	0	0	1	0	0	0	0	0
33	1	0	1	0	0	0	0	1

Continues on the next page

Table Appendix 1-2 Station Numbers and DIP Switch Positions (Table continued)

Station number	DIP switch bit numbers (*1)							
	1	2	3	4	5	6	7	8
. . .	. . .							
60	1	0	1	1	1	1	0	0
61	0	0	1	1	1	1	0	1
62	0	0	1	1	1	1	1	0
63	1	0	1	1	1	1	1	1
64	0	1	0	0	0	0	0	0

*1: Bit 1: Odd parity, Bits 2 to 8: Station number

Appendix 2. Procedure for Erasing VI702 Internal Settings

If you intend to reuse a VI702 card used in another system for a stand-alone ProSafe-RS system, erase the settings within the card using the following procedure.

1. Turn off the power of the computer. For safety, remove the power plug from the outlet.
2. Set the DIP switches (SW1) for the domain number on the VI702 as follows:

Table Appendix 2-1 Setting of DIP Switches for Domain Number Setting (SW1)

Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8
1	1	0	0	0	0	0	1
Parity			MSB				LSB

3. Set the DIP switches (SW2) for the station number on the VI702 as follows:

Table Appendix 2-2 Setting of DIP Switches for Station Number Setting (SW2)

Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8
0	0	0	0	0	0	0	1
Parity	MSB						LSB

4. Check that Bit 1 through Bit 4 of the DIP switches (SW4) for the Action Mode are all set to the off position on the VI702.
5. Remove the cover of the computer.
6. Insert the VI702 in the corresponding slot and fix the card.
7. Put back the cover of the computer.
8. Do not connect the cable to either BUS1 or BUS2.
9. Put back the power cord of the computer.
10. Start the computer, and then go to BIOS setting panel instead of starting Windows. If the Windows started, it is necessary to shutdown and switch off the computer, and start the computer for BIOS setting again.
11. Wait for about a minute after BIOS setting panel appears.
12. Turn off the power of the computer. For safety, remove the power plug from the outlet.
13. Remove the VI702 from the slot.

SEE ALSO For more information about how to display the BIOS setting window, refer to:

The manual of the computer

Appendix 3. Vnet/IP Interface Management Tool

By using the Vnet/IP Interface Management Tool, you can set the domain number and station number managed by the Vnet/IP Interface Package.

Changing the Domain Number and Station Number

Follow these steps to set the domain number and station number managed by the Vnet/IP Interface Package:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Select [YOKOGAWA Virtualization] > [VnetIP interface management tool] from the Start menu.
   Vnet/IP interface management tool starts.
3. Open the Settings tab of the Vnet/IP interface management tool.
4. Set the domain number in [Domain No] and the station number in [Station No], and then click [Save].

TIP

You can set a number in the range from 1 to 31 as the domain number (1 to 16 in the case of CENTUM integration), and from 1 to 64 as the station number. If both domain number and station number are set to 0, Vnet/IP communication is disabled and communication to the control network is not possible.

On a virtual machine where you run an FCS simulator that can be operated through remote connection from another HIS by installing the Expanded Test Functions and SCS Simulator Package, set both the domain number and the station number to 0.

Note that the license of Vnet/IP Interface Package is not required when using only the test function with the domain number and the station number set to 0.

5. Click [CLOSE], and restart the virtual machine.

Operation Status of the Vnet/IP Interface Package

The [Monitor] shows the following information:

- Version information of the Vnet/IP Interface Package
- Operation status of the Vnet/IP Interface Package
- Domain number and station number
- Presence of different Vnet/IP firmware versions

Version information

The version number of the Vnet/IP Interface Package is displayed.

Operation status

One of the following five operation statuses is displayed.

Stop:	Indicates that the Vnet/IP Interface Package is not functioning.
Starting:	Indicates that the domain number, station number, and configuration are being checked before the package goes into operation.
Waiting the license:	Indicates that the package is waiting for the license to be granted.
Working:	Indicates that the package is operating properly.

Stop (error message):	Indicates that the package is not functioning.

Domain number and station number

The domain number and station number are displayed.

Presence of different Vnet/IP firmware revisions

The revision information of the Vnet/IP firmware is displayed. If more than one of stations use old firmwares, they are delimited with a comma.

Display example:	06R, 13L
Meaning:	The Vnet/IP firmware implemented on the right side card of station number 6 and the Vnet/IP firmware implemented on the left side card of station number 13 are old.

What to Do When an Error Occurs

When using the Vnet/IP Interface Management Tool, error messages may appear. This section explains the conditions for error messages to occur and countermeasures.

Invalid Windows service registration

- Message

  Invalid Windows service registration

- Condition for occurrence

  This error message is generated when any one of the Vnet/IP Interface Package services, “YWVNT BKNET Service,” “YWVNT VnetIP Stack Service,” and “YWVNT VnetIP Privileged Service” is not registered as Windows service, or the Vnet/IP Interface Package services are not configured to start automatically.

- Remedy

  Install the Vnet/IP Interface Package again.

SEE ALSO For more information about the procedure to install the Vnet/IP Interface Package, refer to:

B3.3.4, “Installing the Vnet/IP Interface Package on a Virtual Machine” on page B3-24

BUS1 not found

- Message

  BUS1 not found

- Condition for occurrence

  This message is generated when the name of control network 1 is invalid.

- Remedy

  Rename control network 1 to `VnetIPBUS1`.

SEE ALSO For more information about how to change the name of control network 1, refer to:

“■ Rename Local Area Connections” on page B3-37

BUS2 not found

- Message

  BUS2 not found

- Condition for occurrence

  This message is generated when the name of control network 2 is invalid.

- Remedy

  Rename control network 2 to `VnetIPBUS2`.

SEE ALSO For more information about how to change the name of control network 2, refer to:

"■ Rename Local Area Connections" on page B3-37

Invalid domain number or station number

- Message

  Invalid domain number or station number

- Condition for occurrence

  This message is generated when the domain number or station number managed by the Vnet/IP Interface Package are invalid.

- Remedy

  Using the Vnet/IP Interface Management Tool, check the domain number and station number managed by the Vnet/IP Interface Package and set to the correct values.

SEE ALSO For more information about how to set the domain number and station number managed by the Vnet/IP Interface Package, refer to:

"■ Changing the Domain Number and Station Number" on page App.3-1

Station of the specified domain number and station number already exists

- Message

  Station of the specified domain number and station number already exists

- Condition for occurrence

  This message is generated when the same domain number or station number are already used for another station.

- Remedy

  Using the Vnet/IP Interface Management Tool, check the domain number and station number managed by the Vnet/IP Interface Package and set to the correct values.

SEE ALSO For more information about how to set the domain number and station number managed by the Vnet/IP Interface Package, refer to:

"■ Changing the Domain Number and Station Number" on page App.3-1

IT security not applied

- Message

  IT security not applied

- Condition for occurrence

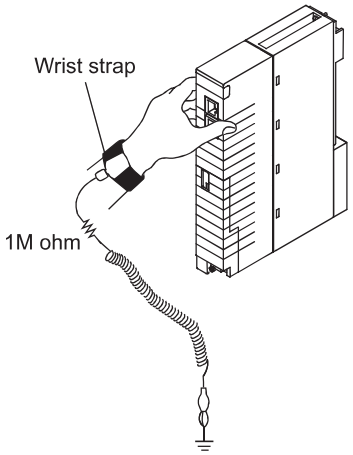
This message is generated when IT security has not been applied after installation of the Vnet/IP Interface Package.

- Remedy
  Apply IT security.

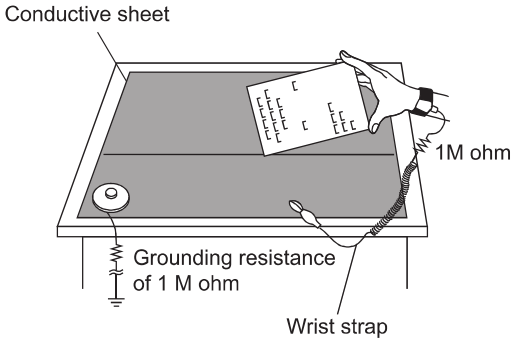
Appendix 4. Antistatic Precautions When Handling Hardware

When doing maintenance work, take the following precautions to avoid electrostatic problems.

- When storing or carrying parts for maintenance, put them in an antistatic bag. (When shipped, they are placed in an antistatic bag labeled with cautions against electrostatic problems.)
- Wear a wrist strap with a 1M ohm grounding resistor then ground the wrist strap.
- When working on the bench, place the parts on a conductive sheet grounded via a 1 M ohm resistor and wear wrist strap. Keep static-chargeable plastic materials away from the parts.
- Never touch the parts with bare hands, without using a wrist strap and a conductive sheet.



Connect the wrist strap to the grounding terminal or unpainted part of the frame (grounded).



When working with a product with battery on a conductive sheet, set the battery ON/OFF switch to the OFF position or remove the battery.

Figure Appendix 4-1 Using a Wrist Strap

The wrist strap and conductive sheet are available from YOKOGAWA sales agents.

Appendix 5. Customization at Installation of Windows 10

This section describes how to customize Windows settings during installation of Windows 10 Enterprise 2016 LTSB.

TIP You do not need to perform this customization on Windows 10 IoT Enterprise 2016 LTSB installed computers provided by YOKOGAWA.

Procedure for Customization at installation of Windows 10

1. The following screen appears during installation of Windows 10 Enterprise 2016 LTSB.

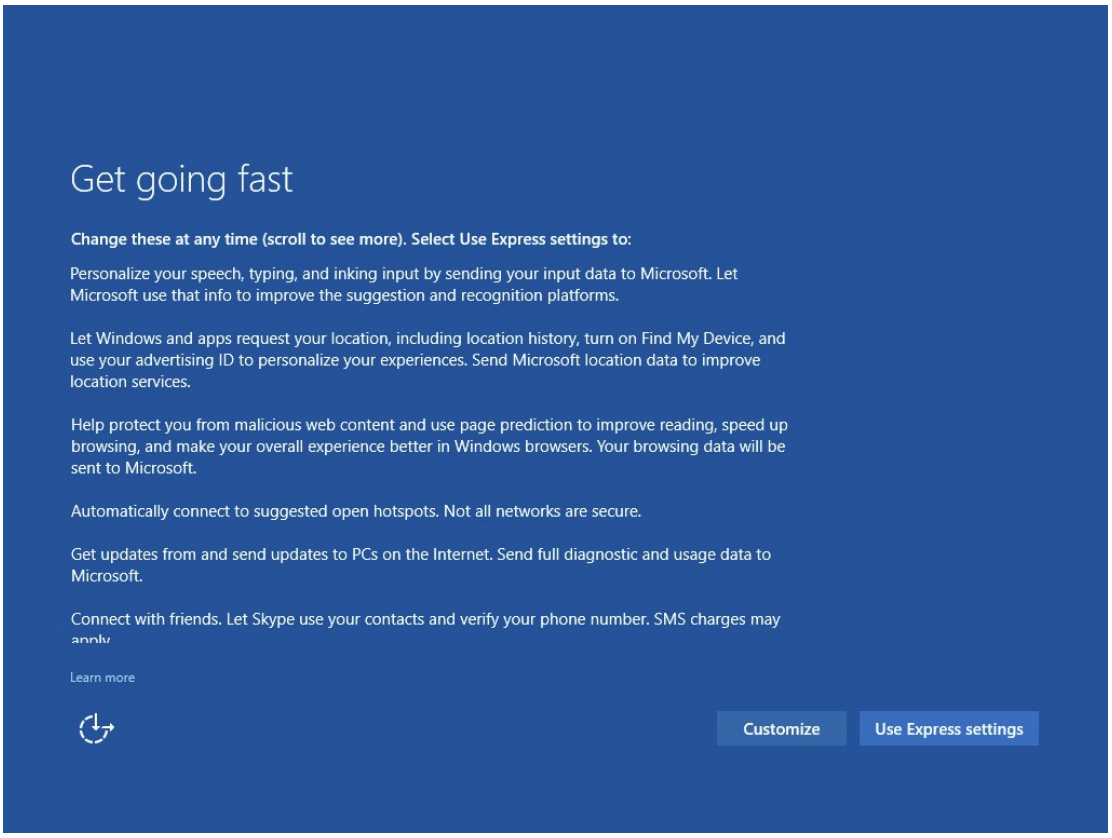


Figure Appendix 5-1 Screen That Appears When Installing Windows 10

Click [Customize].

The Customize Settings window appears.

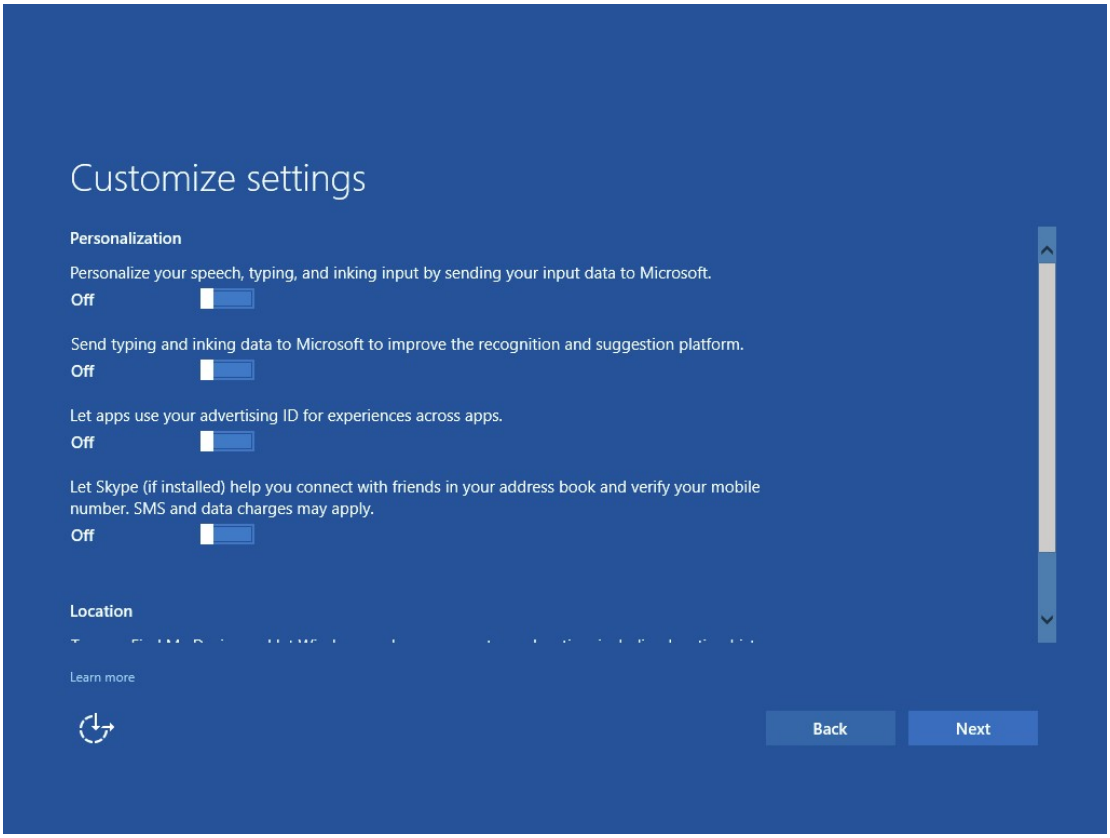


Figure Appendix 5-2 Customize Settings Window

2. Set all settings to [Off].
3. Click [Next] to continue installing Windows 10 Enterprise 2016 LTSB.

Appendix 6. Compatibility between Revisions and Cautionary Notes for Upgrading

IMPORTANT

Be sure to take a backup of the whole project before upgrading ProSafe-RS.

This section provides the compatibility information for earlier versions of ProSafe-RS software released in the past and the cautionary notes for upgrading that were published at the time of each release. In this section, users can confirm the procedures for using the new features supported in each release in the past and the important descriptions about SCS specifications that were released in the past as the compatibility information.

When you upgrade ProSafe-RS, install only the software of the release number you want to use. However, for the required procedures after the installation, read the cautionary notes for upgrading for all release numbers between the release number of the software currently installed on your computer and the release number of the software you want to use.

SEE ALSO For more information about precautions related to major specification additions and changes in previously released revisions, refer to:

Appendix 3., “Precautions related to main specification additions and modifications” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Appendix 6.1 Cautionary Notes for Upgrading to R4.01

This section provides cautionary notes for upgrading from R3.02.20 to R4.01. When you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.

IMPORTANT

Use the R6.02 or a later version of CENTUM VP when integrating ProSafe-RS with CENTUM VP.

In R4.01, be sure to register the RS project in the AD project regardless of the engineering method.

SEE ALSO

For more information about compatibility and cautionary notes for upgrading up to ProSafe-RS R3.02.10, refer to:

Appendix 4., "Compatibility between Revisions and Cautionary Notes for Upgrading" in Installation for ProSafe-RS R3 (IM 32Q01C50-31E)

For more information about cautionary notes when upgrading the revision to ProSafe-RS R3.02.20, refer to:

C5., "Upgrading to R3.02.20" in Installation for ProSafe-RS R3 (IM 32Q01C50-31E)

For more information about creating an AD project, refer to:

"■ Creating AD projects" in C1.2.1, "Creating and deleting AD projects" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects in an AD project, refer to:

C1.2.3, "Registering RS projects in the AD project" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Software Revisions

The respective software release number of R4.01 is as follows:

Software release number R4.01.xx (*1)

- SENG software release number: R4.01.xx (*1)
- SCS system program release number: R4.01.xx (*1)

*1: The last two digits of the revision number will be changed in accordance with the software revisions after the release of R4.01.00.

● Inter-SCS Safety Communication

The release number of the SCS system program of an SCS that performs Inter-SCS safety communication with SCS with system program version R4.01 must be of R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be of R1.02 or later.

● Control Bus Drivers

You do not need to update the control bus driver if the control bus driver provided in R3.02.20 is installed on the computer.

SEE ALSO

For more information about how to update the control bus driver, refer to:

"● Updating the Control Bus Driver" on page C4-5

Basic Procedures for Upgrading

To use the added or modified features, install the ProSafe-RS software R4.01 or later and open the existing SCS project.

Procedure for Using Added and Modified Features

The following functions that have been added or modified in R4.01 cannot be used in the basic upgrading procedures. Once you have upgraded the SENG software to R4.01, offline download to the SCS and other operations are required. The procedures to use the respective functions are described below.

SEE ALSO For more information about settings after upgrading software, refer to:

C4.2.4, “Procedures for using new functions” on page C4-22

New station (S2SC70)

To use the S2SC70 station, which is newly added in R4.01, you need to perform "Procedure C" on an SENG of R4.01 or later. In S2SC70, N-IO systems can be used.

Annunciator messages with tag names

To use annunciator messages with tag names, "Procedure D" must be performed on an SENG of R4.01 or later. To use annunciator messages with tag names, set the applicable parameters in a Builder.

Modbus/TCP subsystem communication

To use subsystem communication using the Modbus/TCP protocol, "Procedure C" must be performed on an SENG of R4.01 or later.

I/O List Engineering of AD Suite

To use I/O List Engineering of AD Suite that has been added in R4.01, "Procedure C" must be performed on an SENG of R4.01 or later. In R4.01, be sure to register the RS project in the AD project regardless of the engineering method. You should then create and set an SCS project; otherwise, I/O List Engineering cannot be implemented. To upgrade an existing SCS to start I/O List Engineering, you need an I/O list matching the definitions of the original SCS project.

History Management Function of AD Suite

To use the history management function of AD Suite that has been added in R4.01, "Procedure A" must be performed on an SENG of R4.01 or later. In R4.01, be sure to register the RS project in the AD project regardless of the engineering method.

Appendix 6.2 Cautionary Notes for Upgrading to R4.02

This section provides cautionary notes for upgrading from R4.01 to R4.02. When you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.

IMPORTANT

Use the R6.02 or a later version of CENTUM VP when integrating ProSafe-RS with CENTUM VP.

In R4.01 or later, be sure to register the RS project in the AD project regardless of the engineering method.

SEE ALSO

For more information about cautionary notes when upgrading the version to ProSafe-RS R4.01 from an earlier version, refer to:

Appendix 6.1, “Cautionary Notes for Upgrading to R4.01” on page App.6-2

For more information about creating an AD project, refer to:

“■ Creating AD projects” in C1.2.1, “Creating and deleting AD projects” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects in an AD project, refer to:

C1.2.3, “Registering RS projects in the AD project” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Software Revisions

The respective software release number of R4.02 is as follows:

Software release number R4.02.xx (*1)

- SENG software release number: R4.02.xx (*1)
- SCS system program release number: R4.02.xx (*1)

*1: The last two digits of the revision number will be changed in accordance with the software revisions after the release of R4.02.00.

● Inter-SCS Safety Communication

The release number of the SCS system program of an SCS that performs Inter-SCS safety communication with SCS with system program version R4.02 must be of R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be of R1.02 or later.

● Control Bus Drivers

You do not need to update the control bus driver if the control bus driver provided in R3.02.20 is installed on the computer.

■ Basic Procedure for Upgrading

To use the added or modified features, install the ProSafe-RS software R4.02 or later and open the existing SCS project.

Integration with External Engineering Tool

To use the feature for integration with iDefine, an external engineering tool, that has been added in R4.02, "Procedure A" must be performed on an SENG of R4.02 or later.

Procedure for Using Added and Modified Features

The following functions that have been added or modified in R4.02 cannot be used in the basic upgrading procedures. After you have upgraded the SENG software to R4.02, offline download to the SCS and other operations are required. The procedures to use the respective functions are described below.

SEE ALSO For more information about settings after upgrading software, refer to:

C4.2.4, “Procedures for using new functions” on page C4-22

Duplexed Interface for DNP3 Communication

To use the duplexed interface for DNP3 communication that has been added in R4.02, "Procedure C" must be performed on an SENG of R4.02 or later. The duplexed interface for DNP3 communication is available only in SSC57.

Support for the RoHS Directive Compliant Processor Module SCP451-□3

To use the RoHS directive compliant processor module SCP451-□3, "Procedure B" must be performed on an SENG of R4.02 or later. The RoHS directive compliant processor module SCP451-□3 can be used in SSC50 and SSC57.

Cautionary Notes for Upgrading When ALE111 is Used

You must be careful when upgrading the system if ALE111 is used for Modbus slave or DNP3 communication.

During the first online change download after SENG has been upgraded, the latest communication program for ALE111 is also downloaded. Because ALE111 is restarted in this process, communication with the Modbus or DNP3 master s is disabled temporarily. Therefore, you must perform online change download with appropriate timing after the upgrade.

For the details, read the following descriptions:

Upgrade Procedure When ALE111 is Used for Modbus Slave Communication

If ALE111 is used for Modbus slave communication and you are upgrading from R4.01.00 or earlier to R4.02.00 or later, follow these steps to download the latest communication program to ALE111:

IMPORTANT

- You can build the SCS project without changing the ALE111 definitions. If you perform an online change download the first time after running a build, the latest communication program is downloaded to ALE111, even if no change has been made to the communication definitions for the ALE111.
- The latest communication program will be downloaded to ALE111 also when you perform an online change download after modifying only the definitions not relevant to ALE111.
- During online change download, communication with the Modbus master is disabled. (*1)You must perform an online change download only when no problem is caused even if the communication with the Modbus master is interrupted.
- When upgrading the system, if you also want to perform modification of application that requires addition of communication modules other than ALE111 for Modbus slave communication at the same time, you must observe the following precautions. You must first perform the following steps 1 through 5 to download the latest program to the existing ALE111, and then modify the application. If you do not follow this procedure, upgrading of the communication program may fail. If failed, offline downloading to the SCS is required.

*1: Even if the communication interface with the Modbus master is duplexed by using two ALE111 modules, the communication is disabled during online change download.

1. Upgrade ProSafe-RS from R4.01.00 or earlier to R4.02.00 or later.
2. Run a build for the SCS project regardless of whether you have made changes.
3. Using Integrity Analyzer and Cross Reference Analyzer, perform an approval check.

TIP

Differences in the communication program are not displayed.

4. Run an online change download.
5. Confirm the revision number of the communication program.
   The revision number of the communication program that is downloaded in R4.02.00 or later is R4.02.00. When the online change download is complete, confirm that the communication program of R4.02.00 has been downloaded to all ALE111 modules by using IOM Report. You can find the revision number of the communication program at the address 0x0120 in the IOM Report for ALE111.

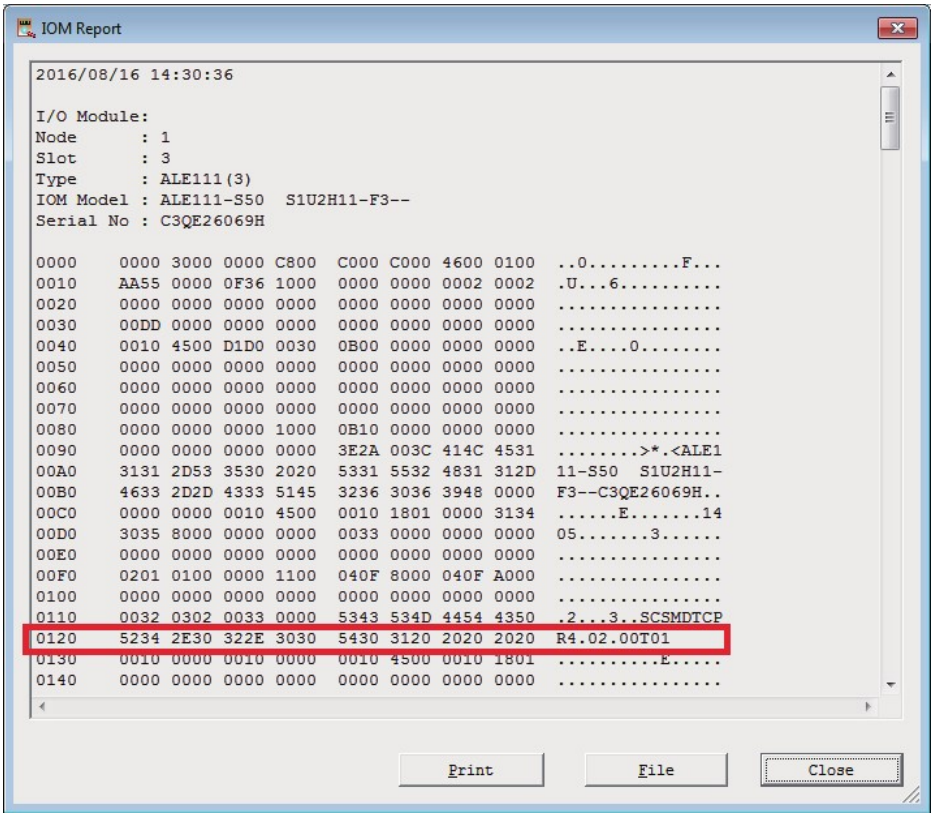


Figure Appendix 6.2-1 IOM Report for ALE111 Used for Modbus Slave Communication

If you want to perform modification of application at the same time, perform step 6.

6. Perform modification of the application that requires addition of communication modules other than ALE111 for Modbus slave communication.

Upgrade Procedure When ALE111 is Used for DNP3 Communication

If ALE111 is used for DNP3 communication and you are upgrading from R4.01.00 or earlier to R4.02.00 or later, follow these steps to download the latest communication program to ALE111:

IMPORTANT

- You can build the SCS project without changing the ALE111 definitions. If you perform an online change download the first time after running a build, the latest communication program is downloaded to ALE111, even if no change has been made to the communication definitions for the ALE111.
- The latest communication program will be downloaded to ALE111 also when you perform an online change download after modifying only the definitions not relevant to ALE111.
- During online change download, communication with the DNP3 master is disabled. You must perform an online change download only when no problem is caused even if the communication with the DNP3 master is interrupted.
- When upgrading the system, if you also want to perform modification of application that requires addition of communication modules other than ALE111 for DNP3 communication at the same time, you must observe the following precautions. You must first perform the following steps 1 through 5 to download the latest program to the existing ALE111, and then modify the application. If you do not follow this procedure, upgrading of the communication program may fail. If failed, offline downloading to the SCS is required.

1. Upgrade ProSafe-RS from R4.01.00 or earlier to R4.02.00 or later.
2. Run a build for the SCS project regardless of whether you have made changes.
3. Using Integrity Analyzer and Cross Reference Analyzer, perform an approval check.

TIP Differences in the communication program are not displayed.

4. Run an online change download.
5. Confirm the revision number of the communication program.
   The revision number of the communication program that is downloaded in R4.02.00 or later is R4.02.00. When the online change download is complete, confirm that the communication program of R4.02.00 has been downloaded to all ALE111 modules by using IOM Report. You can find the revision number of the communication program at the address 0x0120 in the IOM Report for ALE111.

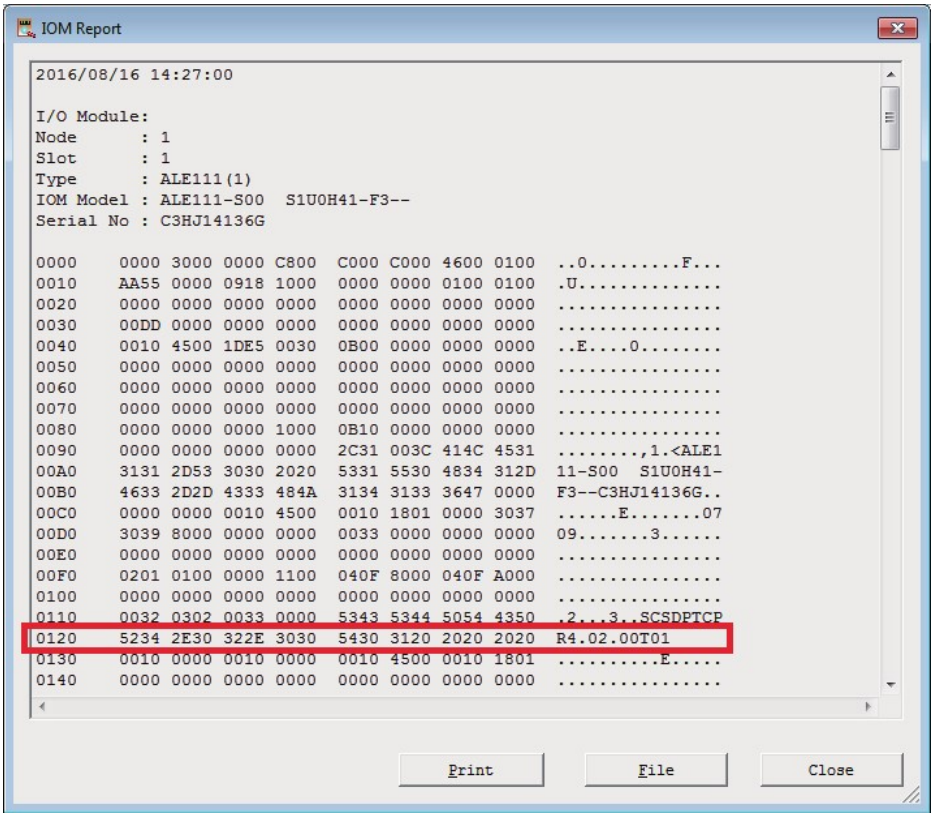


Figure Appendix 6.2-2 IOM Report for ALE111 Used for DNP3 Communication

If you want to perform modification of application at the same time, perform step 6.

6. Perform modification of the application that requires addition of communication modules other than ALE111 for DNP3 communication.

Appendix 6.3 Cautionary Notes for Upgrading to R4.03

This section provides cautionary notes for upgrading from R4.02 to R4.03. When you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.

IMPORTANT

Use the R6.02 or a later version of CENTUM VP when integrating ProSafe-RS with CENTUM VP.

In R4.01 or later, be sure to register the RS project in the AD project regardless of the engineering method.

SEE ALSO

For more information about creating an AD project, refer to:

"■ Creating AD projects" in C1.2.1, "Creating and deleting AD projects" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects in an AD project, refer to:

C1.2.3, "Registering RS projects in the AD project" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about cautionary notes when upgrading the version to ProSafe-RS R4.01 from an earlier version, refer to:

Appendix 6.1, "Cautionary Notes for Upgrading to R4.01" on page App.6-2

For more information about cautionary notes when upgrading the revision to ProSafe-RS R4.02, refer to:

Appendix 6.2, "Cautionary Notes for Upgrading to R4.02" on page App.6-4

Software Revisions

The respective software release number of R4.03 is as follows:

Software release number R4.03.xx (*1)

- SENG software release number: R4.03.xx (*1)
- SCS system program release number: R4.03.xx (*1)

*1: The last two digits of the revision number will be changed in accordance with the software revisions after the release of R4.03.

Inter-SCS Safety Communication

The release number of the SCS system program of an SCS that performs Inter-SCS safety communication with SCS with system program version R4.03 must be of R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be of R1.02 or later.

Control Bus Drivers

The control bus drivers that are installed on the computer should be upgraded to the version supplied in R4.03.

Basic Procedure for Upgrading

To use the added or modified features, install the ProSafe-RS software R4.03 or later and open the existing SCS project.

Procedure for Using Added and Modified Features

The following functions that have been added or modified in R4.03 cannot be used in the basic upgrading procedures. After you have upgraded the SENG software to R4.03, offline download to the SCS and other operations are required. The procedures to use the respective functions are described below.

SEE ALSO For more information about settings after upgrading software, refer to:

C4.2.4, “Procedures for using new functions” on page C4-22

Device Reset Function

To use the device reset function with SAI143, you need to perform “Procedure C” on an SENG of R4.03 or later.

Function Blocks for Fire and Gas Devices

To use the function blocks for fire and gas devices HSDTR and GASDTR, which are newly added in R4.03, you need to perform “Procedure C” on an SENG of R4.03 or later.

Alarm Suppression Function During Device Reset

To use the Alarm Suppression Function During Device Reset, you need to perform “Procedure C” on an SENG of R4.03 or later. The Alarm Suppression Function During Device Reset cannot be used with SSC57.

Chattering Alarm Suppression Function

To use the Chattering Alarm Suppression Function, you need to perform “Procedure C” on an SENG of R4.03 or later. The Chattering Alarm Suppression Function cannot be used with SSC57.

Digital I/O Module (S2MDV843)

To use the digital I/O module S2MDV843 newly added in R4.03, you must follow the “Procedure C” on SENG of R4.03 or later. S2MDV843 can be used with an S2SC70 N-IO system.

Cautionary Notes for Upgrading When ALE111 is Used

You must be careful when upgrading the system if ALE111 is used for Modbus slave or DNP3 communication.

SEE ALSO For more information about the precautions when upgrading a system where ALE111 is used for Modbus slave or DNP3 communication, refer to:

“■ Cautionary Notes for Upgrading When ALE111 is Used” on page App.6-5

Cautionary Notes When Opening a New Revision AD Project from an Older Revision AD Organizer

From AD Organizer that was installed from the ProSafe-RS R4.01 or R4.02 software medium, you cannot open AD projects created by using AD Organizer of ProSafe-RS R4.03 or later or AD projects upgraded to R4.03 or later.

In such a case, apply one of the following compatibility patches:

- Compatibility patch for R4.01: R4.01.34
- Compatibility patch for R4.02: R4.02.01

TIP

- Also after an AD project has been upgraded, SCS projects of different revisions can exist together in the AD project.
- If you want to continue engineering of older revision SCS projects that are contained in the AD project without upgrading them, you must open the AD project from the corresponding older revision AD Organizer.
- For how to obtain the compatibility patches, contact YOKOGAWA.

Appendix 6.4 Cautionary Notes for a Revision Upgrade to R4.03.10

This section provides cautionary notes for a revision upgrade from R4.03 to R4.03.10. When you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.

IMPORTANT

Use the R6.02 or a later version of CENTUM VP when integrating ProSafe-RS with CENTUM VP.

In R4.01 or later, be sure to register the RS project in an AD project regardless of the engineering method.

SEE ALSO

For more information about cautionary notes when upgrading the revision to ProSafe-RS R4.03, refer to:

Appendix 6.3, “Cautionary Notes for Upgrading to R4.03” on page App.6-10

For more information about creating an AD project, refer to:

“■ Creating AD projects” in C1.2.1, “Creating and deleting AD projects” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects in an AD project, refer to:

C1.2.3, “Registering RS projects in the AD project” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Software Revisions

The respective software release number of R4.03.10 is as follows:

Software release number R4.03.10 (*1)

- SENG software release number: R4.03.10 (*1)
- SCS system program release number: R4.03.10 (*1)

*1: The last two digits of the revision number will be changed in accordance with the software revisions after the release of R4.03.10.

● Inter-SCS Safety Communication

The release number of the SCS system program of an SCS that performs Inter-SCS safety communication with SCS with system program version R4.03.10 must be R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be of R1.02 or later.

● Control Bus Drivers

The control bus drivers that are installed on the computer should be upgraded to the version supplied in R4.03.10.

■ Basic Procedure for Upgrading

To use the added or modified features, install the ProSafe-RS software R4.03.10 or later and open the existing SCS project.

Safety Communication I/O Editor

To use Safety Communication I/O Editor of AD Suite, you must perform "Procedure A" on an SENG of R4.03.10.

If I/O list engineering had been selected and subsystem communication had been defined with a version earlier than R4.03.10, from here on you must perform engineering by using Safety Communication I/O Editor. Use Communication I/O List Output Tool to create a safety communication I/O list.

SEE ALSO For more information about Operations of “Procedure A”, refer to:

“■ Procedure A: Opening SCS Projects” on page C4-18

For more information about how to create a safety communication I/O list, refer to:

“■ Communication I/O List Output Tool” in Appendix 3.4, “Major changes in R4” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Procedure for Using Added and Modified Features

The following functions that have been added or modified in R4.03.10 cannot be used in the basic upgrading procedures. After you have upgraded the SENG software to R4.03.10, offline download to the SCS and other operations are required. The procedures to use the respective functions are described below.

SEE ALSO For more information about details of the operation procedure introduced in each function, refer to:

C4.2.4, “Procedures for using new functions” on page C4-22

Fire and Gas Communication

To use fire and gas communication for connecting with wireless gas detectors, you must perform "Procedure C" on an SENG of R4.03.10. Fire and gas communication can be used with S2SC70 only.

Expanding the Number of Data Allocated for Subsystem Communication

With subsystem communication, to expand the number of data that can be allocated to an instance of a subsystem communication FB, you must perform "Procedure C" on an SENG of R4.03.10.

Cautionary Notes for Upgrading When ALE111 is Used

You must be careful when upgrading the system if ALE111 is used for Modbus slave or DNP3 communication.

SEE ALSO For more information about the precautions when upgrading a system where ALE111 is used for Modbus slave or DNP3 communication, refer to:

“■ Cautionary Notes for Upgrading When ALE111 is Used” on page App.6-5

Appendix 6.5 Cautionary Notes for Revision Upgrade to R4.04

This section provides cautionary notes for revision upgrade from R4.03.10 to R4.04. When you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.

In R4.01 or later, be sure to register the RS project in an AD project regardless of the engineering method used.

SEE ALSO For more information about creating an AD project, refer to:

"■ Creating AD projects" in C1.2.1, "Creating and deleting AD projects" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects in an AD project, refer to:

C1.2.3, "Registering RS projects in the AD project" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about cautionary notes when upgrading the revision to ProSafe-RS R4.03.10, refer to:

Appendix 6.4, "Cautionary Notes for a Revision Upgrade to R4.03.10" on page App.6-13

For more information about settings after upgrading software, refer to:

C4.2.4, "Procedures for using new functions" on page C4-22

■ Software Revisions

The respective software release numbers of R4.04 are as follows:

Software release number R4.04.xx (*1)

- SENG software release number: R4.04.xx (*1)
- SCS system program release number: R4.04.xx (*1)

*1: The last two digits of the revision number will be changed in accordance with the software revisions after the release of R4.04.00.

The database revision of an SCS project that is created by SENG with software release number R4.04.xx will be R4.03.10.

● Inter-SCS Safety Communication

The release number of the SCS system program of an SCS that performs Inter-SCS safety communication with SCS with system program version R4.04 must be R1.01.30 or later.

If Vnet/IP is used in the route of the inter-SCS safety communication, the system programs on the SCSs must be of R1.02 or later.

● Control Bus Drivers

The control bus drivers that are installed on the computer should be upgraded to the version supplied in R4.04.

■ Basic Procedure for Upgrading

To use the added or modified features, install the ProSafe-RS software R4.04 or later and open the existing SCS project.

SEE ALSO For more information about settings after upgrading software, refer to:

C4.2.4, "Procedures for using new functions" on page C4-22

Changing the Setting Range of IOP Lower Limit Detection Level

To change the setting range of the IOP lower limit detection level and transmitter error lower limit detection level for AI channels, you must follow “Procedure A” by using SENG of R4.04. This feature is applicable to the AI channels of SAI143-H style 3 or later and S2MMM843.

Functional Improvement of AD Organizer

To use the improved method for starting SCS Manager from AD Organizer and to use the read-only mode of the Safety I/O Editor and the Safety Communication I/O Editor, you must follow “Procedure A” by using SENG of R4.04.

Cautionary Notes for Upgrading When ALE111 is Used

You must be careful when upgrading the system if ALE111 is used for Modbus slave or DNP3 communication.

SEE ALSO

For more information about the precautions when upgrading a system where ALE111 is used for Modbus slave or DNP3 communication, refer to:

“■ Cautionary Notes for Upgrading When ALE111 is Used” on page App.6-5

Appendix 6.6 Cautionary Notes for Revision Upgrade to R4.05

This section provides cautionary notes for revision upgrade from R4.04 to R4.05. When you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.

In R4.01 or later, be sure to register the RS project in an AD project regardless of the engineering method used.

SEE ALSO

For more information about creating an AD project, refer to:

"■ Creating AD projects" in C1.2.1, "Creating and deleting AD projects" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects in an AD project, refer to:

C1.2.3, "Registering RS projects in the AD project" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about cautionary notes when upgrading the revision to ProSafe-RS R4.04, refer to:

Appendix 6.5, "Cautionary Notes for Revision Upgrade to R4.04" on page App.6-15

For more information about the detailed operation procedure required after the revision upgrade, refer to:

C4.2.4, "Procedures for using new functions" on page C4-22

■ Software Revisions

The respective software release numbers of R4.05 are as follows:

Software release number R4.05.xx (*1)

- SENG software release number: R4.05.xx (*1)
- SCS system program release number: R4.05.xx (*1)

*1: The last two digits of the revision number will be changed in accordance with the software revisions after the release of R4.05.00.

The database revision of an SCS project that is created by SENG with software release number R4.05.xx will be R4.05.00.

● Inter-SCS Safety Communication

The release number of the SCS system program of an SCS that performs Inter-SCS safety communication with SCS with system program version R4.05 must be R1.01.30 or later.

If Vnet/IP is used in the route of the inter-SCS safety communication, the system programs on the SCSs must be of R1.02 or later.

● Control Bus Drivers

The control bus drivers that are installed on the computer should be upgraded to the version supplied in R4.05.

■ Cautionary notes on License Management Software in which its vulnerability is resolved

In ProSafe-RS R4.05.00, the vulnerability of License Management Software has been resolved. Therefore, if you use a computer in which ProSafe-RS R4.05.00 or later is installed as a license management station and you want to distribute licenses and distribute master licenses from it, you can distribute only to the license-assigned stations in which the vulnerability is resolved.

The following table shows the products and their revision numbers in which the vulnerability is resolved.

Table Appendix 6.6-1 The revision number of products in which the vulnerability is resolved

Product	Revision number
CENTUM VP	R6.07.00 or later
ProSafe-RS	R4.05.00 or later
PRM	R4.03.00 or later

Cautionary notes on a mixture of vulnerability-resolved computers and vulnerability-unresolved computers

- You cannot distribute licenses or distribute master licenses through network if there is a mixture of vulnerability-resolved computers and vulnerability-unresolved computers in a license project.
- If there is a mixture of vulnerability-resolved computers and vulnerability-unresolved computers in a license project, contact YOKOGAWA.

Basic Procedure for Upgrading

To use the added or modified features, install the ProSafe-RS software R4.05 or later and open the existing SCS project.

SEE ALSO For more information about Operations of “Procedure A”, refer to:

“■ Procedure A: Opening SCS Projects” on page C4-18

Safety I/O Parameter Profile of AD Suite

To use the safety I/O parameter profile of AD Suite, you must perform "Procedure A" on an SENG of R4.05.

Improved AD Suite Functions

To use the following improved AD Suite functions, you must perform "Procedure A" on an SENG of R4.05.

- Improved workflow of AD Suite and iDefine
  This functional improvement is available when collaborating with iDefine 1.16.5 or later.
- Improved Safety I/O Editor, IOM Definition Editor, and System Structure Navigator

Improved Logic Simulation Test Function

To use the improved logic simulation test function, you must perform "Procedure A" on an SENG of R4.05. This functional improvement is available when collaborating with iDefine 1.16.5 or later. However, it is not available with SCSV1.

Procedure for Using Added and Modified Features

The basic upgrading procedures are not enough to use the following functions that have been added or modified in R4.05. After you have upgraded the SENG software to R4.05, offline download to the SCS and other operations are required. The procedures to use the respective functions are described below.

SEE ALSO For more information about details of the operation procedure introduced in each function, refer to:

C4.2.4, “Procedures for using new functions” on page C4-22

Skipping the Password Dialog Box for Manual Operation FBs

To use the function to skip the Password dialog box for manual operation FBs, you must perform "Procedure F" on an SENG of R4.05. This function is not available with SCSU1 and SCSV1.

When using this function, configure the parameter on the SCS Constants Builder after upgrading to R4.05, and then offline download the project. Thereafter, you can change the parameter by online change download. This function does not work when used in combination with HIS of CENTUM VP before R6.07.

Forced I/O Viewer Function

To use the Forced I/O Viewer function, you must perform "Procedure B" on an SENG of R4.05. This function is not available with SCSV1.

Support of the CPU Module S2CP471

To use the CPU module S2CP471, you must perform "Procedure B" on an SENG of R4.05. S2CP471 can be used in SSC60 and S2SC70.

Notes When Aliases are Defined for User-defined Columns in AD Organizer

This section describes the behavior when the system is upgraded if an alias of a user-defined column already defined is identical to the name of a standard column such as “Typical” that has been added to the Safety I/O Editor and Safety Communication I/O Editor in R4.05. It also describes the data migration procedure required in such a case.

SEE ALSO For more information about details of the data migration procedure required on iDefine after the upgrade, refer to:

iDefine User Guide (PR03076-MAN-970_01)

Column Names After the Upgrade

If an alias of a user-defined column already defined is identical to the name of a newly added standard column, the alias name of the user-defined column is changed during the upgrade. An underscore “_” is added to the beginning of the original alias name.

(Example) When the alias name is Typical

After upgraded to R4.05, the alias name becomes “_Typical”.

Migrating the Data of the Duplicate Column

The data of the original user-defined column remains after the upgrade. You can use a grid rule to migrate the data to a new standard column. In the Grid Rule Editor, create a grid rule for data copying.

For example, to copy the data of the _Typical column to the Typical column, configure the settings in the Define Rule window as follows:

- Select [Set] for Rule Type and [Typical] for Target Column.
- Set nothing in the Condition section.
- In the Action section, select [Column Name] for the operand type and set [_Typical] as the name of the column to be operated.

By running the created rule, the data of the _Typical column is copied to the Typical column. Confirm the result, and delete the data of the _Typical column.

Cautionary Notes for Upgrading When ALE111 is Used

You must be careful when upgrading the system if ALE111 is used for Modbus slave or DNP3 communication.

SEE ALSO For more information about the precautions when upgrading a system where ALE111 is used for Modbus slave or DNP3 communication, refer to:

"■ Cautionary Notes for Upgrading When ALE111 is Used" on page App.6-5

Appendix 6.7 Cautionary notes for upgrading to R4.06

This section provides cautionary notes and actions required for a revision upgrade from R4.05 to R4.06. When you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.

IMPORTANT

When integrating ProSafe-RS with CENTUM VP, use the R6.08 or a later version of CENTUM VP for the installation on the same computer.

In R4.01 or later, be sure to register the RS project in an AD project regardless of the engineering method.

SEE ALSO

For more information about creating an AD project, refer to:

"■ Creating AD projects" in C1.2.1, "Creating and deleting AD projects" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects in an AD project, refer to:

C1.2.3, "Registering RS projects in the AD project" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about cautionary notes when upgrading the revision to ProSafe-RS R4.05, refer to:

Appendix 6.6, "Cautionary Notes for Revision Upgrade to R4.05" on page App.6-17

For more information about the detailed operation procedure required after the revision upgrade, refer to:

C4.2.4, "Procedures for using new functions" on page C4-22

■ Software revisions

The respective software release numbers of R4.06 are as follows:

Software release number R4.06.xx (*1)

- SENG software release number: R4.06.xx(*1)
- SCS system program release number: R4.06.xx (*1)

*1: The last two digits of the revision number will be changed in accordance with the software revisions after the release of R4.06.00.

The database revision of an SCS project that is created by SENG with software release number R4.06.xx will be R4.06.00.

● Control bus drivers

The control bus drivers that are installed on the computer must be upgraded to the version supplied in R4.06.

■ Basic procedure for upgrading

To use the added or modified features, install the ProSafe-RS software R4.06 or later and open the existing SCS projects ("Procedure A").

SEE ALSO

For more information about Operations of "Procedure A", refer to:

"■ Procedure A: Opening SCS Projects" on page C4-18

Support of displaying the list of AD Suite work files

To use the displayed list of AD Suite work files, you must perform “Procedure A” on an SENG of R4.06.

Improved AD Suite functions

To use the following improved AD Suite functions, you must perform “Procedure A” on an SENG of R4.06.

- Improved grid rule function
- Improved revision history function
- Improved functions of Safety I/O Editor, Safety Communication I/O Editor, Safety I/O Parameter Profile Editor, and IOM Definition Editor

POU password

In iDefine 1.16.6 or later, you can set a password for POU. To refer to POU with SCS Manager by using the POU password set in iDefine, you must perform “Procedure A” on SENG of R4.06.

Procedures for using added and modified features

The basic upgrading procedures are not enough to use the following features that have been added or modified in R4.06. After you upgrade the SENG software to R4.06, you must perform offline download to the SCS and other operations. The following procedures are required to use the new features.

SEE ALSO For more information about operation “Procedure B” to “Procedure F” for using new functions, refer to:

C4.2.4, “Procedures for using new functions” on page C4-22

SCS supporting SIL2 (LISC70)

To use the SCS supporting SIL2 (LISC70), you must perform “Procedure C” on an SENG of R4.06.

Added system functions and function block

To use the system functions (NUMBITS_8/NUMBITS_16) and the system function block (SYS_CH_OUTEN) added in R4.06, you need to perform “Procedure C” on an SENG of R4.06. NUMBITS_8/NUMBITS_16 and SYS_CH_OUTEN cannot be used on SSC10 and SSC60.

Steps when an SCS project is already placed on another computer such as a file server

If an SCS project is already placed on a file server PC that is different from the SENG PC, files in the SCS project database may be corrupted while the SCS project is operated on the SENG PC. When an SCS project is already placed on a PC such as a file server which is different from the SENG PC that operates the SCS project, make sure to implement the avoidance described in SEE ALSO to prevent file corruption in the SCS project database.

SEE ALSO For more information about avoidance, refer to:

“■ Precautions when Placing the SCS Project on Another PC such as a File Server” in 1.2, “Engineering” in ProSafe-RS Release Information (IM 32P01A50-01EN)

Cautionary notes for upgrading when ALE111 is used

You must be careful when upgrading the system if ALE111 is used for Modbus slave or DNP3 communication.

SEE ALSO For more information about the precautions when upgrading a system where ALE111 is used for Modbus slave or DNP3 communication, refer to:

"■ Cautionary Notes for Upgrading When ALE111 is Used" on page App.6-5

Appendix 6.8 Cautionary notes for upgrading to R4.07

This section provides cautionary notes and actions required for a revision upgrade from R4.06 to R4.07. When you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.

IMPORTANT

When integrating ProSafe-RS with CENTUM VP, use the R6.08 or a later version of CENTUM VP for the installation on the same computer.

In R4.01 or later, be sure to register the RS project in an AD project regardless of the engineering method.

SEE ALSO

For more information about creating an AD project, refer to:

"■ Creating AD projects" in C1.2.1, "Creating and deleting AD projects" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects in an AD project, refer to:

C1.2.3, "Registering RS projects in the AD project" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about cautionary notes when upgrading the revision to ProSafe-RS R4.06, refer to:

Appendix 6.7, "Cautionary notes for upgrading to R4.06" on page App.6-21

For more information about the detailed operation procedure required after the revision upgrade, refer to:

C4.2.4, "Procedures for using new functions" on page C4-22

■ Software revisions

The respective software release numbers of R4.07 are as follows:

Software release number R4.07.xx (*1)

- SENG software release number: R4.07.xx (*1)
- SCS system program release number: R4.07.xx (*1)

*1: The last two digits of the revision number will be changed in accordance with the software revisions after the release of R4.07.00.

The database revision of an SCS project that is created by SENG with software release number R4.07.xx will be R4.07.00.

● Control bus drivers

The control bus drivers that are installed on the computer must be upgraded to the version supplied in R4.07.

■ Basic procedure for upgrading

To use the added or modified features, install the ProSafe-RS software R4.07 or later and open the existing SCS projects ("Procedure A").

SEE ALSO

For more information about Operations of "Procedure A", refer to:

"■ Procedure A: Opening SCS Projects" on page C4-18

Procedures for using added and modified features

The basic upgrading procedures are not enough to use the following features that have been added or modified in R4.07. After you upgrade the SENG software to R4.07, you must perform offline download to the SCS and other operations. The following procedures are required to use the new features.

SEE ALSO For more information about operation “Procedure B” to “Procedure F” for using new functions, refer to:

C4.2.4, “Procedures for using new functions” on page C4-22

Making POWE/LOGE a Safety Function

To use the POWE/LOGE as a safety function, you must perform “Procedure C” on an SENG of R4.07. In new SCS projects created with R4.07.00 or later, POWE/LOGE is treated as a safety function.

Steps when an SCS project is already placed on another computer such as a file server

If an SCS project is already placed on a file server PC that is different from the SENG PC, files in the SCS project database may be corrupted while the SCS project is operated on the SENG PC. When an SCS project is already placed on a PC such as a file server which is different from the SENG PC that operates the SCS project, make sure to implement the avoidance described in SEE ALSO to prevent file corruption in the SCS project database.

SEE ALSO For more information about avoidance, refer to:

“■ Precautions when Placing the SCS Project on Another PC such as a File Server” in 1.2, “Engineering” in ProSafe-RS Release Information (IM 32P01A50-01EN)

Cautionary notes for upgrading when ALE111 is used

You must be careful when upgrading the system if ALE111 is used for Modbus slave or DNP3 communication.

SEE ALSO For more information about the precautions when upgrading a system where ALE111 is used for Modbus slave or DNP3 communication, refer to:

“■ Cautionary Notes for Upgrading When ALE111 is Used” on page App.6-5

Appendix 6.9 Cautionary notes for upgrading to R4.08

This section provides cautionary notes and actions required for a revision upgrade from R4.07 to R4.08. When you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.

IMPORTANT

When integrating ProSafe-RS with CENTUM VP, use the R6.10 or a later version(*1) of CENTUM VP for the installation on the same computer.

*1: CENTUM VP R6.09 with CENTUM VP R6.09.04 applied can also be used.

In R4.01 or later, be sure to register the RS project in an AD project regardless of the engineering method used.

SEE ALSO

For more information about creating an AD project, refer to:

"■ Creating AD projects" in C1.2.1, "Creating and deleting AD projects" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects in an AD project, refer to:

C1.2.3, "Registering RS projects in the AD project" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about cautionary notes when upgrading the revision to ProSafe-RS R4.07, refer to:

Appendix 6.8, "Cautionary notes for upgrading to R4.07" on page App.6-24

For more information about the detailed operation procedure required after the revision upgrade, refer to:

C4.2.4, "Procedures for using new functions" on page C4-22

■ Software revisions

The respective software release numbers of R4.08 are as follows:

Software release number R4.08.xx (*1)

- SENG software release number: R4.08.xx (*1)
- SCS system program release number: R4.08.xx (*1)

*1: The last two digits of the revision number will be changed in accordance with the software revisions after the release of R4.08.00.

The database revision of an SCS project that is created by SENG with software release number R4.08.xx will be R4.08.00.

● Control bus drivers

The control bus drivers that are installed on the computer must be upgraded to the version supplied in R4.08.

■ Basic procedure for upgrading

To use the added or modified features, install the ProSafe-RS software R4.08 or later and open the existing SCS projects ("Procedure A").

SEE ALSO For more information about Operations of “Procedure A”, refer to:

“■ Procedure A: Opening SCS Projects” on page C4-18

■ Procedures for using added and modified features

The basic upgrading procedures are not enough to use the following features that have been added or modified in R4.08. After you upgrade the SENG software to R4.08, you must perform offline download to the SCS and other operations. The following procedures are required to use the new features.

SEE ALSO For more information about operation “Procedure B” to “Procedure F” for using new functions, refer to:

C4.2.4, “Procedures for using new functions” on page C4-22

● Modbus device reference number expansion

To expand the reference numbers of Modbus devices, you must perform “Procedure C” on an SENG of R4.08. Modbus device reference numbers are expanded in SCS projects newly created in R4.08.00 or later. The applicable SCSs are SCSP1/SCSU1/SCSP3/SCSL2.

■ Steps when an SCS project is already placed on another computer such as a file server

If an SCS project is already placed on a file server PC that is different from the SENG PC, files in the SCS project database may be corrupted while the SCS project is operated on the SENG PC. When an SCS project is already placed on a PC such as a file server which is different from the SENG PC that operates the SCS project, make sure to implement the avoidance described in SEE ALSO to prevent file corruption in the SCS project database.

SEE ALSO For more information about avoidance, refer to:

“■ Precautions when Placing the SCS Project on Another PC such as a File Server” in 1.2, “Engineering” in ProSafe-RS Release Information (IM 32P01A50-01EN)

■ Cautionary notes for upgrading when ALE111 is used

You must be careful when upgrading the system if ALE111 is used for Modbus slave or DNP3 communication.

SEE ALSO For more information about the precautions when upgrading a system where ALE111 is used for Modbus slave or DNP3 communication, refer to:

“■ Cautionary Notes for Upgrading When ALE111 is Used” on page App.6-5

Appendix 6.10 Cautionary notes for upgrading to R4.09

This section provides cautionary notes and actions required for a revision upgrade from R4.08 to R4.09. When you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.

IMPORTANT

When integrating ProSafe-RS with CENTUM VP, use the R6.10 or a later version of CENTUM VP for the installation on the same computer.

In R4.01 or later, be sure to register the RS project in an AD project regardless of the engineering method.

SEE ALSO

For more information about creating an AD project, refer to:

"■ Creating AD projects" in C1.2.1, "Creating and deleting AD projects" in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about how to register RS projects in an AD project, refer to:

C1.2.3, "Registering RS projects in the AD project" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about cautionary notes when upgrading the revision to ProSafe-RS R4.08, refer to:

Appendix 6.9, "Cautionary notes for upgrading to R4.08" on page App.6-26

For more information about the detailed operation procedure required after the revision upgrade, refer to:

C4.2.4, "Procedures for using new functions" on page C4-22

■ Software revisions

The respective software release numbers of R4.09 are as follows:

Software release number R4.09.xx (*1)

- SENG software release number: R4.09.xx (*1)
- SCS system program release number: R4.09.xx (*1)

*1: The last two digits of the revision number will be changed in accordance with the software revisions after the release of R4.09.00.

The database revision of an SCS project that is created by SENG with software release number R4.09.xx will be R4.08.00.

● Control bus drivers

The control bus drivers that are installed on the computer must be upgraded to the version supplied in R4.09.

■ Basic procedure for upgrading

To use the added or modified features, install the ProSafe-RS software R4.09 or later and open the existing SCS projects ("Procedure A").

SEE ALSO

For more information about Operations of "Procedure A", refer to:

"■ Procedure A: Opening SCS Projects" on page C4-18

Procedures for using added and modified features

The basic upgrading procedures are not enough to use the following features that have been added or modified in R4.09. After you upgrade the SENG software to R4.09, you must perform offline download to the SCS and other operations. The following procedures are required to use the new features.

SEE ALSO For more information about operation “Procedure B” to “Procedure F” for using new functions, refer to:

C4.2.4, “Procedures for using new functions” on page C4-22

Improvement of POU online change function

To improve the POU online change function, you must perform “Procedure E” on an SENG of R4.09. For SCS projects newly created with SENG R4.09.00 or later, online change download is available when newly creating, deleting, or renaming all program, user-defined function, and user-defined function block POUs.

Steps when an SCS project is already placed on another computer such as a file server

If an SCS project is already placed on a file server PC that is different from the SENG PC, files in the SCS project database may be corrupted while the SCS project is operated on the SENG PC. When an SCS project is already placed on a PC such as a file server which is different from the SENG PC that operates the SCS project, make sure to implement the avoidance described in SEE ALSO to prevent file corruption in the SCS project database.

SEE ALSO For more information about avoidance, refer to:

“■ Precautions when Placing the SCS Project on Another PC such as a File Server” in 1.2, “Engineering” in ProSafe-RS Release Information (IM 32P01A50-01EN)

Cautionary notes for upgrading when ALE111 is used

You must be careful when upgrading the system if ALE111 is used for Modbus slave or DNP3 communication.

SEE ALSO For more information about the precautions when upgrading a system where ALE111 is used for Modbus slave or DNP3 communication, refer to:

“■ Cautionary Notes for Upgrading When ALE111 is Used” on page App.6-5

Revision Information

Title : Installation Guide

Manual No. : IM 32P01C50-01EN

Dec. 2023/11th Edition/R4.10 or later

B1.2	Added or deleted descriptions of Windows update programs.
B2.1, B2.2, B2.3, B3.2, B3.2.1, B3.2.2, B3.2.3, B3.3.2, B3.9.1, B3.9.2, B5.1, B6, C7.1	Added descriptions of supported OS, and deleted descriptions of unsupported OS.
B3.3.5, C7.2.1, C7.2.2	Deleted OS descriptions.
B3.5	Changed .NET Framework version.
C4.2.3	Added descriptions of upgrading to R4.10.
D1.1	Updated description of the information for connecting CENTUM VP and ProSafe-RS.

Jun. 2023/10th Edition/R4.09

B1.2	Updated descriptions of Windows update programs.
B3.5	Changed descriptions of redistributable package
C4.2.3	Added descriptions of upgrading to R4.09.
D1.1	Updated description of the information for connecting CENTUM VP and ProSafe-RS.
D1.2	Updated description of the information for connecting ProSafe-RS and iDefine.

Nov. 2022/9th Edition/R4.08

B1.2, B2.3, B3.2, B3.3, B5.1, B6	Added or updated descriptions of Windows update programs.
C4.2.3	Added descriptions of upgrading to R4.08.

Jan. 2022/8th Edition/R4.07

B1.2	Added descriptions for downloading Windows update for Windows Server 2019 and updated descriptions for downloading Windows update for Windows 10 Enterprise 2019 LTSC and Windows Server 2012 R2.
B2.1, B2.2, B2.3, B3.2.1, B3.2.2, B3.2.3, B3.3.5, B3.9.1, B5.1, B6, C7.2.2	Added descriptions of Windows Server 2019.
B2.3, B3.2, B5.1, B6	Added descriptions of installing Windows update programs.
B3.3.2	Added descriptions of the RIP Listener service.
B3.3.4	Updated descriptions about update programs in preparation.
B3.5, B3.6, B5, B6, C4	Added descriptions of password change.
C4.1	Added descriptions about linked domain management.

C4.1.1, C4.1.2	Added descriptions of version upgrade and revision upgrade during linked domain management operation.
C4.2.3	Added descriptions of upgrading to R4.07.
C7.1	Added descriptions of time zone cannot be changed (Windows Server 2019).

Feb. 2021/7th Edition/R4.06

A1, B2.1, B2.2, B2.3, B2.4, B3.2, B3.3, B3.9, B5.1, B6, C4.1, C7.2	Deleted descriptions of unsupported OS.
A2.2, B1.2, B2.1, B2.3, B2.5, B3.5, B3.6, B3.8, B4.5, B5.1, B5.2, B5.3, B6, C2	Added descriptions about linked domain management.
B1.2	Added or deleted descriptions about downloading Windows update programs.
B3.2.2, B3.9.2	Added descriptions of Windows 10 Enterprise 2019 LTSC.
B3.5, C4.1	Updated descriptions of redistributable modules.
C4.1, C4.2	Updated descriptions of actions after the installation for an upgrade or after upgrading ProSafe-RS software.
C4.2.3	Added descriptions of upgrading to R4.06.
D1	Updated the package code 0204 from FAST/TOOLS Integration Package to CI Server Integration Package.
D1.1	Added descriptions about linked domain management to the information for connecting CENTUM VP and ProSafe-RS.
D1.2	Updated descriptions of the information for connecting ProSafe-RS and iDefine, and added descriptions about linked domain management.
D1.3	Added descriptions about linked domain management to the information for connecting ProSafe-RS and PRM.

Apr. 2019/6th Edition/R4.05

Introduction	Updated description of registered trademarks and trademarks.
B1.2, B2.3, B3.2.3, B3.2.5, B3.3.3, B5.1	Updated descriptions of Windows update programs.
B1.2, B2.3, B3.6, B5.1	Updated descriptions of IT security.
B3.5, C4.1.1, C4.1.2	Updated descriptions of redistributable modules.
B3.6, B4.4	Added descriptions of the Forced I/O Viewer function.
C4.1.1, C4.1.2	Added descriptions of updating the Vnet/IP Interface Package.
C4.2	Updated descriptions due to the change in project database format.
C5	Added descriptions of updating to R4.05.
D1.1.5	Added information about connecting CENTUM VP and Forced I/O Viewer Package.
D1.2	Updated information for connecting ProSafe-RS and iDefine.
D1.3.2	Added information about connecting PRM Client and Forced I/O Viewer Package.

Aug. 2018/5th Edition/R4.04

Introduction	Updated description of registered trademarks of YOKOGAWA.

A2.2.2, A2.2.3, B1.3, B3.1, B3.3, B3.3.3, B3.4, C6.1.2, Appendix 3	Added descriptions about virtualization platform.
B1.2, B2.3, B3.2.3, B3.2.5, B5.1	Added descriptions of Windows update programs.
B2.1 to B2.3, B3.2.1, B3.2.4, B3.3.4, B3.9.1, B6, C8.2.1	Added descriptions of Windows Server 2016
B2.3, B3.5, B5.1	Changed descriptions of redistributable package
B2.3, B3.2.2, B3.2.4, B5.1	Added descriptions of disabling the Automatic cleanup task.
B3.2.2, B3.2.5, B3.5, B6	Deleted description of .NET Framework 3.5.1
B3.2.2, B3.2.4	Added descriptions of DCOM Settings
B3.5, C4.1	Added description of using iDefine interface package.
B3.9.2	Added descriptions about suppressing toast notification regarding Windows Firewall.
C4.1	Added procedure for upgrading the revision of products when two or more upgrade license support products are installed.
C4.1.1	Added the upgrading the version of ProSafe-RS software.
C4.1.2	Added the upgrading the revision of ProSafe-RS software.
C5	Added descriptions of upgrading to R4.04
D1.1	Updated description of the information for connecting CENTUM VP and ProSafe-RS.
D1.2	Updated description of the information for connecting ProSafe-RS and iDefine.

Oct. 2017/4th Edition/R4.03.10

B3.4	Deleted precautions when installing ProSafe-RS and CENTUM, or ProSafe-RS and PRM, on the same computer.
B4.1	Added descriptions of the Help files for PROFINET Configurator.
C4.1	Added descriptions of the upgrade license.
C4.2	Added descriptions of I/O list engineering.
C4.3	Added descriptions of how to start engineering after upgrading the ProSafe-RS software.
C5	Added descriptions of updating to R4.03.10.
C6.1	Added precautions for uninstallation when ProSafe-RS and CENTUM VP are installed on the same computer.

May 2017/3rd Edition/R4.03

Entire manual	Updated descriptions of the Start menu.
Introduction	Deleted Windows Vista from Trademark Acknowledgments.
B2	Updated descriptions of configuring the security settings on the domain controller
B3.2, B3.5, B3.8, C9.2	Deleted descriptions of Windows Vista and Windows Server 2008.

B3.2, B3.3, B3.4, B3.8, B6, C8.2, Appendix 4	Added descriptions of Windows 10
B3.3, C8.2	Updated descriptions of configuring network settings
B3.4, B5, B6, C4.1	Updated descriptions of security groups
B3.5, C8	Updated descriptions of IT security settings. Moved descriptions of the IT Security Tool and IT security-related maintenance to the Security Guide.
B6, C4.1, C4.3	Added descriptions of setting up Windows.
C5	Added descriptions of upgrading to R4.03
D1, D1.1	Updated descriptions of CENTUM VP and ProSafe-RS
D1.2	Updated descriptions of the connection information for ProSafe-RS and iDefine.
Appendix 5.2	Updated descriptions of cautionary notes for upgrading when ALE111 is used.

Oct. 2016/2nd Edition/R4.02

Entire manual	Changed the symbols that indicate warning and caution.
Introduction	Updated descriptions in "■ Safety, Protection, and Modification of the Product," "■ Symbols," and "■ Trademark Acknowledgments." Added a new term in "■ Full Names and Simplified Terms."
A1, A2.1	Added descriptions of iDefine.
B3.1	Updated descriptions of removing the Vnet/IP interface card.
C5	Added descriptions of upgrading to R4.02
C8.1.1	Added descriptions of a computer on which only AD Server is installed and a computer dedicated to license management.
D1, D1.2	Added information about connecting ProSafe-RS and iDefine.
D1.3	Updated descriptions of ProSafe-RS and PRM.
Appendix 4	Added descriptions of compatibility between revisions and cautionary notes for upgrading.

Dec. 2015/1st Edition/R4.01

Newly published.

■ For Questions and More Information Online Query: A query form is available on the following URL for online query. http://www.yokogawa.com/iss
■ Written by Yokogawa Electric Corporation
■ Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Attachment 9.5 License Management Guide
IM32P01C60-01EN

User's Manual

ProSafe-RS
ProSafe-RS Lite

License Management Guide

IM 32P01C60-01EN

YOKOGAWA
Yokogawa Electric Corporation

IM 32P01C60-01EN
8th Edition

Introduction

This manual describes how to manage licenses, which is a process required to activate and deactivate CENTUM VP and ProSafe-RS software packages.

Prerequisites for using this manual include completing the installation and preliminary configuration of the CENTUM VP and ProSafe-RS software packages.

This manual is structured as follows:

- Overview of license management
  Provides an overview of license management.
- Basic operations in license projects
  Describes the basic operations in managing licenses.
- Maintaining license projects
  Describes how to maintain a license project.
- Upgrading the Licenses from CENTUM VP R5 to R6, or from ProSafe-RS R3 to R4
  Describes how to update licenses when a product is upgraded.
- Working with upgrade licenses
  Describes how to operate the upgrade licenses.

8th Edition : Dec. 2023 (YK)
All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Safety Precautions for Use

Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Be sure to confirm the specifications and required settings of the devices that are used in combination with the Product by referring to the instruction manual or other documents of the devices.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:



Indicates that caution is required. This symbol for the Product indicates the possibility of dangers such as electric shock on personnel and equipment, and also indicates that the user must refer to the User's Manuals for necessary actions. In the User's Manuals, this symbol is used together with a word "CAUTION" or "WARNING" at the locations where precautions for avoiding dangers are described.

<French> Signale qu'il faut faire preuve de prudence. Ce symbole pour le produit signale la possibilité d'un danger pour le personnel et l'équipement comme un choc électrique, et signale également que l'utilisateur doit se référer au Manuel de l'utilisateur afin de prendre les mesures nécessaires. Dans le Manuel de l'utilisateur, ce symbole est utilisé conjointement avec la mention «CAUTION» ou «WARNING» aux endroits où sont décrites les précautions pour éviter les dangers.



Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.

<French> Signale qu'il faut faire preuve de prudence avec la surface brûlante. Les appareils sur lesquels est apposé ce symbole risquent de devenir brûlants. Tout contact physique ou matériel avec ces appareils risque de provoquer des brûlures ou des dommages.



Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.



Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.

~ Indicates an AC supply.

⎓ Indicates a DC supply.

| Indicates that a component such as a power supply switch is turned ON.

○ Indicates that a component such as a power supply switch is turned OFF.

Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

Warning and Disclaimer

- Except as specified in the warranty terms, YOKOGAWA shall not provide any warranty for the Product.
- YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Product.

Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the Software Product's merchantability or suitability for any particular purpose, except as specified in the warranty terms.
- Purchase the appropriate number of licenses of the Software Product according to the number of computers to be used.
- No copy of the Software Product may be made for any purpose other than backup; otherwise, it is deemed as an infringement of YOKOGAWA's Intellectual Property rights.
- Keep the software medium of the Software Product in a safe place.
- No reverse engineering, reverse compiling, reverse assembling, or converting the Software Product to human-readable format may be performed for the Software Product.
- No part of the Software Product may be transferred, converted, or sublet for use by any third-party, without prior written consent from YOKOGAWA.

Documentation Conventions

Symbols

The following symbols are used in the User's Manuals.

 WARNING	Indicates precautions to avoid a danger that may lead to death or severe injury.
 CAUTION	Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.
IMPORTANT	Indicates important information required to understand operations or functions.
TIP	Indicates additional information.
	Indicates referenced content. In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

Typographical Conventions

The following typographical conventions are used throughout the User's Manuals.

Commonly Used Conventions throughout the User's Manuals

- Δ Mark
  Indicates that a space must be entered between character strings.
  Example:

  ```
  .ALΔPIC010Δ-SC
  ```

- Character string enclosed by braces { }
  Indicates character strings that may be omitted.

  Example:

  ```
  .PRΔTAG{Δ.sheet name}
  ```

Conventions Used to Show Key or Button Operations

- Characters enclosed by brackets [ ]
  When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a button name in a window, or an item in a list box displayed in a window.

  Example:

  To alter the function, press the [ESC] key.

Conventions of a User-defined Folder

- User-defined folder name enclosed by parenthesis ( )
  User definable path is written in a pair of parentheses.

  Example:

  ```
  (RS Project Folder)\SCS0101
  ```

If the RS Project Folder is `C:\MYRSPJT`, the above path becomes `C:\MYRSPJTSCS0101`.

Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.
If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

Definitions of Node and Module Terms

In the User's Manuals, nodes and modules are referred to by using collective terms, another terms, or abbreviations based on the following definitions:

- Definitions of nodes
  - Node: A node is a collective term for an FIO node and an N-IO node.
  - FIO node: This is a collective term for a safety control unit, a safety node unit, and a unit for optical ESB bus repeater module.
  - CPU node: This is another term for a safety control unit. The abbreviation of safety control unit is SCU.
  - I/O node: This is another term for a safety node unit. The abbreviation of safety node unit is SNU.
  - N-IO node: This is a collective term for a node interface unit and an N-IO I/O unit. The abbreviation of node interface unit is NIU.
- Definitions of modules
  - I/O module: This is a collective term for an FIO I/O module and an N-IO I/O module.
  - FIO I/O module: This is a collective term for an analog I/O module and a digital I/O module for FIO, and a communication module.
  - N-IO I/O module: This is a collective term for the modules that can be mounted on an N-IO I/O unit.
  - AIO/DIO module: This is a collective term for an analog I/O module, a digital I/O module, and a universal type I/O module.
  - Analog I/O module: This is a collective term for an analog input module and an analog output module.
  - Digital I/O module: This is a collective term for a digital input module and a digital output module.
  - Universal type I/O module: This is a collective term for the I/O modules for which the channel signal category can be changed by software.

- Input module: This is a collective term for an analog input module, digital input module, and a universal type I/O module with defined input channels.
- Output module: This is a collective term for an analog output module, digital output module, and a universal type I/O module with defined output channels.
- Communication module: This is a collective term for a serial communication module, an Ethernet communication module, and a fire and gas communication module.

Full Names and Simplified Terms

In the User's Manuals, simplified terms listed in the following table are used.

Table Info-1 Full Names and Simplified Terms

Full Name	Simplified Term
Automation Design Suite	AD Suite
Automation Design Organizer	AD Organizer
Automation Design Server	AD Server
Automation Design project	AD project
Automation Design Master Database	ADMDB
Automation Design Suite Administration Tool	ADS Administration Tool
iDefine for ProSafe-RS	iDefine
Modification Package	ModPack
SCSV1-S (SCS supporting the SSC10S/SSC10D safety control units)	SCSV1
SCSP1-S (SCS supporting the SSC50S/SSC50D safety control units)	SCSP1
SCSP2-S (SCS supporting the SSC60S/SSC60D safety control units)	SCSP2
SCSP3-S (SCS supporting the S2SC70S/S2SC70D safety control units)	SCSP3
SCSL2-S (SCS supporting the L1SC70S/L1SC70D safety control units)	SCSL2
SCSU1-S (SCS supporting the SSC57S/SSC57D safety control units)	SCSU1

Copyright and Trademark Notices

All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, PRM, Exaopc, FieldMate Validator, and STARDOM are registered trademarks or trademarks of Yokogawa Electric Corporation.
- The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

License Management Guide

IM 32P01C60-01EN 8th Edition

CONTENTS

1. Overview of license management 1-1
   - 1.1 License management 1-2
     - 1.1.1 License management targets 1-4
     - 1.1.2 How license management works 1-6
     - 1.1.3 Overview of license management process 1-10
   - 1.2 License Manager 1-12
     - 1.2.1 License Manager function 1-13
     - 1.2.2 User privileges in License Manager 1-14
     - 1.2.3 Starting and exiting License Manager and working with the operation modes 1-15
     - 1.2.4 Window Structures of License Manager 1-18
2. Basic operations in license projects 2-1
   - 2.1 Process for managing licenses for the first time 2-2
   - 2.2 Creating, switching, and deleting license projects 2-4
   - 2.3 Reading a license 2-6
   - 2.4 Defining stations to which licenses need to be assigned 2-7
   - 2.5 Assigning licenses to license-assigned stations 2-11
   - 2.6 Checking license assignment consistency 2-12
   - 2.7 Distributing and accepting licenses through a network 2-13
   - 2.8 Distributing and accepting licenses using external storage media 2-16
   - 2.9 Monitoring the status of assigned licenses 2-18
   - 2.10 Saving license projects 2-19
   - 2.11 Managing licenses of a computer switchover type UGS 2-20
   - 2.12 Managing licenses of a network switchover type redundant UGS 2-22
3. Maintaining license projects 3-1
   - 3.1 Reading additional licenses on a license management station 3-2
   - 3.2 Modifying licenses 3-3
     - 3.2.1 Modifying license assignments 3-5
     - 3.2.2 Distributing modified licenses 3-7
     - 3.2.3 Accepting modified licenses 3-9
     - 3.2.4 Returning licenses using external storage media 3-11
   - 3.3 Adding and deleting license-assigned stations 3-12
   - 3.4 Redistributing licenses to license-assigned stations 3-14

3.4.1 Distributing and accepting master licenses through a network..... 3-15
3.4.2 Distributing and accepting master licenses using external storage media.....3-16
3.5 Increasing the software package capacity.....3-17
3.6 Backing up and restoring a license project..... 3-19
3.7 Moving licenses to other projects.....3-21
3.8 Changing the computer name of a license-assigned station.....3-25
3.9 Functions to help with license assignment work..... 3-26
3.9.1 Importing and exporting package lists.....3-27
3.9.2 Searching for characters in the license project window..... 3-31
3.9.3 Folding the display of a license project..... 3-32
3.9.4 Filtering information that appears in the license project window..... 3-33
3.9.5 Deleting software package licenses from a license project.....3-34
3.9.6 Creating an assigned licenses status file..... 3-35
4. Upgrading the Licenses from CENTUM VP R5 to R6, or from ProSafe-RS R3 to R4..... 4-1
4.1 Process for License Upgrading.....4-2
4.2 Upgrading the Licenses for Some HISs..... 4-5
5. Working with upgrade licenses.....5-1

License Management Guide

IM 32P01C60-01EN 8th Edition

CONTENTS

Appendix

Appendix 1. Items checked in the license assignment consistency check. App.1-1
Appendix 2. Displaying the status of assigned licenses on a license-assigned station..... App.2-1
Appendix 3. Messages..... App.3-1
Appendix 4. Upgrading licenses of CENTUM VP R5 software packages..... ..... App.4-1

1. Overview of license management

This section provides an overview of license management.

1.1 License management

This section provides an overview of license management and License Manager, which is a software used to manage licenses.

About license management

A license is the right to use a software package.

To activate a software package, allocate a license to every computer where the software package that you want to activate is installed. In addition, you can delete licenses for software packages that are no longer used on a specific computer. In this manual, these operations are referred to as activating and deactivating a software package.

License management is the process by which you determine which software package to use on which computer, distribute or delete licenses for each individual computer, and activate or deactivate the software packages.

The following table describes the license types.

Table 1.1-1 License types

Type	Description
Software license	License required to use the product software
Version upgrade license	License required to upgrade the version of the software license
Upgrade license	License required to apply the revisions when the product software is revised Types of upgrade licenses are as follows: • Upgrade license (revision up/patch) • Upgrade license (revision up) • Upgrade license (patch)

About License Manager

License Manager is the software program designed specifically to manage licenses.

License Manager is automatically installed when you install a product to be managed in license management on a computer. You can also install License Manager solely on a computer.

The following figure shows the License Manager window.

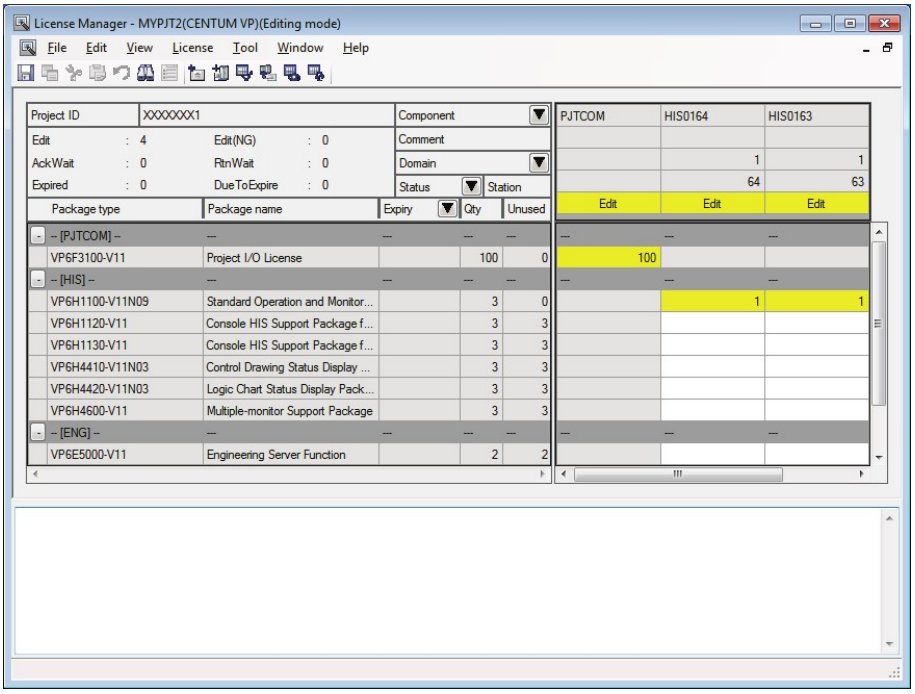


Figure 1.1-1 License Manager

SEE ALSO For more information about the products managed in license management, refer to:

"■ Products managed in license management" on page 1-4

1.1.1 License management targets

This section describes the products that are managed in license management and the scope for managing licenses.

Products managed in license management

License Manager manages the licenses of the following products:

- CENTUM VP R5.01 or later
- ProSafe-RS R3.01 or later
- PRM R4.01 or later

TIP

The software that is bundled with hardware is not managed in the license management. For example, the software bundled with Communication Gateway Unit (CGW) or Bus Converter (BCV) is not managed.

SEE ALSO

For more information about license management of PRM, refer to:

Plant Resource Manager License Management (IM 30B05A40-01EN)

License management of iDefine used for ProSafe-RS

License Manager does not manage the license of iDefine that is used in ProSafe-RS engineering.

SEE ALSO

For more information about license management for iDefine, refer to:

License User Guide (PR03076-MAN-971_02)

Scope of license management

A project that defines the license management targets is referred to as a license project. A license project manages the same scope specified by the project ID.

In ProSafe-RS, do not register SCS projects that belong to different license projects to the same RS project.

TIP

- CENTUM VP and ProSafe-RS are managed as two separate systems. For this reason, the license projects for CENTUM VP and ProSafe-RS are also managed separately.
- System engineering information is managed in projects, "VP project" of CENTUM VP and "RS project" and "SCS project" of ProSafe-RS, whereas system license information is managed in a license project.

Managing licenses for multiple systems

You can use License Manager on a single computer to manage license projects for multiple projects.

In addition, if you install License Managers for different products on a computer, you can manage licenses of multiple products by using their respective License Managers.

Different Version of License

A license can be distributed to the station if the license version and the software version that is installed in the station is identical.

For example, CENTUM VP R6 licenses are available to distribute only to the station that is installed with the CENTUM VP R6 software, not to the station that is installed with the CENTUM VP R5 software.

Similarly, CENTUM VP R5 licenses are available to distribute only to the station that is installed with the CENTUM VP R5 software, not to the station that is installed with the CENTUM VP R6 software.

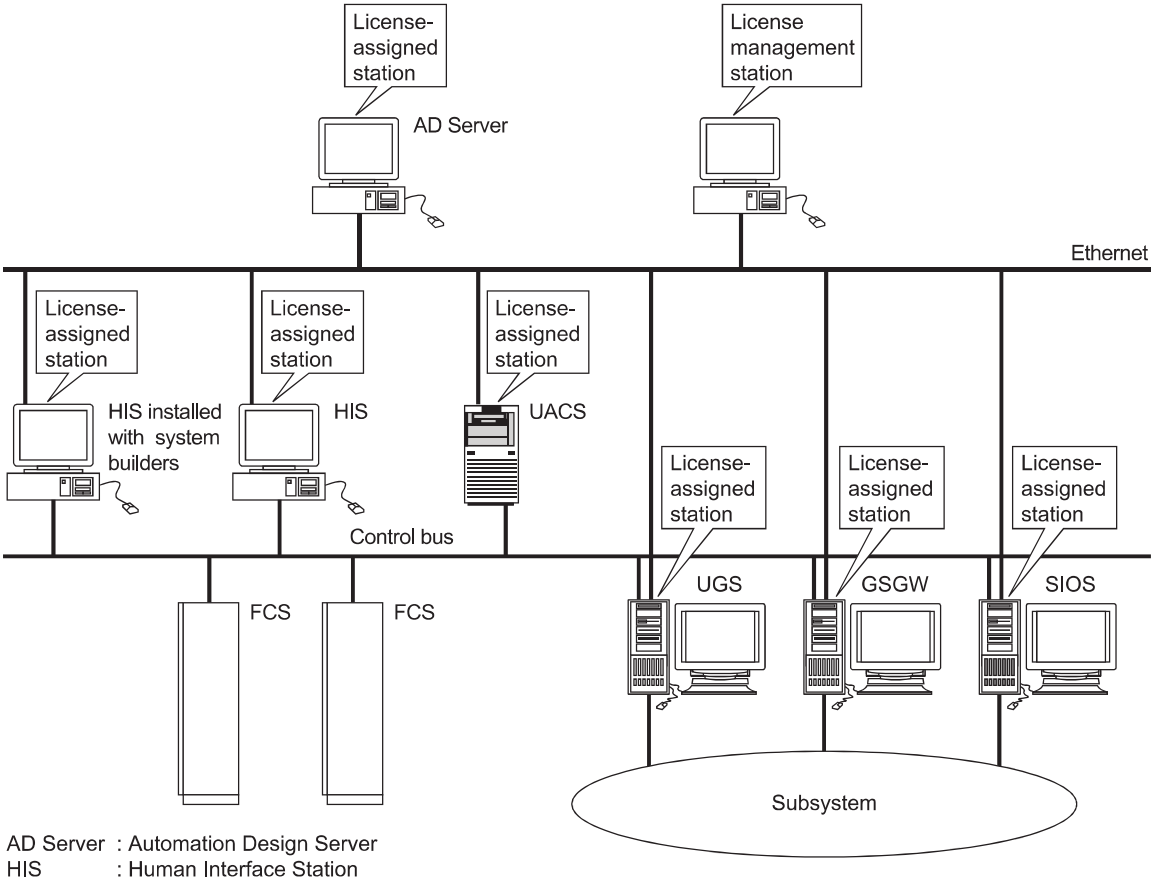
1.1.2 How license management works

This section describes the system configuration for license management and the process for managing licenses.

License management system configuration

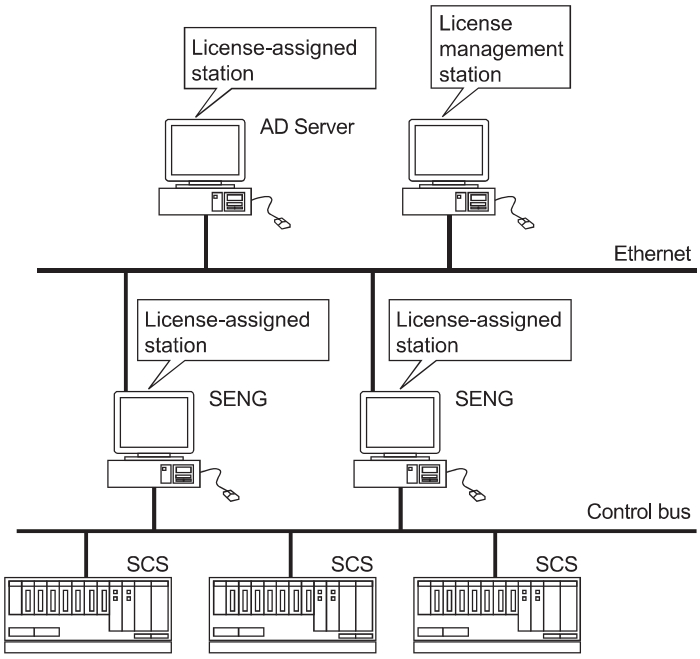
License Manager is installed on every computer where a license management target product is installed. You can use License Manager on one of these computers to manage licenses for the entire license project, and License Manager on the remaining computers to manage their own licenses.

A computer that manages licenses for one entire license project is called a license management station, while a computer whose licenses are being managed is called a license-assigned station.



AD Server : Automation Design Server
HIS : Human Interface Station
FCS : Field Control Station
UGS : Unified Gateway Station
GSGW : Generic Subsystem Gateway Station
SIOS : System Integration OPC Station
UACS : Unified Alarms & Conditions Server

Figure 1.1.2-1 Example of the license management system configuration for CENTUM VP



AD Server :Automation Design Server
SENG : Safety Engineering Station
SCS : Safety Control Station

Figure 1.1.2-2 Example of the license management system configuration for ProSafe-RS

TIP

As a general rule, to set up a license management station, you should use a computer where a license management target product is installed and is running 24 hours a day. You can also use a computer where only License Manager is installed.

Configuration for management of multiple projects by AD server

When multiple engineering projects are managed by using the AD server, a station that has a license of the Engineering Server Function is required to be included in one of license projects for engineering project. Avoid registering the station having the license of the Engineering Server Function for multiple license projects. Specifically, perform following instructions.

- When the AD server is the station that has only the Engineering Server Function
  Create a station that has only the Engineering Server Function in just one license project. Assign the license of the Engineering Server Function in the license project for which the station that has only the Engineering Server Function has been registered.
- When the AD server is the station that carries functions other than the Engineering Server Function
  Assign and distribute the license of the Engineering Server Function only in one license project.

The following figure shows that a station that has the AD server is defined in the license project (LPJT-A) for PJT-A and that the License Manager station in LPJT-A distributes the license of the Engineering Server Function.

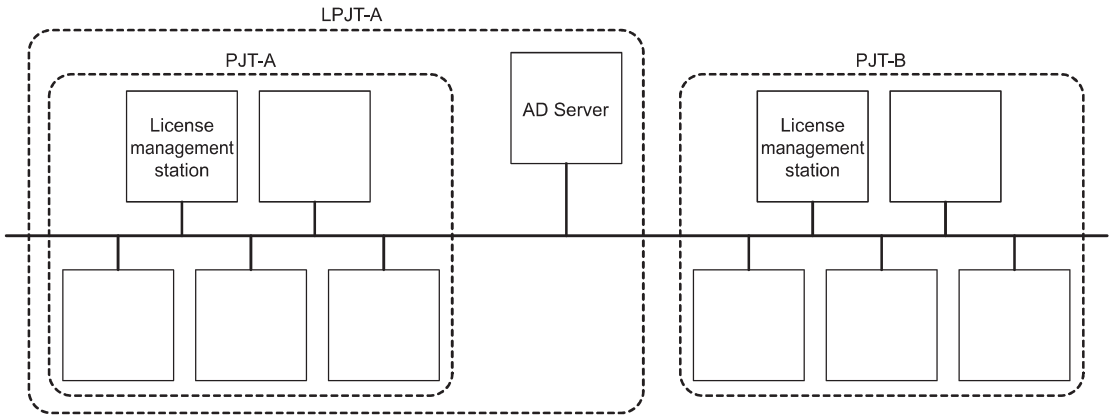


Figure 1.1.2-3 When AD server manages multiple projects

License management process

Yokogawa provides usage rights for purchased software packages in the form of license key files. License key files are stored on license media and supplied to users.

The license management station recognizes purchased licenses by reading the license key files from the license media.

After you assign licenses to each station, distribute the licenses to activate the software packages accordingly.

TIP

The license management station permits license update from CENTUM VP R5 to R6, and from ProSafe-RS R3 to R4.

Licenses are assigned to the following stations:

- License-assigned stations

  Licenses for the software packages installed on the license-assigned stations are assigned.

- License management station

  Licenses for the software packages installed on the license management station itself are assigned. (*1)

- FCS/SCS

  Are assigned licenses for the software used in FCS or SCS.

- PJTCOM

  PJTCOM is a virtual station in which the Project I/O License is assigned.

*1: The station with only License Manager installed is excluded.

TIP

Licenses for software that is bundled with hardware are not managed by License Manager.

After assigning licenses, distribute the licenses to the stations. At this point, the licenses that have been assigned to each station are distributed as follows:

- Licenses assigned to license-assigned stations

  Distributed from the license management station to the relevant license-assigned station.

- Licenses assigned to the license management station

  Distributed from the license management station to itself.

- Licenses assigned to an FCS or SCS

Licenses assigned to an FCS are distributed to the station installed with system builders, whereas licenses assigned to an SCS are distributed to SENG.

- Licenses assigned to PJTCOM

  In a CENTUM VP configuration, the licenses assigned to PJTCOM are distributed to the station installed with the system builders. In a ProSafe-RS configuration, they are distributed to the SENG.

After licenses have been distributed, activate the software packages by accepting the licenses on each station.

SEE ALSO For more information about PJTCOM, refer to:

"■ Station name and computer name default values" on page 2-9

1.1.3 Overview of license management process

This section describes the license management process when building a license project for the first time, and the tasks that need to be completed before and after the process.

IMPORTANT

Before performing the actual license management process, first prepare the information that is required for the process.

Tasks to be completed before starting license management

Before starting license management, you must perform the following tasks:

- Install the software package

  Install the software packages on all computers where you want to run the license management target product.

- Select the license management station

  If you want to use a computer as license management station only, install License Manager.

  In other cases, select a computer installed with license management target product as a license management station. License Manager is automatically installed on computer installed with license management target product.

TIP

To check license consistency for the entire system, it is recommended that you use a computer that is running continuously as the license management station. However, license-assigned stations and FCS/SCS stations continue to operate normally even if the license management station stops.

Building a license project for the first time

This section describes the license management process when building a license project for the first time.

License management includes tasks performed on the license management station and the license-assigned stations.

Tasks performed on a license management station

First, start License Manager on the license management station.

The tasks performed on a license management station are as follows:

1. Create new license projects
   Create a license project. When creating a license project, specify a name for the license project.
2. Read the license
   Read the license key file from the license media and register the available licenses. At this point, you need to enter the Project ID number.

IMPORTANT

- The license key file needs to be read by License Manager within the validity period printed on the license media. If the validity duration expires, you will not be able to read the license key file using License Manager. If the validity duration has expired, contact Yokogawa.
- You must retain the license key file even after expiration because it is used when restoring a license project.

3. Specify the stations
   Specify the stations whose licenses need to be managed.
4. Assign licenses to the stations
   Assign available licenses to each station.
5. Check license consistency
   Check that the basic software and options software have been combined correctly and that the licenses have been properly assigned.
6. Distribute licenses to stations
   Distribute licenses to the license-assigned stations through the network or by using external media.

Tasks performed on a license-assigned station

After you distribute licenses from the license management station to a license-assigned station, start License Manager on the license-assigned station.

Perform the following task:

- Accept the licenses
  Using License Manager, accept the licenses to activate the software packages.

TIP

When you distribute licenses for the first time, they are accepted automatically.
For the second and subsequent distributions, you need to perform the task to accept licenses.

IMPORTANT

You need to perform this task on all license-assigned stations. In addition, you also need to perform the same task for the license management station if you are assigning licenses to the station itself and activating its software package.

Tasks to be performed after licenses have been accepted

On the license management station and license-assigned stations, perform the procedures required for the individual packages that have been activated.

SEE ALSO

For more information about work required after activation, refer to:

B4., “Configuring the Functions Specific to SENG” in Installation Guide (IM 32P01C50-01EN)

1.2 License Manager

This section describes the functions, user privileges, operation, and window structures of License Manager.

1.2.1 License Manager function

This section describes the functions of License Manager on the license management station and license-assigned stations.

Functions of License Manager on a license management station

You can use the following functions of License Manager on a license management station:

- Manage licenses

  Create license projects and perform license management for the entire system, such as the assignment, distribution, and modification of licenses.

- Monitor the status of assigned licenses

  Monitor the status of assigned licenses for the entire system.

- Automatically back up license management information

  Automatically back up license management information to prepare for the possibility of a license management station failure.

- Redistribute licenses

  Redistribute licenses to a replacement license-assigned station if the original station fails.

- Accept licenses distributed to the local station

  Accept licenses that have been distributed to the license management station itself, and activate or deactivate the software packages.

Functions of License Manager on a license-assigned station

You can use the following functions of License Manager on a license-assigned station:

- Accept distributed licenses

  Accept licenses to activate or deactivate the software packages.

- Monitor distributed licenses

  Monitor licenses that have been distributed to the local station.

1.2.2 User privileges in License Manager

This section describes the user privileges in License Manager.

■ Privileges that entitle users to license management

The License Manager functions that you can use vary according to your user privileges. If you are part of a user group that has Administrator privileges, you can have maintenance privileges for License Manager. Only users with maintenance privileges can operate a license management station in Editing mode.

Table 1.2.2-1 User groups with maintenance privileges

Product name	User group	
	Legacy model(*1)	Standard model(*1)
CENTUM VP	Administrators	CTM_MAINTENANCE, CTM_MAINTENANCE_LCL
ProSafe-RS	Administrators	PSF_MAINTENANCE, PSF_MAINTENANCE_LCL

*1: This is the security model that is configured in IT security.

SEE ALSO For more information about Editing mode, refer to:

"■ Operation modes" on page 1-16

1.2.3 Starting and exiting License Manager and working with the operation modes

This section describes how to start and exit License Manager and the operation modes.

Starting License Manager

Start License Manager on the license management station or a license-assigned station.

License Manager window appears.

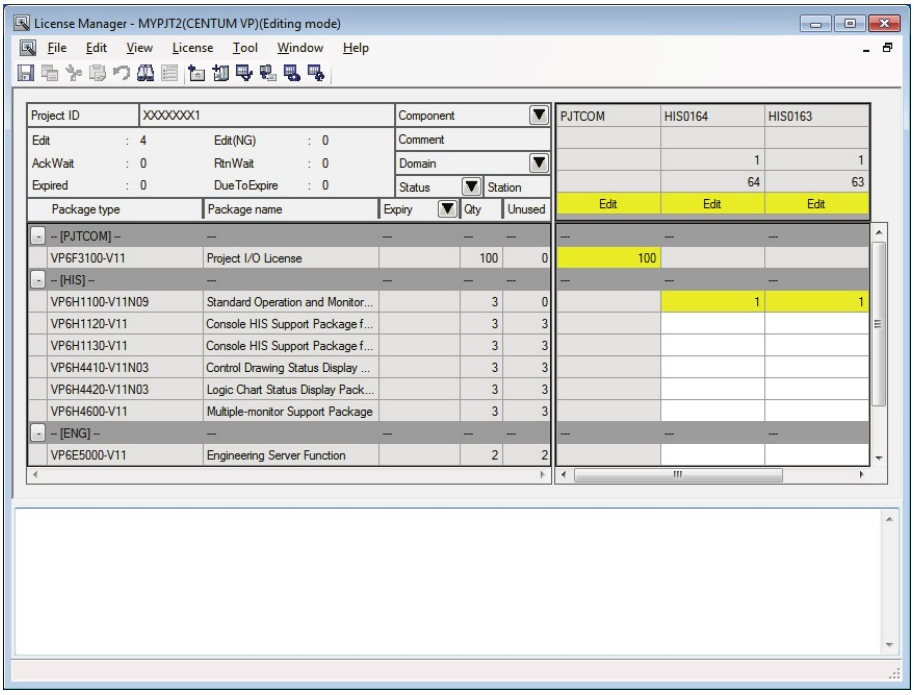


Figure 1.2.3-1 License Manager on the license management station

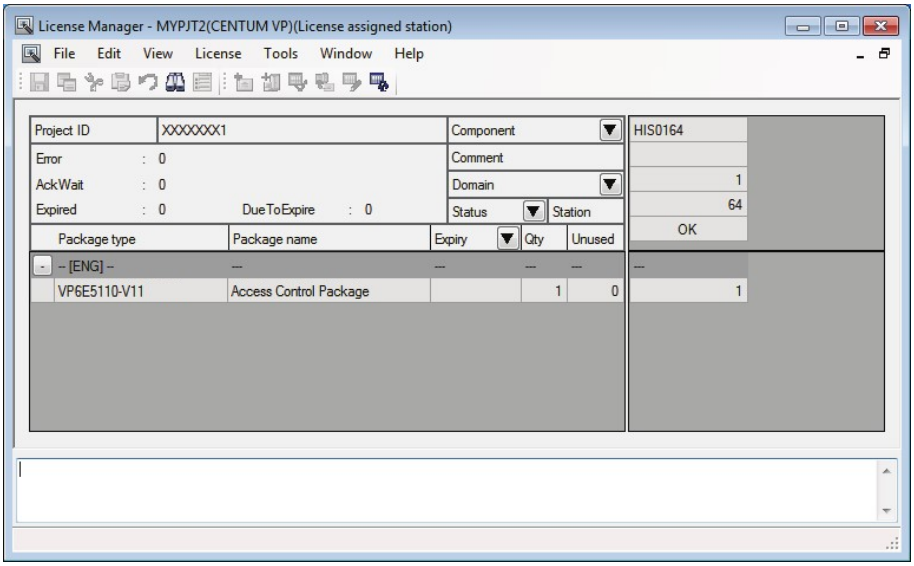


Figure 1.2.3-2 License Manager on a license-assigned station

TIP

When starting License Manager on the license management station from the second time onwards, a dialog box may appear to confirm whether you want to open data you were working with. The dialog box appears if you had closed License Manager after modifying the license assignments but without distributing them in the previous session. When this dialog box appears, click [Yes] to open the license project in the state where license assignments were being modified, but not distributed. Otherwise, click [No] to open the license project in the most recent status when licenses were distributed successfully.

Exiting License Manager

From the License Manager menu bar, select [File] > [Exit].

Operation modes

The functions that can be used in License Manager change according to the operation mode. The following table shows the functions that can be used in each License Manager operation mode:

Table 1.2.3-1 Operation modes in License Manager

Station	Operation mode	Functions
License-management station	Editing mode	Create a new license project Read licenses from the license media Define license management targets Assign licenses to license-assigned stations Distribute licenses to license-assigned stations Accept licenses distributed to its local station and activate or deactivate the installed software packages.
	Monitoring mode	Display the status of assigned licenses on license-assigned stations
License-assigned stations	Assigned station mode	Accept licenses distributed to local stations and activate or deactivate the installed software packages. Display the status of assigned licenses for its local stations

Switching operation modes

You can switch between the different operation modes of the license management station in the following ways:

Switching from Monitoring mode to Editing mode

From the License Manager menu bar, select [View] > [Editing mode].

Switching from Editing mode to Monitoring mode

From the License Manager menu bar, select [View] > [Monitoring mode].

Functions of License Manager and user privileges

The functions in License Manager that are available for use vary according to your user privileges.

Only users with maintenance privileges can operate a license management station in Editing mode.

The following table shows the License Manager functions available for the different stations and their operation modes:

Table 1.2.3-2 License Manager functions available for the different stations and their operation modes

Category	License Manager function	Station		
		Management station (Editing mode)	Management station (Monitoring mode)	Assigned station
Managing license information	Create a new license project	Yes	Yes (*1)	Yes (*1)
	Delete a license project	Yes	No	No
	Modify the properties of a license project	Yes	No	No
	Back up a license project	Yes	No	No
	Restore a license project	Yes	Yes (*1)	Yes (*1)
Defining the station configuration	Add a station	Yes	No	No
	Delete a station	Yes	No	No
	Modify station properties	Yes	No	No
Managing licenses	Add a license	Yes	No	No
	Move a license	Yes	No	No
	Delete a license	Yes	No	No
	Merge new installation licenses with upgrade installation licenses	Yes	No	No
	Upgrade a license	Yes	No	No
Editing license assignments	Assign a license	Yes	No	No
	Import a package list	Yes	No	No
	Export a package list	Yes	Yes	Yes (*2)
	Check consistency	Yes	No	No
	Export the status of license assignments that are being edited	Yes	No	No
Distributing and accepting licenses	Distribute a license (through the network)	Yes	No	No
	Distribute a master license (through the network) (*3)	Yes	No	No
	Accept a license (through the network)	Yes	Yes (*1)	Yes (*1)
	Distribute a license (using external media)	Yes	No	No
	Distribute a master license (using external storage media) (*3)	Yes	No	No
	Accept a license (using external media)	Yes	No	Yes (*1)
	Return a license (using external media)	Yes	No	No
Monitoring the license status	Monitor the status of assigned licenses	No	Yes	Yes (*2)
	Export the status of assigned licenses to a file	No	Yes	Yes (*2)
Other	Switch to Editing mode	No	Yes (*1)	No
	Switch to Monitoring mode	Yes	No	No

*1: Only available for users with maintenance privileges
*2: Only applicable for licenses distributed to that license-assigned station
*3: The Distribute Master licenses function redistributes assignment information that has already been distributed.

1.2.4 Window Structures of License Manager

This section describes the window structures of License Manager.

Main window

The following figure shows the names of the different parts of the License Manager main window.

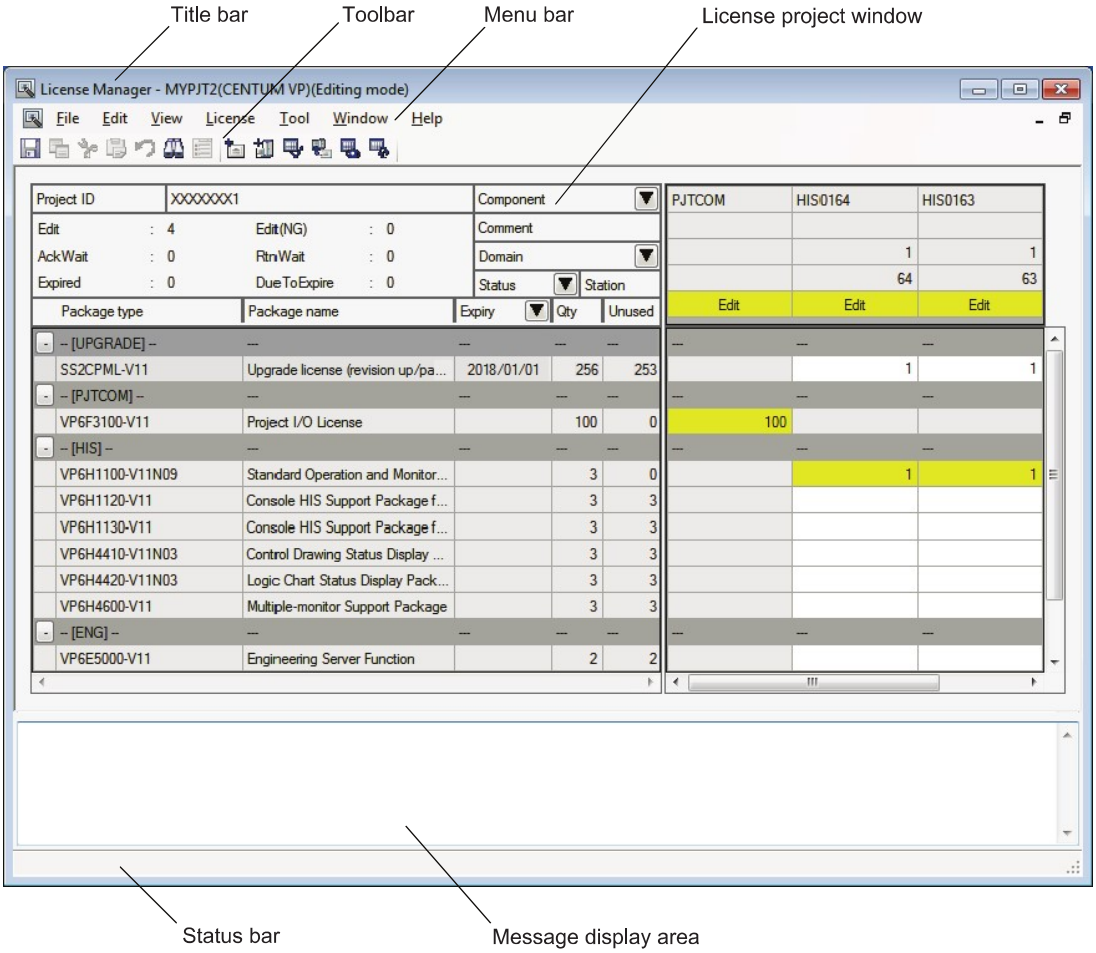


Figure 1.2.4-1 License Manager main window

License project window

The following figure shows the names of the different parts of the license project window.

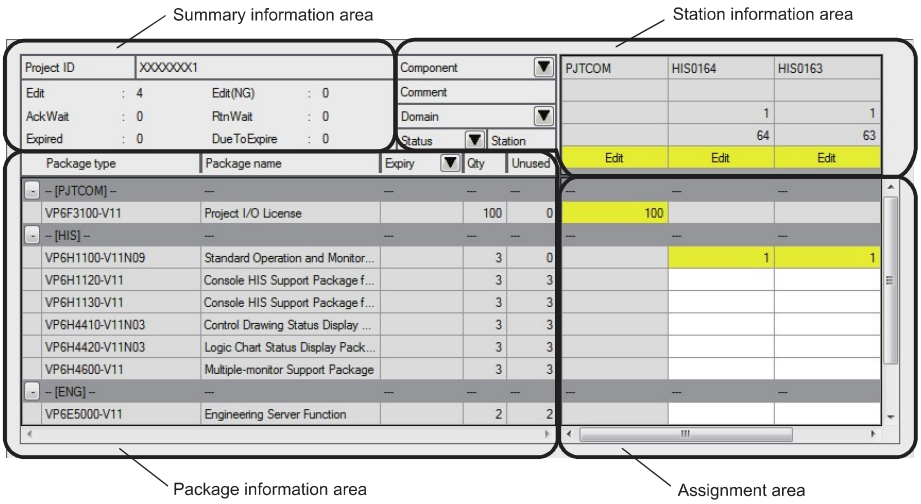


Figure 1.2.4-2 License project window

summary information area

The summary information area shows the Project ID and the status of assigned licenses for the entire license project.

In License Manager on the license management station, this area shows the status of assigned licenses for the entire license project. In License Manager on the license-assigned station, the area shows the status of licenses assigned to the local station.

The following items appear in the summary information area:

- Project ID
- Status display: The information displayed varies according to different operation modes, as shown in the following table.

Table 1.2.4-1 Status display details

Station	Status	Description	Status applicable for
License management station (Editing mode)	Edit	Number of stations with licenses that are being edited	Entire license project
	Edit(NG)	Number of stations that are diagnosed with errors in the consistency check	
	AckWait	Number of stations waiting for license acceptance	
	RtnWait	Number of stations waiting for a license to be returned	
	Expired	Number of stations with an expired license	
	DueToExpire	Number of stations with licenses that will expire within 30 days	
License management station (Monitoring mode)	Error	Number of stations with a license error	Entire license project
	Unknown	Number of stations for which the status cannot be confirmed due to a communication error	
	AckWait	Number of stations waiting for license acceptance	
	RtnWait	Number of stations waiting for deleted licenses to be returned using external media	
	Expired	Number of stations with an expired license	
	DueToExpire	Number of stations with licenses that will expire within 30 days	

Continues on the next page

Table 1.2.4-1 Status display details (Table continued)

Station	Status	Description	Status applicable for
License-assigned station	Error	License error	Local station
	Expired	Licenses have expired.	
	DueToExpire	Licenses will expire within 30 days.	
	AckWait	Waiting for license acceptance	

Package information area

The package information area shows the software packages with the licenses that are available for use.

In License Manager on the license management station, this area shows the managed software packages. In License Manager on the license-assigned station, this area shows the software packages that have been assigned a license on the local station.

The following table shows the definition items on the package information area. You can switch displaying or hiding the each definition item after you select View from the menu bar in the license manager.

Table 1.2.4-2 Definition items in the package information area

Item	Description	Default
Package type	The package model specification code for the license (example: VP6H1100-V10N03)	Displayed
Internal package type	CENTUM VP R5 package model specification code corresponding to the CENTUM VP R6 package model specification code, or ProSafe-RS R3 package model specification code corresponding to the ProSafe-RS R4 package model specification code (CENTUM VP example: LHS1100-V10/N0003) (*1)	Hidden
Package name	The package name for the license	Displayed
Paid	This item indicates whether the license is paid or free.	Hidden
Expiry	If the license has an expiry date, the expiry date appears. For software licenses, the software package is available until the expiry date. For upgrade licenses, you can install the product revisions or patches that were issued before the expiry date.	Displayed
Ver.	The version number of the license This item is left blank for upgrade licenses.	Hidden
Qty	The quantity of the license This item is fixed to 256 for upgrade licenses.	Always displayed
Unused	The number of licenses not assigned to any station	Always displayed

*1: The internal package model can be displayed on the definition item in the package information area on some screens, because some software uses the CENTUM VP R5 or ProSafe-RS R3 license package model specification code.

Only for upgrade licenses, the background color of the Expiry cell changes as follows.

Table 1.2.4-3 Background color of the Expiry cell

Background color	Description
White	The current date is before the expiry date of the upgrade license.
Yellow	The current date exceeded the expiry date of the upgrade license.

If you exceed the number of unused licenses when assigning licenses, there is a change in the background color of the cell that indicates the number of unused licenses.

Table 1.2.4-4 Background color of the unused cell

Background color	Description
White	The number of unused licenses for this software package is more than 0.
Red	The number of unused licenses for a software package is a negative value. This is because you assigned more licenses than the quantity you own for a station.

Station information area

The station information area shows the information of each destination station for assigned licenses.

In the license management station, License Manager shows the information of stations for the entire license project. License Manager on the license-assigned station shows only information of its own station.

TIP

- If FCS licenses are assigned by using the license management station, the destination FCS information appears on the station information area in the license-assigned station that is installed with system builders. If SCS licenses are assigned by using the license management station, the destination SCS information appears on the station information area in the license-assigned station that is installed with SENG.
- If Project I/O licenses are assigned to PJTCOM by using the license management station, the PJTCOM information also appears in the station information area on the license-assigned station installed with the system builders or on the SENG specified as the license-assigned station.

The following items appear in the station information area:

- Component: The station name
- Comment: Station comments
- Domain: The domain numbers of the stations
- Station: The station numbers of the stations
- Status: The status of assigned licenses for the stations

Table 1.2.4-5 The status of assigned licenses for a station

Station	Status of assigned licenses	Background color	Status	Description
License management station (Editing mode)	OK	No background color	Normal	Licenses have been distributed and accepted
	EDIT	Yellow	Warning	License assignment is currently being edited, or upgrade licenses have been added, but not yet distributed.
	AckWait	Yellow	Warning	Licenses have been distributed and are waiting for acceptance
	RtnWait	Yellow	Warning	Waiting for deleted licenses to be returned using an external storage media
	Edit(NG)	Red	Error	License assignment is currently being edited (there is an error in the assignment details)

Continues on the next page

Table 1.2.4-5 The status of assigned licenses for a station (Table continued)

Station	Status of assigned licenses	Background color	Status	Description
License management station (Monitoring mode) (*1)(*2)	OK	No background color	Normal	Licenses are being assigned successfully
	DueToExp	Yellow	Warning	Licenses will expire within 30 days
	Unknown	Yellow	Warning	Cannot confirm status due to a communication error
	NoLicense	Red	Error	No license
	Error	Red	Error	There is a license error
	Expired	Red	Error	Licenses have expired
License-assigned stations(*1)	OK	No background color	Normal	Licenses are being assigned successfully
	DueToExp	Yellow	Warning	Licenses will expire within 30 days
	Error	Red	Error	There is a license error
	Expired	Red	Error	Licenses have expired
	NoLicense	Red	Error	No license

*1: When the licenses are waiting for acceptance, the prefix * is added to the character strings indicating the status of assigned licenses. (Example: *OK)
*2: When the licenses are waiting to be returned, the prefix ** is added to the character strings indicating the status of assigned licenses. (Example: **OK)

SEE ALSO For more information about PJTCOM, refer to:

"■ Station name and computer name default values" on page 2-9

Assignment area

In the assignment area, you can view whether a license has been assigned to a station.

In License Manager on the license management station, you can view whether licenses have been assigned for the entire system. In Editing mode, you can modify the license assignment.

In License Manager on a license-assigned station, you can view the license assignment status for the local station.

The background color of this area also indicates the license assignment status.

Table 1.2.4-6 Background display of the assignment area

Background color	Description
White	This cell can be assigned licenses.
Yellow	License assignment was modified or added for this cell, or upgrade license was added to extend the expiration for this cell.
Red	This cell was diagnosed with errors in the consistency check.
Gray	This cell cannot be assigned licenses.

SEE ALSO For more information about consistency checks, refer to:

"■ Building a license project for the first time" on page 1-10

2. Basic operations in license projects

This section describes the basic operations in license projects.

2.1 Process for managing licenses for the first time

This section describes the items required for managing licenses for the first time and the basic workflow for activating the software package.

Requirements

You need the following items to start managing licenses:

- License media (license key files)
- License sheet that lists the project IDs

Basic workflow

The basic workflow for managing licenses for the first time is shown in the following figure. Follow this workflow to activate a software package.

The steps until license distribution are performed using the License Manager on the license management station.

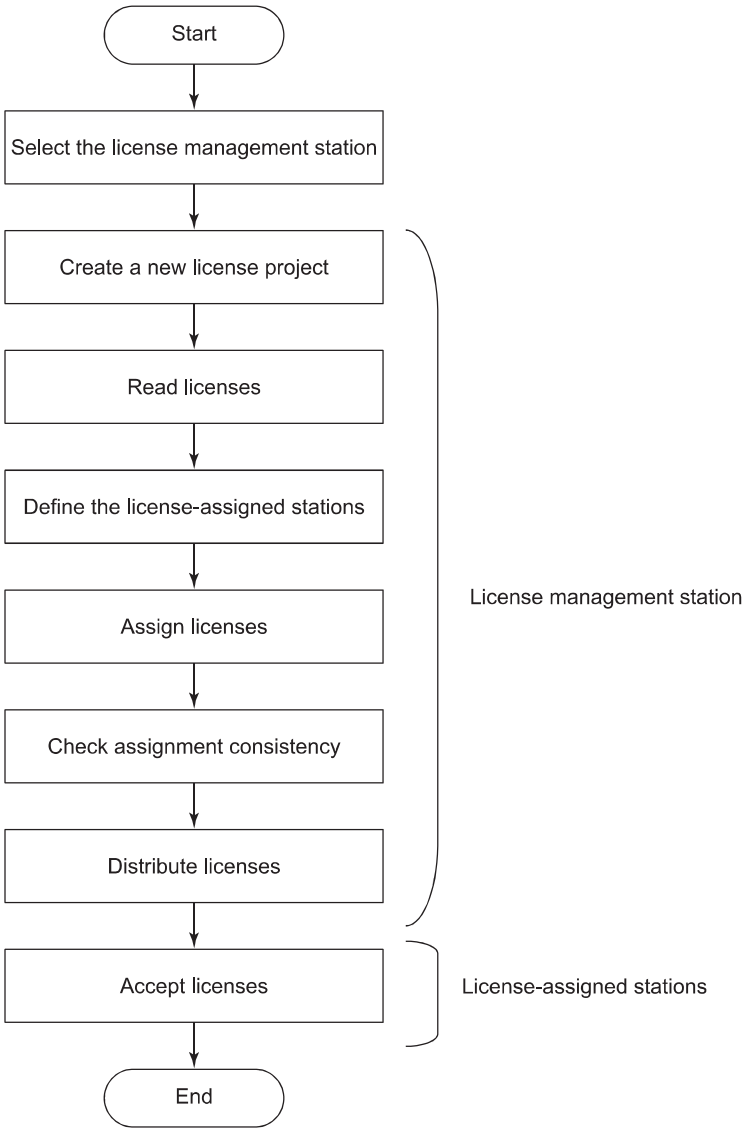


Figure 2.1-1 Steps for managing licenses for the first time

Selecting the license management station

From the computers installed with License Manager, select a computer to use as the license management station. If there are any computers that operate 24 hours a day, it is recommended that you select such a computer from the perspective of the consistency check.

2.2 Creating, switching, and deleting license projects

This section describes how to create, switch, and delete a license project for license management. When creating a license project, specify a backup folder.

TIP You can distribute licenses even if you do not specify a backup folder. However, in License Manager, license projects are automatically backed up when a license project is saved. For this reason, you should specify a backup folder first.

Creating a license project

Follow these steps to create a license project:

1. Sign in to the license management station computer as a user with maintenance privileges.
2. Start License Manager.
   License Manager window appears.
3. From the menu bar, select [File] > [New] > [Project].
   The Create new license project dialog box appears.
4. Specify the following information:
   - In the Project name box, type a name for the license project using a character string containing between 1 and 8 characters.
     You can use uppercase single-byte English letters, numeric characters, hyphens (-), and underscores (_). However, the first character must be an uppercase English letter.
   - If multiple system products are installed, select a system product name from the System type drop-down list.
5. Click [OK].
   The license project is created and the license project window appears in the License Manager window.

TIP When you manage licenses for multiple projects on one license management station, also use this procedure to create license projects.

Specifying a backup folder

For the license project backup folder, you must specify a folder in the hard drive of another computer on the same network, or a hard drive that is added to your computer, and that is writable by everyone. You can also specify a shared folder on the file server that was configured by using the IT Security Tool.

Follow these steps to specify a backup folder for license projects:

1. In the license project window, select the Project ID field.
2. From the menu bar, select [File] > [Property].
   The License project property dialog box appears.
3. Click the [...] button next to the Backup folder box.
   The folder selection dialog box appears.
4. Select the drive and folder for the backup.
   In the Comments box, type some comments if required.
5. Click [OK].
   The backup folder for the license project has now been specified.

Switching a display of license project

License Manager can manage multiple license projects. If you want to manage multiple license projects such as CENTUM VP and ProSafe-RS by one License Manager, you can switch the license project to be displayed.

Perform this step to switch the display of license project:

- From the menu bar of License Manager, select [Window], and select the check box of the license project you want to display.
  The selected license project appears in the license project window. If multiple license projects are selected, multiple selected license projects appear.

Deleting a license project

Follow these steps to delete a license project:

1. In the license project window, select the Project ID field.
2. From the menu bar, select [File] > [Delete].
   A dialog box appears to confirm whether you want to delete the license project.
3. Click [Yes].
   The license project is deleted.

2.3 Reading a license

Licenses are read by the license management station. This section describes how to read a license key file from the license medium and register the licenses in the license project.

Reading a license

When reading a license, you need a license medium.

When reading a license for the first time in a newly created license project, project ID written in the license sheet is required.

Follow these steps to read a license:

1. Insert the license media into the drive of the license management station.
2. From the License Manager menu bar, select [License] > [Add licenses].
   The folder selection dialog box appears.
3. Select the drive in which you inserted the license media.
4. Click [OK].
5. Perform one of the following operations:
   - When you read a license for the first time in a newly created license project, a dialog box to verify project ID is displayed. Enter the project ID number mentioned in the license sheet.
   - If a license has already been read in the license project, move to step 6.
6. Click [OK].
   A confirmation dialog box appears to confirm whether you want to save the license project.
7. Click [Yes].
   The license key file is read from the license medium. If you click [No], the read operation is terminated.

When the license key file is read, the Project ID number and package types (license information) displayed in the license project window are updated.

TIP

- If the entered project ID number and the project ID number stored on the license media do not match, an error occurs. Enter the correct project ID number.
- If there is more than one license medium with the same project ID, read the license key file from each license medium.
- Under the folder that you specify by selecting [License] > [Add licenses], you can place only one license key file. If you use license key files by copying them from the license medium to a local disk or somewhere else, you must create a folder to store each individual license key file.

2.4 Defining stations to which licenses need to be assigned

This section describes how to define stations.

On the license management station, you can define each computer and FCS or SCS to which you want to assign licenses, as a license-assigned station. You can also define the license management station itself as a license-assigned station and assign licenses to it.

Note that, if you read Project I/O Licenses on the license management station, a license-assigned station of PJTCOM is automatically defined. And PJTCOM is added to the license project window.

TIP

As an alternative to the manual data entry described in this section, you can also import station configuration and license assignment information from a package list. A package list is a CSV file that describes the configuration of stations and license assignment information for each of the stations.

SEE ALSO

For more information about importing package lists, refer to:

"■ Importing a package list" on page 3-29

For more information about PJTCOM, refer to:

"■ Station name and computer name default values" on page 2-9

■ Defining a license-assigned station

Follow these steps to define a license-assigned station:

1. From the License Manager menu bar, select [File] > [New] > [Station].
   Alternatively, in the station information area in the license project window, right-click and select [Add station].

   The Add station dialog box appears.

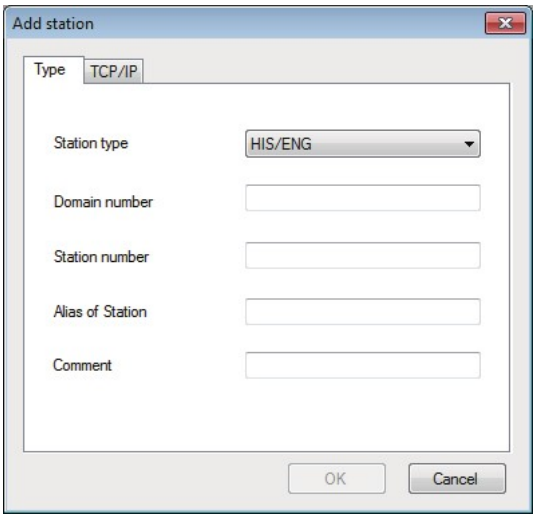


Figure 2.4-1 Add station dialog box

2. In the Type tab, specify station type settings.
   The options are described in the following "Options in the Add station dialog box" section.
3. Click the [TCP/IP] tab.
   In the Host Name box under the Ethernet TCP/IP Settings, the default computer name appears.

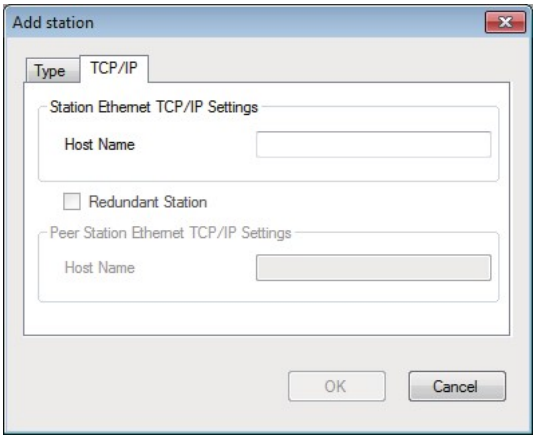


Figure 2.4-2 Add station dialog box

4. Specify a computer name, if required.
   If you select FCS, SCS, or PJTCOM from the Station type drop-down list, you do not need to specify any TCP/IP tab items.
5. Click [OK].
   The defined station is added to the license project window.

TIP

To use a network switchover type UGS, select "UGS" in Station type. To use a computer switchover type UGS, select "UGS2" in Station type. If you select UGS in Station type, the [Redundant Station] check box becomes available. If you select UGS2 in Station type, the [Redundant Station] check box is grayed out and becomes unavailable.

SEE ALSO

For more information about PJTCOM, refer to:

"■ Station name and computer name default values" on page 2-9

For more information about computer switchover type redundancy, refer to:

2.11, "Managing licenses of a computer switchover type UGS" on page 2-20

For more information about network switchover type redundancy, refer to:

2.12, "Managing licenses of a network switchover type redundant UGS" on page 2-22

■ Add station dialog box specifications

The items that you specify in the Type tab of the Add station dialog box are as follows:

- Station type
  Select the station type from the drop-down list. Only the stations that can be defined for the product being managed by the license project appear.
- Domain number
  Specify the domain number of the control bus.

  For stations not connected to the control bus, leave this blank.
- Station number
  Specify the station number of the local station that is connected on the control bus.

  For stations not connected to the control bus, leave this blank.
- Alias of station
  You can enter a station alias of your choice. Enter up to eight single-byte alphanumeric characters. If you specify a station alias, the station alias appears with higher priority than the station name in the component area of the license project window.
- Comment

You can enter a comment of your choice.

When you add a station, an automatic check is performed to check for errors relating to duplications and input range. If there is an error in the specified information, the Station properties error dialog box appears. Check the details of the error and change the specifications.

Station name and computer name default values

Station names are automatically determined based on the station type, domain number, and station number.

The station name format is as follows:

Station type dd (domain number) ss (station number)

Example: HIS0164

The following table shows the CENTUM VP and ProSafe-RS station types, automatically determined station names, and default computer names.

Table 2.4-1 Station names and default computer names in CENTUM VP

Station type	Station name	Default computer name
HIS/ENG	HIS[ddss]	HIS[ddss]
FCS	FCS[ddss]	N/A
SIOS	BCVO[ddss](SIOS)	E[ddss]
GSGW	FCS[ddss](GSGW)	GSGW[ddss]
APCS	FCS[ddss](APCS)	APCS[ddss]
UGS (*1)	BCVU[ddss](UGS) BCVU[ddss](UGS)(Peer) (*2)	E[ddss] E[ddss](Peer) (*2)
UGS2 (*3)	BCVU[ddss](UGS)	E[ddss]
UACS	UACS[ddss]	UACS[ddss]
PC (*4)	STN[ddss] (*5)	None
PJTCOM (*6)	PJTCOM	N/A

*1: Select this station type when using a network switchover type UGS.
*2: This is the second computer for a network switchover type redundant UGS.
*3: Select this station type when using a computer switchover type UGS.
*4: The station type of an AD server that does not coexist with Operation and Monitoring Function and system builders is "PC". The station name is same as the computer name.
*5: If a domain number or station number is not specified, a station name is not automatically determined.
*6: A virtual station assigned with Project I/O Licenses. Only one PJTCOM can be defined in a license project. It is automatically created when you add the license key.

Table 2.4-2 Station names and default computer names in ProSafe-RS

Station type	Station name	Default computer name
HIS/SENG (*1)	HIS[ddss]	HIS[ddss]
SENG	STN[ddss] (*2)	None
SCS	SCS[ddss]	N/A
PC (*3)	None	None
PJTCOM (*4)	PJTCOM	N/A

*1: This is a station defined as HIS on CENTUM VP System View.
*2: If a domain number or station number is not specified, the station name will be the same as the computer name.
*3: The station type of an AD server that does not coexist with SENG is "PC."
*4: A virtual station assigned with Project I/O Licenses. Only one PJTCOM can be defined in a license project. It is automatically created when you add the license key.

When using virtual test functions

When you use virtual test functions, provide either of the following settings on the computer where you run the FCS simulator or the SCS simulator:

- For a computer installed with a control bus interface card or Vnet/IP interface card, define it in the same manner as when you define an HIS, SENG, or other station.
- For a computer not installed with a control bus interface card or Vnet/IP interface card, define it with the station type "PC". You do not need to specify the domain number and station number.

For a computer that runs the UACS simulator, define it in the same manners as when you define a UACS station.

Relationship of License Project and AD Project in ProSafe-RS

In ProSafe-RS R4 or later, all RS projects corresponding to the station (SCS) defined for the license project, must be registered in the same AD project. This relationship is shown in the figure below.

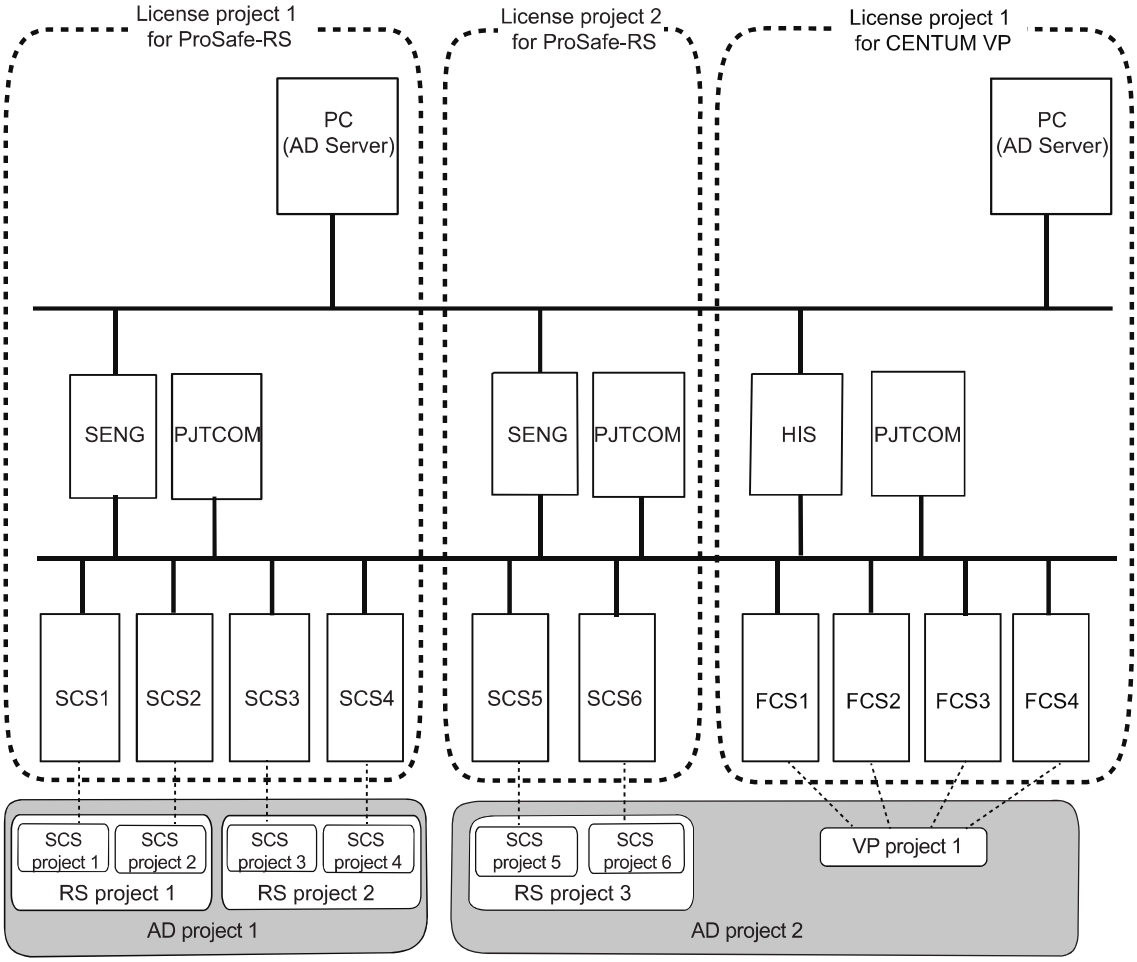


Figure 2.4-3 Relationship of License Project and AD Project in ProSafe-RS

2.5 Assigning licenses to license-assigned stations

Using License Manager on the license management station, you can assign licenses to the stations on which you want to use the software packages.

Even in an environment for virtual testing that does not include any actual stations, licenses are required according to the number of stations defined in the CENTUM VP or ProSafe-RS project.

Assigning licenses

1. In the license project window, select a cell in the assignment area.
2. Type the number of licenses assigned to each station.
   - To assign a license, type 1. If you do not want to assign a license, leave it blank.
   - As for the project I/O license, the quantity of the license is shown in the cell in the assignment area of PJTCOM. Ensure that the quantity that is shown in the cell is the same as the quantity of the project I/O license that is provided.

   The status of stations that have been assigned a license changes to EDIT and the background color of the respective cell changes to yellow.

TIP

If licenses cannot be assigned to a station, you cannot enter the number of licenses in that cell.

SEE ALSO

For more information about status display, refer to:

"■ License project window" on page 1-18

For more information about PJTCOM, refer to:

"■ Station name and computer name default values" on page 2-9

Copying license assignment information

Follow these steps to copy license assignment information from one station to another:

1. In the license project window, click the name of the station from which you want to copy information.
2. From the License Manager menu bar, select [Edit] > [Copy].
   Alternatively, right-click the station name and select [Copy].
3. Select the name of the station to which you want to paste the information.
4. From the menu bar, select [Edit] > [Paste].
   Alternatively, right-click the name of the station and select [Paste].

   The status of the station to which you pasted the license assignment information changes to EDIT and the background color of the relevant cell changes to yellow. If the number of available licenses is exceeded as a result of the [Paste] operation, the status changes to NG. In this case, review the license assignment information.

To cut and paste the license assignment information for a station, select [Cut] instead of [Copy].

2.6 Checking license assignment consistency

Using License Manager, you can perform consistency checks to find errors related to license assignments. For example, you can find errors such as exclusions and dependencies of software packages on stations assigned with licenses.

In the consistency check, all stations that have been assigned licenses are checked.

A consistency check is automatically performed when licenses are distributed, but you can also perform a check at any time.

SEE ALSO For more information about items verified during a consistency check, refer to:

Appendix 1., “Items checked in the license assignment consistency check” on page App.1-1

Checking the consistency of license assignment

To perform a consistency check, from the License Manager menu bar, select [License] > [Check consistency].

The consistency check result appears in the message display area. If an error is detected, the corresponding cell in the assignment area changes to red, modify the assignment to rectify the error.

2.7 Distributing and accepting licenses through a network

This section describes how to distribute assigned licenses from the license management station to a license-assigned station through a network, and how to activate the licenses.

Distributing a license to license-assigned stations through a network

Follow these steps to distribute a license from the license management station to a licenseassigned station through a network:

IMPORTANT

The license-assigned station to which the license is being distributed must be running.

1. From the License Manager menu bar, select [License] > [Distribute licenses].
   A list of the stations that have been assigned a license and have the EDIT status appears in the Distribute licenses dialog box.

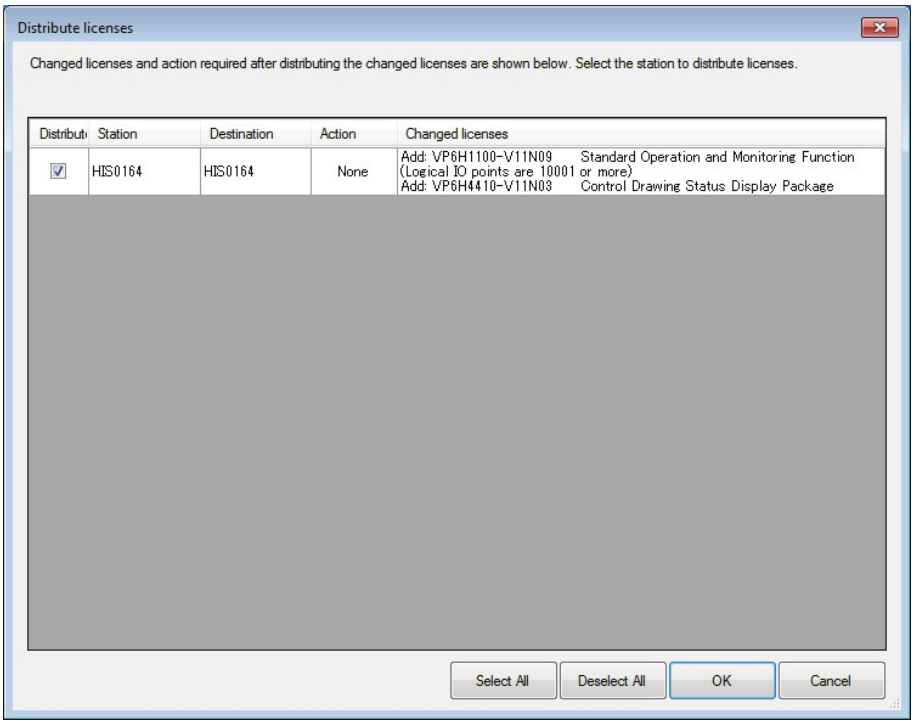


Figure 2.7-1 Distribute licenses dialog box

   In the Distribute licenses dialog box, the Action column indicates the actions required to accept the license assignment changes on the license-assigned station. Changed licenses column indicates the package names of licenses. When distributing licenses for the first time, all licenses are shown in the format: "Add: <Package type>."

2. In the Distribute column, select the check box for the stations to which you want to distribute a license. By default, all stations are selected as distribution destinations.

3. Click [OK].
   License Manager automatically checks the following:

   - Is there consistency in the license assignments for the stations to which licenses need to be distributed?

- Has the number of licenses distributed to the license-assigned stations exceeded the number of licenses of the software package?
- On the license-assigned stations for distribution, are there any errors in the version number, language, station type, and assignment exclusions between products?

4. If there are no errors in the check, a dialog box appears to confirm whether you want to save the license project.
5. Click [Yes].
   The licenses are distributed to the stations targeted for distribution. If you click [No], the distribution operation is terminated.

When distribution of the license to the license-assigned stations is successful, the status of the station is updated from EDIT to AckWait.

TIP After the licenses have been accepted on the distribution destination station, the status of the station changes to OK.

If a warning is generated during the license verification, a warning message appears in the message display area and a confirmation dialog box appears. The license is distributed to the target station after confirmation is received.

If the operation to send the license information fails, and an error occurs during the license verification, distribution of the license to the destination stations is suspended and an error message appears in the message display area. Remove the cause of the error and distribute the license again. If you selected multiple stations, you need to distribute licenses to all destinations. If distribution to any station fails, the entire distribution operation fails.

Distributing FCS or SCS licenses

FCS or SCS licenses are viewed when generating and downloading the system builders. For this reason, distribute FCS/SCS licenses as follows:

- For FCS

  The distribution destination for FCS licenses is stations assigned with a Standard Engineering Function license, not the actual FCS.

TIP All stations that are assigned with a Standard Engineering Function license must be connected to the network. If the stations cannot be connected to the network at the time, distribute the licenses to all the stations that are assigned with a Standard Engineering Function license through an external storage medium.

- For SCS

  The distribution destination for SCS licenses is the stations assigned with SENG, not the actual SCS.

TIP All SENGs must be connected to the network. When temporarily the stations cannot be connected to the network, distribute the licenses to all SENGs via an external storage medium.

If multiple stations appear in the distribution destination, the status of the FCS or SCS station changes to OK once a license is assigned to at least one station.

Distributing Licenses to PJTCOM

- For CENTUM VP R6
  The licenses are distributed to the station to which the license for the basic engineering functions is assigned.
- For ProSafe-RS R4
  The licenses are distributed to the SENG.

SEE ALSO For more information about PJTCOM, refer to:

"■ Station name and computer name default values" on page 2-9

■ Accepting a license and activating a software package on a license-assigned station

After the license management target product is installed, the licenses initially distributed through the network are accepted automatically. After the licenses have been accepted, the status of the license-assigned station changes to OK.

The software package is activated on stations to which licenses have been distributed. You do not need to perform any procedures using License Manager on the license-assigned stations. When you start License Manager on a license-assigned station, the assignment status for the local station appears and you can confirm the license status in the station information area.

TIP When distributing licenses to a license-assigned station two or more times, you need to accept the licenses on the license-assigned station. The software packages are activated when you restart the station after accepting the licenses.

2.8 Distributing and accepting licenses using external storage media

You can use external storage media to distribute licenses to a station that cannot communicate with the license management station, and activate software packages.

To distribute licenses using external storage media, first save the "license file" generated by License Manager on the license management station to an external storage medium. When this license file is read by the license-assigned station, the software package becomes available on that station.

IMPORTANT

It is recommended that you use an unused CD-R for the external storage media to avoid virus infection.

License files

A license file is a file that stores licenses assigned to stations. A license file is generated for each station.

Distributing licenses by using external storage media

To distribute licenses using external storage media, first generate the license file using License Manager on the license management station.

Follow these steps to create license files:

1. From the License Manager menu bar, select [License] > [External storage media] > [Distribute licenses].
   The stations that have been assigned licenses and have the EDIT status appear in the distribute licenses using external storage media dialog box.
2. In the Distribute column, select the check box for the stations to which you want to distribute a license.
3. Click [OK].
   A license assignment consistency check is performed for the stations to which licenses need to be distributed. If the consistency check does not return any errors, a dialog box appears to confirm whether you want to save the license project.
4. Click [Yes].
   A dialog box appears to specify a folder. If you click [No], the license file is not generated.
5. Specify the folder to which you want to save the license files.
6. Click [OK].
   In the folder that you specified for generating the license file, a folder with a different ID is created for each station, and the license file is exported. When the license file is saved, the status of the station is updated from EDIT to OK.

If a consistency error occurs, the process of saving the license file to destination stations is terminated, and an error message appears in the message display area. Remove the cause of the error and distribute the license again.

License file names, paths, and validity durations

The names, paths, and validity durations for license files are as follows:

- License file names and paths
  `[user-specified_folder]\[station_ID]\[project_name]. [station_name].lf`

Example: F:\PC001\MYPJT.PC001.lf

- License file validity durations
  The validity duration for license files is three days. Ensure that you load a license file onto the license-assigned station within three days after the file is created. If the validity duration has expired, you will not be able to load the file.

TIP

If you are unable to load the license file because the validity duration has expired, or if you lose the license file, use the Distribute Master licenses function to redistribute the license.

Activating a software package using external storage media

A license distributed using external storage media needs to be read by the license-assigned station and the software package needs to be activated. The procedure for activating a software package is as follows.

Store the license file generated on the license management station on external storage media.

IMPORTANT

On the license-assigned station, stop the antivirus software, and applications of products that you started and for which you want to accept licenses.

1. Log on to the license-assigned station as a user with maintenance privileges.
2. Insert the external storage media containing the license file into the drive.
3. Start License Manager.
   License Manager window appears.
4. From the menu bar, select [License] > [External storage media] > [Accept licenses].
   The folder selection dialog box appears.
5. From the external storage media drive, select the folder containing the license file.
6. Click [OK].
   If the license file has not expired or if there are no errors in the license file, the Accept licenses dialog box appears.
7. Click [OK].
   The license file is read and the software package is activated. In addition, the license project window is updated and you can check the assignment status for the local station.

TIP

If the version of the license to be distributed and the version of the software in the destination station does not match, the license cannot be accepted.

2.9 Monitoring the status of assigned licenses

You can perform the following license monitoring using License Manager on the license management station and license-assigned stations:

- License management station
  Monitor the status of assigned licenses in the entire license project.
- License-assigned stations
  Monitor the status of assigned licenses to the local station.

■ Monitoring the status of assigned licenses

From the License Manager menu bar on the license management station, select [View] > [Monitoring mode].

As soon as you switch to Monitoring mode, the status of assigned licenses appears for stations to which licenses have been distributed.

If you want to retrieve the most current assignment status from each station, on the menu bar, select [View] > [Refresh].

TIP

Stations in the license project, to which a license has not been distributed are not displayed.

On license-assigned stations, the status of assigned licenses for the local station appears as soon as License Manager starts.

SEE ALSO

For more information about status display, refer to:

"■ License project window" on page 1-18

● Monitoring the status of assigned licenses in the task tray

You can monitor the status of assigned licenses by viewing the icons displayed in the task tray.

SEE ALSO

For more information about the icons displayed in the task tray, refer to:

"■ Displaying the status of assigned licenses in the task tray" on page App.2-1

■ Notifying of alarms

When an abnormal license assignment status is detected, system alarms are generated and you can confirm the messages.

On stations that do not receive system alarm messages, a dialog box appears, notifying you to confirm them.

SEE ALSO

For more information about alarms, refer to:

Appendix 3., "Messages" on page App.3-1

2.10 Saving license projects

You can save station definitions and license assignments that you have been editing before distributing licenses. This data is saved as “work-in-progress” data in the license project. To save a license project, from the License Manager menu bar, select [File] > [Save].

When you open License Manager the next time, you can choose to either open the "work-in-progress" data, or open the (master) data for which licenses have been distributed.

2.11 Managing licenses of a computer switchover type UGS

To manage the licenses of a computer switchover type UGS, you must assign a station name for computer switchover type UGS to the target UGS. License Manager recognizes a pair of UGSs that make up a computer switchover type redundant UGS as one station. You must assign licenses for redundancy to that station.

TIP

When you use a computer switchover type redundant UGS, licenses for redundancy are required. When you use a computer switchover type UGS in a non-redundant configuration, only the license for Unified Gateway Station (UGS2) Standard Function is required.

■ Defining a computer switchover type UGS

Follow these steps to define a computer switchover type UGS:

1. On the license management station, start License Manager in Editing mode.
2. From the menu bar, select [File] > [New] > [Station].
   The Add station dialog box appears.
3. In the Station Type drop-down list of the Type tab, select "UGS2" and specify the following items:
   - Domain number
   - Station number

TIP

You can type a station alias and comments of your choice.

4. In the Station Ethernet TCP/IP Settings section of the TCP/IP tab, type the name of the first computer.
5. Click [OK].
   The defined UGS is added to the license project window as one station.

■ Assigning licenses to a computer switchover type UGS

Assign licenses for a computer switchover type UGS.

SEE ALSO

For more information about assigning licenses, refer to:

"■ Assigning licenses" on page 2-11

■ Distributing licenses to a computer switchover type UGS

You can distribute licenses in the same manner as other cases.

SEE ALSO

For more information about distributing licenses through a network, refer to:

"■ Distributing a license to license-assigned stations through a network" on page 2-13

■ Accepting licenses on a computer switchover type UGS

For a computer switchover type redundant UGS, accept licenses only on the active UGS.

For a non-redundant computer switchover type UGS, you can accept licenses in the same manner as other cases.

SEE ALSO For more information about accepting licenses, refer to:

"■ Accepting a license and activating a software package on a license-assigned station" on page 2-15

2.12 Managing licenses of a network switchover type redundant UGS

If you make individual stations redundant, you need to assign licenses to each redundant station and then distribute and accept them.

TIP You cannot make an existing station redundant by changing the station properties. To change an existing station to a redundant station, you must delete the existing station first, and then define a new redundant station.

■ Defining a network switchover type redundant UGS

Follow these steps to define a network switchover type redundant UGS:

1. On the license management station, start License Manager in Editing mode.
2. From the menu bar, select [File] > [New] > [Station].
   The Add station dialog box appears.
3. In the Station type drop-down list of the Type tab, select a station and specify the following items:
   - Domain number
   - Station number

TIP You can type a station alias and comments of your choice.

4. In the Station Ethernet TCP/IP Settings section of the TCP/IP tab, type the name of the first computer.
5. Select the Redundant Station check box.
   The Peer Ethernet TCP/IP Settings section becomes available.
6. In the Peer Ethernet TCP/IP Settings section, type the name of the second computer.
7. Click [OK].
   Two columns showing the network switchover type redundant UGS are added to the license project window. If there is an error in the information specified, the Station properties error dialog box appears. Change the information according to the error details.

■ Assigning licenses to a network switchover type redundant UGS

When assigning licenses to a network switchover type redundant UGS, ensure that the assignment information is the same on both stations

SEE ALSO For more information about assigning licenses, refer to:

"■ Assigning licenses" on page 2-11

■ Distributing licenses to a network switchover type redundant UGS

To distribute licenses to a network switchover type redundant UGS, select both stations and distribute licenses at the same time. You cannot distribute licenses to one station only.

SEE ALSO For more information about distributing licenses through a network, refer to:

"■ Distributing a license to license-assigned stations through a network" on page 2-13

Accepting licenses on a network switchover type redundant UGS

For a network switchover type redundant UGS, accept licenses on both stations.

SEE ALSO For more information about accepting licenses, refer to:

"■ Accepting a license and activating a software package on a license-assigned station" on page 2-15

3. Maintaining license projects

This section describes how to maintain license projects.

3.1 Reading additional licenses on a license management station

The procedure for reading additional purchased licenses on a license management station is the same as that for reading new licenses.

SEE ALSO For more information about reading licenses, refer to:

"■ Reading a license" on page 2-6

3.2 Modifying licenses

This section describes how to modify license assignments within the same license project, and how to distribute and accept licenses after changing the assignments.

The following figure shows the workflow of assigning licenses of the software packages that are required by a station.

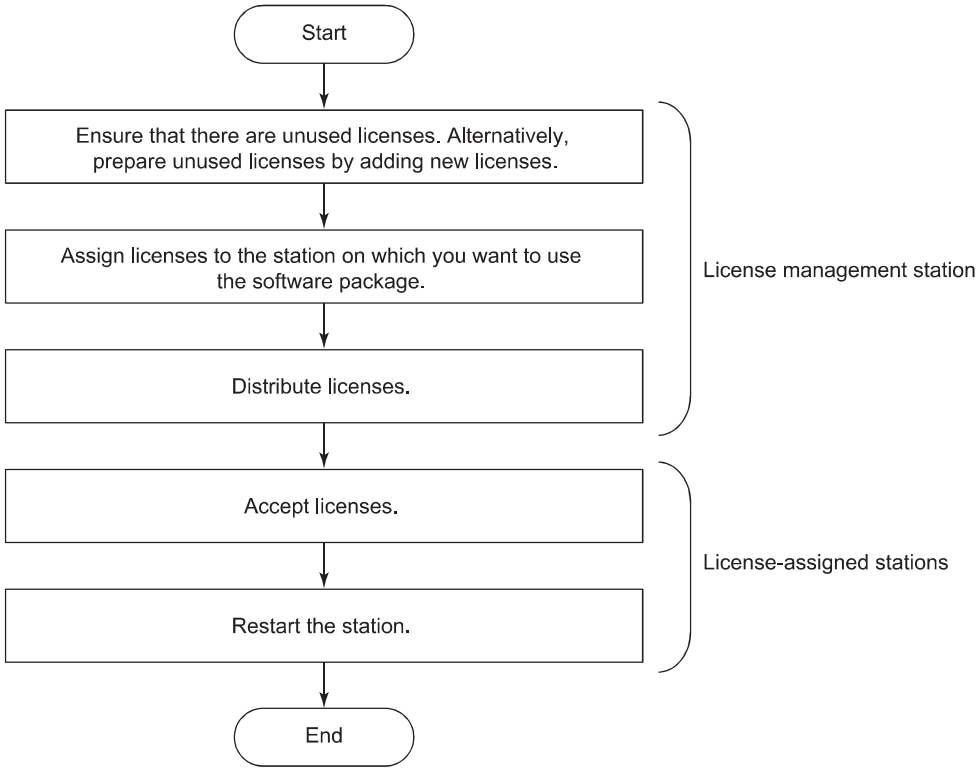


Figure 3.2-1 Assigning software package licenses to a station

The following figure shows the workflow of deleting licenses of a software packages that are no longer required from a station.

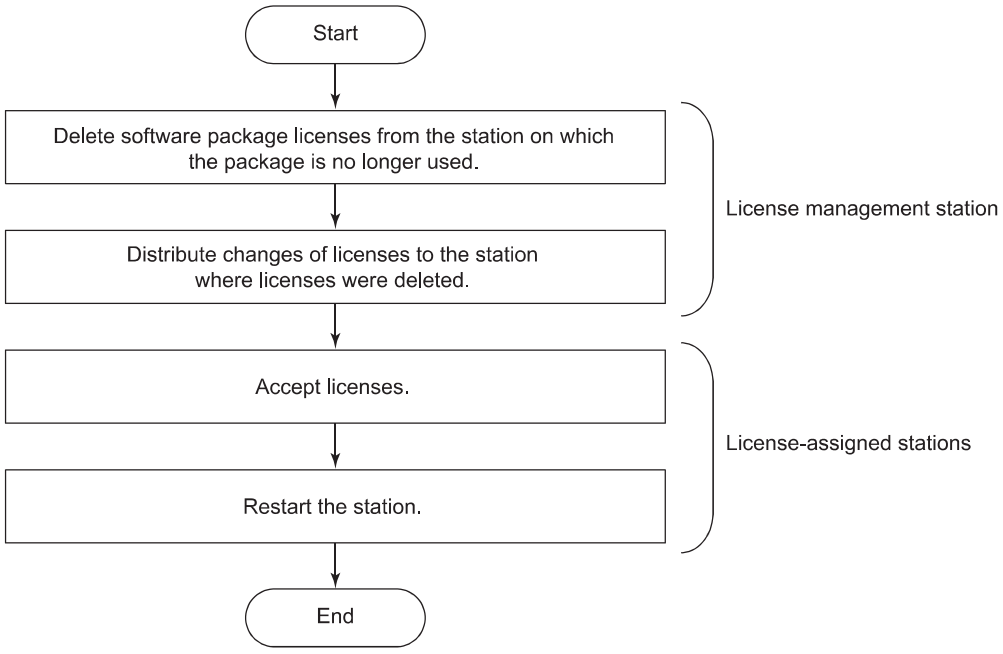


Figure 3.2-2 Deleting software package licenses from a station

The following figure shows the workflow of moving the license of a software package that is no longer used on a certain station to another station.

Example:

Moving a license from HIS0163 to HIS0162

HIS0163: Station from which a software package license is deleted.

HIS0162: Station to which the software package license is assigned.

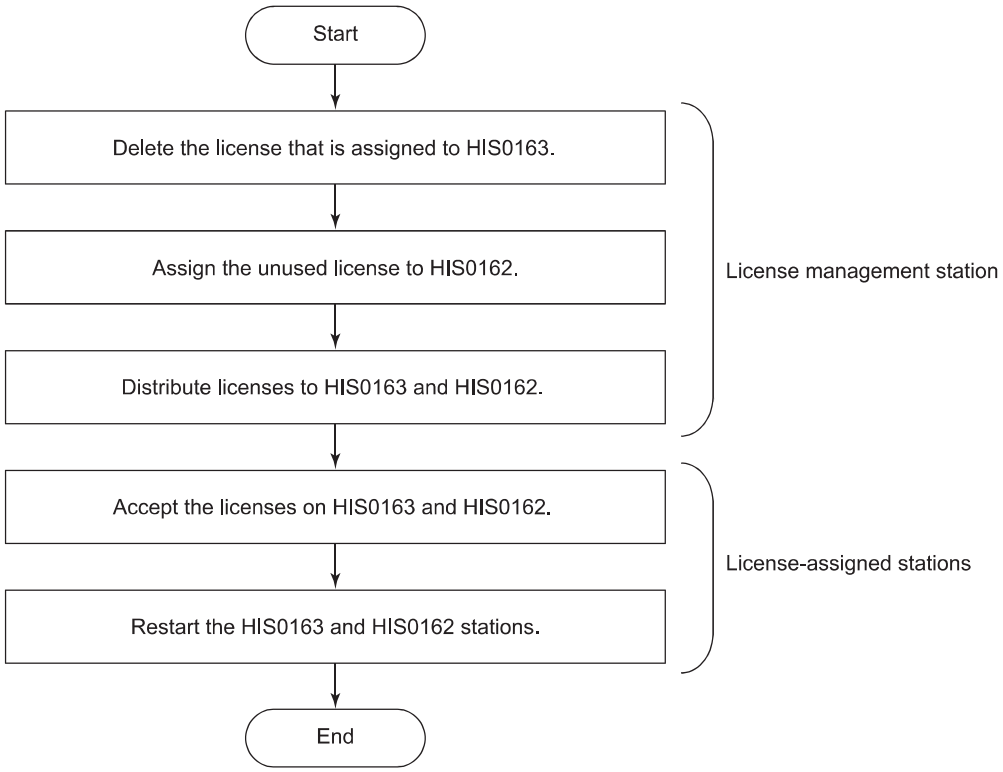


Figure 3.2-3 Moving a software package license between stations

3.2.1 Modifying license assignments

You can add or delete licenses on a license-assigned station by using License Manager on the license management station.

■ Adding a license to a license-assigned station

Follow these steps to add a license to a license-assigned station:

1. On the license management station, start License Manager in Editing mode.
2. Select the cell corresponding to the software package that you want to add to the licenseassigned station, and enter 1.
   - As for the project I/O license, the quantity of the license is added in the cell in the assignment area of PJTCOM. Ensure that the quantity that is shown in the cell is the same as the quantity of the project I/O license that is provided.

   The background color of the cell changes to yellow and the status of the station to which the license has been added changes to EDIT.
3. From the license management station, distribute the license to the station to which the license has been added.
4. On the license-assigned station, start License Manager and accept the license changes. The software package is activated.

TIP

- Status after distribution: AckWait; Background color after distribution: Yellow
- Status after acceptance: OK; Background color after acceptance: No background color

SEE ALSO

For more information about PJTCOM, refer to:

"■ Station name and computer name default values" on page 2-9

For more information about assigning licenses, refer to:

"■ Assigning licenses" on page 2-11

For more information about distributing licenses, refer to:

3.2.2, "Distributing modified licenses" on page 3-7

For more information about accepting licenses, refer to:

3.2.3, "Accepting modified licenses" on page 3-9

■ Deleting a license from a license-assigned station

Follow these steps to delete a license from a license-assigned station:

1. On the license management station, start License Manager in Editing mode.
2. Select the cell corresponding to the software package that you want to delete from the license-assigned station. On the keyboard, press the [Delete] key.
   The cell becomes empty and its background color changes to yellow. The status of the station from which the license has been deleted changes to EDIT.
3. From the license management station, distribute licenses to the station from which the license has been deleted.
4. On the license-assigned station, start License Manager and accept the license changes. The software package is deactivated.

TIP

- Status after distribution: AckWait; Background color after distribution: Yellow
- Status after acceptance: OK; Background color after acceptance: No background color

SEE ALSO

For more information about assigning licenses, refer to:

"■ Assigning licenses" on page 2-11

For more information about distributing licenses, refer to:

3.2.2, "Distributing modified licenses" on page 3-7

For more information about accepting licenses, refer to:

3.2.3, "Accepting modified licenses" on page 3-9

3.2.2 Distributing modified licenses

When license assignments are changed on the license management station, you need to distribute the affected licenses from the license management station to the license-assigned stations.

The procedure for distributing licenses is different depending on whether the station is connected to a network.

■ Distributing licenses with assignment changes through a network

The procedure for distributing licenses with assignment changes through a network is the same as that for distributing new licenses.

While distributing licenses, stations whose status has been changed to EDIT as a result of the license assignment being changed (added or deleted) for that station, appear in the Distribute licenses dialog box.

In the Distribute licenses dialog box, the Action column indicates the action(s) required to accept the distributed licenses on the license-assigned station. The Changed licenses column indicates the names of packages with license assignment changes.

- Added licenses: "Add: <package type>"
- Deleted licenses: "Del: <package type>"

Select the Distribute check box for stations to which you want to distribute a license and click [OK].

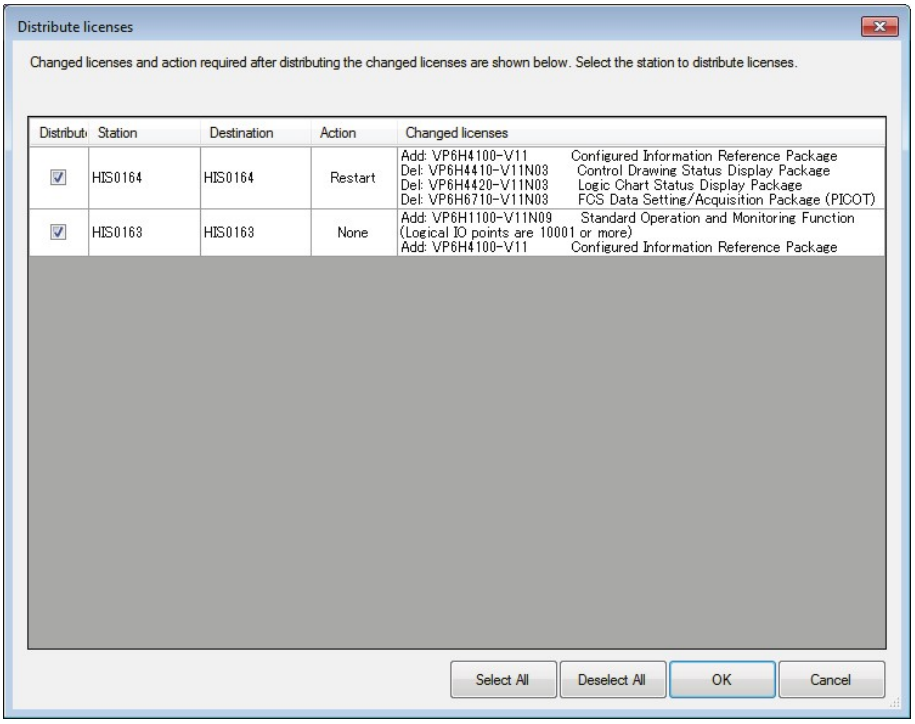


Figure 3.2.2-1 Distribute licenses dialog box

After licenses have been successfully distributed to the license-assigned stations, the status of the station changes from EDIT to AckWait.

SEE ALSO For more information about distributing licenses to license-assigned stations through a network, refer to:

"■ Distributing a license to license-assigned stations through a network" on page 2-13

Distributing licenses with assignment changes using external storage media

The procedure for distributing licenses with assignment changes to the stations that are not connected to the network is the same as that for distributing new licenses.

SEE ALSO For more information about distributing license by using external storage media, refer to:

"■ Distributing licenses by using external storage media" on page 2-16

3.2.3 Accepting modified licenses

This section describes the procedure for activating and deactivating software packages with license changes. To accept licenses that have been distributed to the license-assigned stations, you need to replace the existing license file with the new license file on the respective stations. You must restart the stations after accepting the modified licenses. The software packages are either activated or deactivated based on the license changes.

The procedure for accepting licenses is different depending on whether the station is connected to a network.

Accepting licenses with assignment changes through a network

Follow these steps to accept modified licenses on license-assigned stations that have received licenses through a network:

IMPORTANT

On the license-assigned station, stop the antivirus software, and applications of products that you started and for which you want to accept licenses.

1. Log on to the license-assigned station as a user with maintenance privileges.
2. Start License Manager.
   License Manager appears and the assignment status of the local station appears in the license project window. In the summary information area, confirm that the status of the station is AckWait and there are licenses that are waiting to be accepted.
3. From the menu bar, select [License] > [Accept licenses].
   The modified licenses and the actions required after acceptance appear in the Accept licenses dialog box.

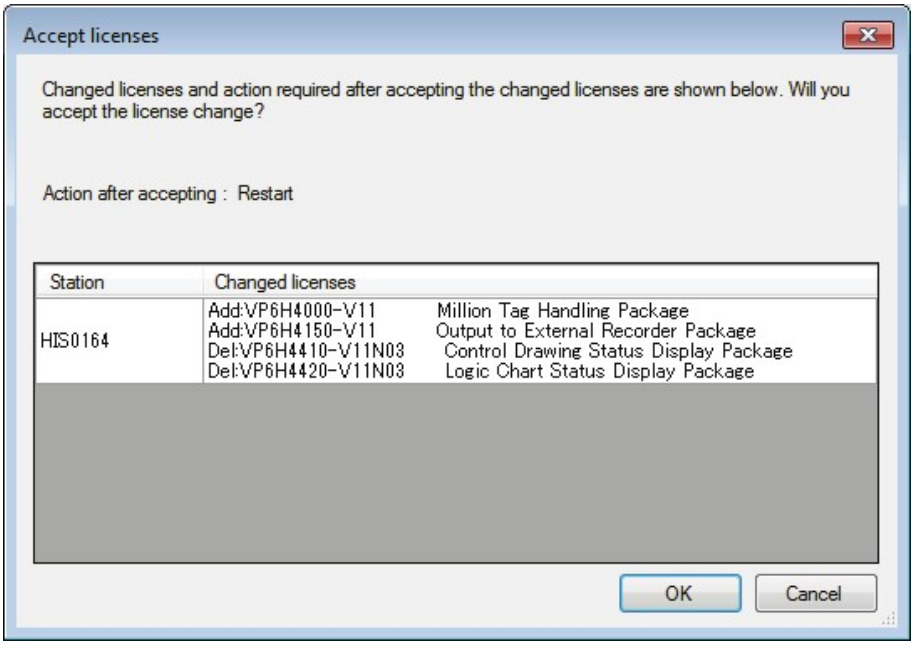


Figure 3.2.3-1 Accept licenses dialog box

4. Click [OK].
   A dialog box appears, asking you to confirm whether the applications of the product whose license you are accepting have been closed.
5. If the applications are not running, click [Yes].

If the applications are still running, click [No]. The license acceptance operation is terminated.

6. When there is a need to restart the station after accepting licenses, a dialog box appears, asking whether you want to continue with accepting licenses.
7. Click [Yes]. The acceptance operation starts.
   After the acceptance operation is completed, the station restarts automatically and the software packages are either activated or deactivated based on the license changes.

TIP

When you accept a license on a license-assigned station, the status of the corresponding station changes from AckWait to OK in License Manager on the license management station.

■ Accepting licenses with assignment changes using external storage media

When you distribute licenses using external storage media, the license-assigned station reads the modified licenses and activates or deactivates the software package. You can accept modified licenses using external storage media in the same way as you activate a license using external storage media. When you restart the stations after accepting licenses, software packages are either activated or deactivated based on the modified licenses.

When you delete previously distributed licenses, a returned license file is created on the license-assigned station. A returned license file is a file that stores information confirming that a license that was distributed using external storage media has been deleted and is no longer in use. A dialog box appears, asking you to specify the location where you want to save the returned license file.

SEE ALSO

For more information about accepting licenses by using external storage media, refer to:

"■ Activating a software package using external storage media" on page 2-17

3.2.4 Returning licenses using external storage media

On a license-assigned station, if a previously distributed license is deleted when you accept license modifications using external storage media, a returned license file is generated. When the returned license file is read by the license management station, it is considered as an unused license and can be assigned to another station.

The license management station shows the RtnWait status when licenses are to be deleted and are waiting to be returned from a license-assigned station using external storage media. Therefore, you need to return the licenses promptly.

SEE ALSO For more information about status display, refer to:

"■ License project window" on page 1-18

■ Format for the generated returned license file

The file name of the returned license file and the path to which it is exported is as follows:

`[user-specified_folder]\[station_ID]\[project_name].[station_name].rlf`

Example: F:\HIS0164\MYPJT.HIS0164.rlf

■ Returning licenses using external storage media

Follow these steps to read a returned license file on the license management station:

1. Go to the returned license file that was generated by the license-assigned station when accepting the license, and copy the returned license file to an external storage medium.
2. Insert the external storage media into the drive of the license management station.
3. On the license management station, start License Manager in Editing mode.
4. From the menu bar, select [License] > [External storage media] > [Return licenses].
   The folder selection dialog box appears.
5. Select the returned license file from the external storage medium.
6. Click [OK].
   When the returned license file is read, the status of the corresponding station changes from RtnWait to OK, and the number of unused licenses increases. The procedure for returning the license is completed.

● Regenerating another returned license file

If you cannot find the returned license file, you can generate it again as follows:

1. Start License Manager on the license-assigned station where you previously generated the returned license file.
2. From the menu bar, select [License] > [External storage media] > [Output returned licenses].
   A dialog box appears asking you to select the location for generating the returned license file.
3. Select the location where you want to save the returned license file.
4. Click [OK].
   The returned license file is generated in the specified folder.

3.3 Adding and deleting license-assigned stations

You can add stations to a license project in order to manage the licenses of a station, and delete unnecessary stations from a license project.

If the properties of a station that has been distributed with licenses are changed, you must change the properties of that station to ensure that licenses on that station remain manageable. This can be done by using License Manager on the license management station.

■ Adding a license-assigned station

In License Manager on the license management station, define the station that you are adding as a license-assigned station. The procedure for adding a license-assigned station is the same as that for defining a new license-assigned station.

SEE ALSO For more information about defining a license-assigned station, refer to:

"■ Defining a license-assigned station" on page 2-7

■ Deleting an unnecessary license-assigned station

IMPORTANT

- To delete a station from a license project, first delete the licenses that are assigned to that station. You can delete a station even if the status is EDIT. However, when deleting an FCS or SCS station from a license project, first delete the assignments, distribute and accept the licenses, and check that the status is OK before deleting the station. You cannot delete the station if the status is EDIT or AckWait.
- If you delete a license-assigned station that is running, the licenses on that station become deactivated. When you restart the license-assigned station, the station is removed from the license management targets and no licenses are assigned. Use discretion when deleting a station.

Follow these steps to delete a license-assigned station:

1. On the license management station, start License Manager in Editing mode.
2. Delete the license assignments for the station that you want to delete.
3. In the license project window, click the station name.
4. From the menu bar, select [File] > [Delete].
   Alternatively, right-click the station name and select [Delete station].

   The Delete Station dialog box appears.
5. Click [Yes].
   The column of the deleted station is removed from the license project window.
6. From the menu bar, select [File] > [Save].
   The station is deleted.

● Deleting redundant stations

To delete redundant stations that are no longer required, first delete the licenses that are assigned to both stations.

Then, select the name of either of the stations and delete it. This deletes both stations at the same time from the license project.

Changing the properties of a station

Follow these steps to change the properties of a station:

1. On the license management station, start License Manager in Editing mode.
2. In the license project window, click the station name.
3. From the menu bar, select [File] > [Properties].
   Alternatively, right-click the station name and select [Station property].

   The Station property dialog box appears.
4. Enter the data for the properties that you want to change and click [OK].
   The station properties are changed and the status changes to EDIT.

TIP

If you only change the alias of the station and comments, the station status remains the same.

5. From the menu bar, select [File] > [Save].
   The properties are changed.

Station properties

The station properties are listed as follows:

TIP

If you want to change properties listed as View only, delete the station, and add a new station.

Table 3.3-1 List of station properties

Property	Attributes
Station type	View only
Domain number	View only
Station number	View only
Comment	Modifiable
Station alias	Modifiable
Host name	Modifiable
Redundant station	View only
Peer host name	Modifiable

3.4 Redistributing licenses to license-assigned stations

You can use the Distribute master license function to redistribute licenses that were last distributed from the license management station to license-assigned stations. If a license-assigned station fails, you can replicate the license assignments for the failed station by distributing the master license to the replacement computer where the license management target product is installed.

Master license

A master license is a license that was last distributed to a specified station by the user. A master license file is a file that contains a master license, and the content is different for each station.

The file format of master license files is the same as that of license files.

SEE ALSO For more information about license files, refer to:

2.8, “Distributing and accepting licenses using external storage media” on page 2-16

Redistributing a license to redundant stations

If you specify one redundant station as the destination for master license distribution, the most recently distributed license will be redistributed to the specified redundant station only. You do not need to distribute licenses to both stations at the same time.

3.4.1 Distributing and accepting master licenses through a network

This section describes how to distribute and accept master licenses on stations connected to a network.

■ Distributing and accepting master licenses through a network

Follow these steps to distribute and accept master licenses through a network:

1. On the license management station, start License Manager in Editing mode.
2. From the menu bar, select [License] > [Distribute master licenses].
   In the Distribute Master licenses dialog box, all stations that have been previously distributed with licenses appear.

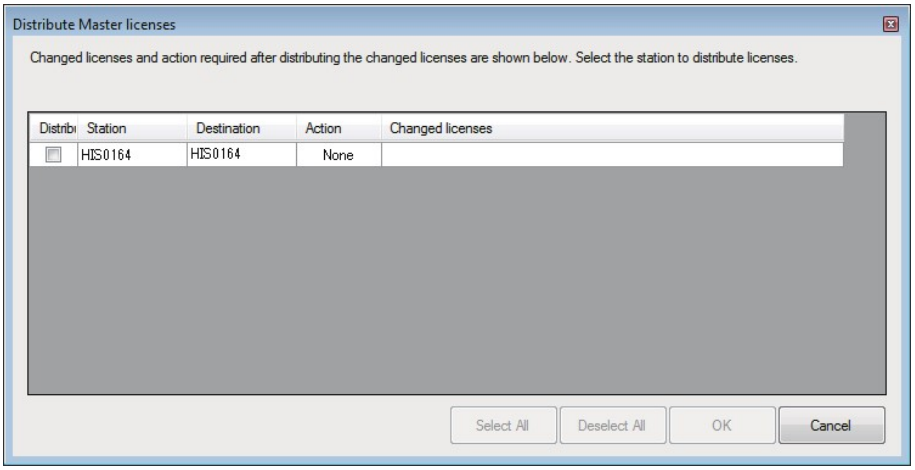


Figure 3.4.1-1 Distribute Master licenses dialog box

3. Select the Distribute check box for the stations to which you want to distribute a master license.
4. Click [OK].
   The master license is distributed to the license-assigned station.

When the master license distribution is completed, the software packages to which licenses were distributed are activated in stations that have None in the Action column.

SEE ALSO

For more information about preliminary checking of license information, refer to:

"■ Distributing a license to license-assigned stations through a network" on page 2-13

For more information about Accepting licenses through a network, refer to:

"■ Accepting licenses with assignment changes through a network" on page 3-9

3.4.2 Distributing and accepting master licenses using external storage media

This section describes how to distribute and accept master licenses on stations not connected to a network, by using external storage media.

■ Distributing and accepting master licenses for stations not connected to a network using an external storage media

Follow these steps to distribute and accept master licenses for stations not connected to a network, by using external media:

1. On the license management station, start License Manager in Editing mode.
2. From the menu bar, select [License] > [External storage media] > [Distribute master licenses].
   All stations that have been previously distributed with licenses appear in the dialog box.
3. Select the Distribute check box for the stations to which you want to distribute a license.
4. Click [OK].
   A dialog box appears to specify a folder.
5. Specify the folder to which you want to save the master license.
6. Click [OK].
   In the folder that you specified for saving the license file, a folder is created for each station that has been distributed with the master license. The license files are saved to these folders.
7. Copy the license file to an external storage medium.

IMPORTANT

To avoid virus infections, it is recommended that you copy licenses into an unused CD-R.

On the license-assigned station, load the license file that is stored on the external storage medium and accept the master licenses.

SEE ALSO For more information about accepting master licenses using external storage media, refer to:

"■ Activating a software package using external storage media" on page 2-17

3.5 Increasing the software package capacity

If you need to increase the number of I/O that can be handled by FCS or SCS, add a Project I/O License.

If you need to increase the number of I/O points that can be handled by Operation and Monitoring Function and Basic Engineering Function, add a Project I/O License for expansion.

TIP

For example, use an upgrade installation license when you increase the number of Field Control Stations that can be handled by Operation and Monitoring Function and Standard Builder Function in CENTUM VP R5.

An upgrade installation license is loaded into License Manager on the license management station, merged with a new installation license, and then distributed to a license-assigned station. An upgrade installation license cannot be distributed independently. It can be distributed as an expanded new installation license after merging it with a new installation license.

This section describes the procedures for increasing the capacity of a software package by merging a new installation license with an upgrade installation license.

IMPORTANT

Licenses cannot be divided after they have been merged. Perform merging licenses very carefully.

Increasing the software package capacity

Follow these steps to increase the capacity of a software package:

1. On the license management station, start License Manager in Editing mode.
2. Read the upgrade installation licenses on the license management station.
3. Assign the new installation licenses and upgrade installation licenses to the same station.
4. From the menu bar, select [License] > [Merge licenses].
   A dialog box appears, asking you to confirm the packages for upgrading.
5. Click [Yes].
   The new installation licenses and upgrade installation licenses are merged. You can check the merged licenses by viewing the package type.

Before merging

Project ID	XXXXXXX1			Component		PJTCOM	HIS0164
Edit : 2	Edit(NG) : 0			Comment			
AckWait : 0	RtnWait : 0			Domain			1
Expired : 0	DueToExpire : 0			Status	Station		64
Package type	Package name	Expiry	Qty	Unused		Edit	Edit
-- [PJTCOM] --	---	---	---	---		---	---
VP6F3100-V11	Project I/O License		100	0		100	
-- [HIS] --	---	---	---	---		---	---
VP6H1100-E11N59	Standard Operation and Monitoring...		1	0			1
VP6H1100-V11N05	Standard Operation and Monitoring...		3	2			1
VP6H1120-V11	Console HIS Support Package for ...		3	3			

After merging

Project ID	XXXXXXX1			Component		PJTCOM	HIS0164
Edit : 2	Edit(NG) : 0			Comment			
AckWait : 0	RtnWait : 0			Domain			1
Expired : 0	DueToExpire : 0			Status	Station		64
Package type	Package name	Expiry	Qty	Unused		Edit	Edit
-- [PJTCOM] --	---	---	---	---		---	---
VP6F3100-V11	Project I/O License		100	0		100	
-- [HIS] --	---	---	---	---		---	---
VP6H1100-V11N05	Standard Operation and Monitoring...		2	2			
VP6H1100-V11N09	Standard Operation and Monitoring...		1	0			1
VP6H1120-V11	Console HIS Support Package for ...		3	3			

Making VP6H1100-V11N09 by merging VP6H1100-V11N05 with VP6H1100-E11N59

Figure 3.5-1 Merging new installation licenses with upgrade installation licenses

6. Distribute the expanded license to license-assigned stations, and then accept them on the license-assigned stations.

TIP

If there are multiple licenses that can be merged, you can merge them as one group in a single merge operation.

SEE ALSO

For more information about reading licenses, refer to:

"■ Reading a license" on page 2-6

For more information about assigning licenses, refer to:

"■ Assigning licenses" on page 2-11

For more information about distributing licenses through a network, refer to:

"■ Distributing a license to license-assigned stations through a network" on page 2-13

For more information about accepting licenses through a network, refer to:

"■ Accepting licenses with assignment changes through a network" on page 3-9

3.6 Backing up and restoring a license project

If a license management station fails, you can set up a new license management station by restoring the backed up license project in another station, or on a computer where License Manager alone is installed.

This section describes the procedures for backing up a license project manually and restoring it.

■ Manually backing up a license project

Follow these steps to back up a license project manually:

1. On the license management station, start License Manager in Editing mode.
2. From the menu bar, select [Tools] > [Backup].
   The license project is backed up.

SEE ALSO For more information about specifying the backup folder for the license project, refer to:

"■ Specifying a backup folder" on page 2-4

■ Restoring a license project on another license management station

For this procedure, you will need the license media that contains the purchased license key file.

Follow these steps to restore a license project on another license management station:

1. On the station to which you want to restore the license project, start License Manager in Editing mode.
2. From the menu bar, select [Tools] > [Restore].
   The folder selection dialog box appears.
3. Select the folder that stores the backup of the license project that you want to restore, and click [OK].

TIP If a license project with the same name already exists, the restore process is terminated.

The Restore license project dialog box appears, displaying a list of license key files required for the restoration.

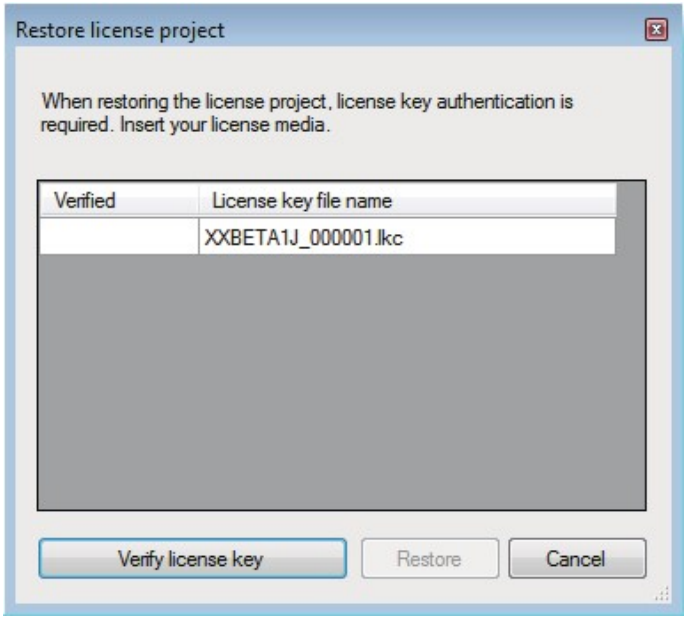


Figure 3.6-1 Restore license project dialog box

4. Insert any one of the license media in which the license key file to verify is stored, and click [Verify license key].
   The folder selection dialog box appears.
5. Select the drive for the external storage media and click [OK].
   On the Verified column in the Restore license project dialog box, the check box of the selected license key file is selected.
6. When the Verified check box is selected, in the Restore license project dialog box, click [Restore].
   The license project is restored, and a new license project window appears in License Manager.

TIP

After you have restored the license projects on the new license management station, use the Distribute master licenses function to distribute master licenses to license-assigned stations through the network. This enables you to monitor the license assignment status.

3.7 Moving licenses to other projects

This section describes the procedure for moving licenses to other license projects.

For example, if an optional software package is no longer needed in one license project, you can move the license for that software package to a different license project and assign it to an HIS or SENG that is managed by that license project.

After loading the migration license key file on License Manager, delete the license from the license project from which it has been moved. This is to allow the license to be moved to a different license project.

Next, you need to create a license key file for the destination license project, and load it in the license project.

Migration license key files

To move licenses to other license projects, you will need a separate license medium for storing the migration license key file. Contact YOKOGAWA to request the license medium. The migration license key file contains the following information:

- Project IDs of the source license project and the destination license project
- The package type and version information of the license that you want to move
- Number of licenses being moved

Procedure for moving licenses to other license projects

The following figure illustrates the procedure for moving licenses to another license project.

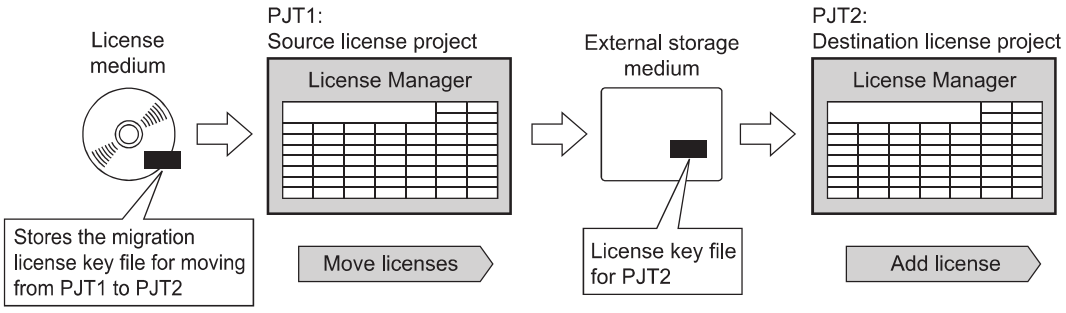


Figure 3.7-1 Moving licenses to another license project

The following flowchart illustrates the workflow for moving licenses to another license project.

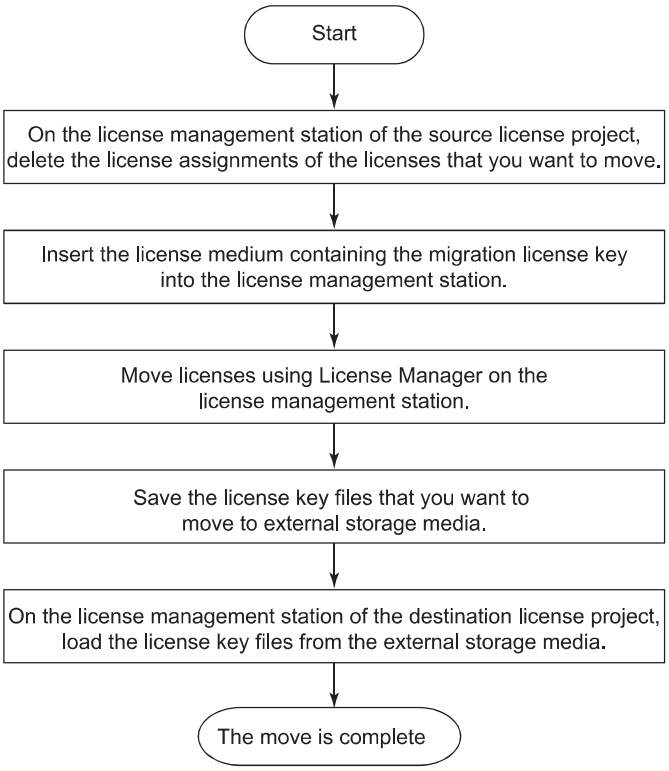


Figure 3.7-2 Workflow for moving a license

Moving licenses to another license project

Follow these steps to move a license to another license project:

1. On the license management station of the source license project containing the licenses you want to move, start License Manager in Editing mode.
2. Ensure that the licenses are released from all the stations by deleting the assignments of the licenses that you want to move. You can do this in the same way you modified license assignments.
3. On the license management station, insert the license medium containing the migration license key into the media drive.
4. From the menu bar, select [License] > [Move licenses].
   The folder selection dialog box appears.
5. Select the migration license key file and click [Open].
   A dialog box appears to confirm whether you want to move the license.

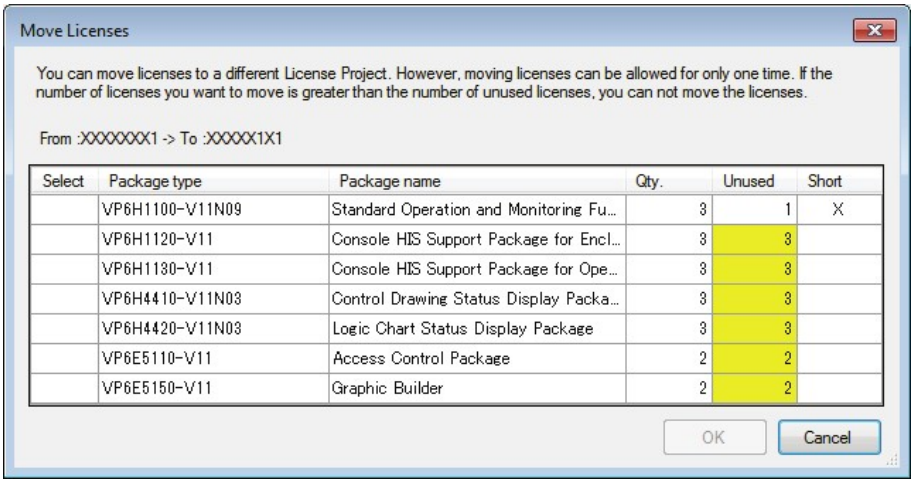


Figure 3.7-3 Confirmation of License move dialog box

6. Check the package type and number of licenses for the license that you are moving and click [OK].
   A dialog box appears, asking you to specify the location for saving the license key files that you want to move.

TIP

- If the number of unused licenses is less than the number of licenses to be moved, you will not be able to click OK. In this case, the corresponding Short column is selected.
- If the number of unused licenses is more than the number of licenses to be moved, you can select the license that you want to move.

7. Specify the location for saving the license key files to be moved.
8. Click [OK].
   The license key files for the destination are created in the specified folder.
9. Save the created license key files on an external storage media.
10. On the destination license management station, start License Manager.
11. Read the licenses in the same way as when adding a license.
    The licenses are successfully moved to another project.

IMPORTANT

When you restore a license project, specific license key files are required. So, you must keep the following license medium and license key files:

- License medium that stores the migration license key file
- License key files moved to the destination project that were created on the license management station of the source project

The file names of the license key files are as follows:

- Migration license key file: <SrcProjectID>_<SerialID>.lkc
- License key files moved to the destination project: <ProjectID>_<SerialID>.lkc

ProjectID: Project ID of the destination project

ProjectID: Project ID of the source project

SerialID: ID that is assigned when the license key is issued

SEE ALSO For more information about reading licenses, refer to:

"■ Reading a license" on page 2-6

For more information about changing license assignments, refer to:

3.2, "Modifying licenses" on page 3-3

3.8 Changing the computer name of a license-assigned station

To change the computer name of a license-assigned station to which licenses are already assigned, you must first delete the station from the license project and change the computer name, then perform the task to add the station to the license project again.

Changing the computer name of a license-assigned station

Follow these steps to change the computer name of a license-assigned station:

1. On the license management station, start License Manager in Editing mode.
2. Delete the license assignments of the license-assigned station for which you want to change the computer name.
3. Distribute and accept the licenses.
4. In License Manager on the license management station, confirm that the status of the license-assigned station has become OK, and then delete the license-assigned station from the license project.
5. Change the computer name.
6. Add the license-assigned station to the license project with the new computer name.
7. Assign licenses to the license-assigned station and distribute the licenses.
8. Restart the license-assigned station.

SEE ALSO For more information about adding and deleting license-assigned stations, refer to:

3.3, “Adding and deleting license-assigned stations” on page 3-12

3.9 Functions to help with license assignment work

In License Manager, you can use the following functions to help with license assignment work.

- Importing and exporting package lists

  You can use a general text editing tool to create a package list from information for stations that make up a license project and information on license assignments, and import it into a license project. You can also export a package list from a license project.

- Searching for character strings in the license project window
- Folding the display of software packages in the license project window
- Filtering information that appears in the license project window
- Deleting software package licenses from a license project
- Creating an assigned licenses status file

3.9.1 Importing and exporting package lists

A package list is a CSV file that contains information about the stations that make up a project, and information about the license assignments of each station.

You can define station configurations and license assignments by importing package lists into a license management station.

You can also export a package list from a license management station.

Package list file format

The following example shows a CSV-format package list displayed in a spreadsheet application.

	A	B	C	D	E	F	G	H
1	@ProjectID	XXXXXXX1						
2	@Product	CENTUM VP						
3	@StationType					PJTCOM	HIS/ENG	HIS/ENG
4	@StationName					PJTCOM	HIS0164	HIS0163
5	@ComputerName						HIS0164	HIS0163
6	@StationAlias							
7	@StationComment							
8	#	PackageType	Paid	Expiry	Ver.			
9	@Package	VP6F3100-V11	P		R6	100		
10	@Package	VP6H1100-V11N09	P		R6		1	1
11	@Package	VP6H4100-V11	P		R6		1	1
12	@Package	VP6H4150-V11	P		R6		1	1
13	@Package	VP6H4450-V11	P		R6		1	1
14	@Package	VP6H6510-V11	P		R6		1	1
15	@Package	VP6H6530-V11	P		R6		1	1

Figure 3.9.1-1 Package list in CSV format

The following table shows examples of identifiers and formats for license management information that are required in a package list, and whether specifying them in the package list is mandatory or not.

Table 3.9.1-1 Identifiers and formats for license management information and whether they are mandatory or not

Specified items	Identifiers and formats	Details	Required to specify during import?
Project ID	@ProjectID , <project ID>	Project ID for the license project	Required
Product name	@Product , <product_name>	The product name for the license project	Required
Station type	@StationType ,,,, <station_type_1>, <station_type_2> ,... , <station_type_N>	All station types in a license project	Required
Station name	@StationName ,,,, <station_name_1>, <station_name_2> ,... , <station_name_N>	All station names in a license project	Required (*1)
Computer name	@ComputerName,,,, <computer_name_1>, < computer_name_2> ,... , < computer_name_N>	The computer names of all stations in the license project	Required (*2)
Station alias	@StationAlias ,,,, <station_alias_1>, <station_alias_2> ,... , <station_alias_N>	The station alias of all stations in the license project	Optional

Continues on the next page

Table 3.9.1-1 Identifiers and formats for license management information and whether they are mandatory or not (Table continued)

Specified items	Identifiers and formats	Details	Required to specify during import?
Station comment	@StationComment ,,,, < station_comment_1>, < station_comment_2> ,... , < station_comment_N>	Comments for all stations in the license project	Optional
Package information	@Package, < MS_code > , <paid_flag> , < duration> , <version> , < assignment_numbers_for_station_1> , < assignment_numbers_for_station_2>	Package license information and assignment information	Required
Comment line	Lines starting with #		Optional

*1: Not required for stations not connected to a control bus.
*2: Not required for an FCS or SCS.

Table 3.9.1-2 Identifier format values and descriptions

Specified items	Value	Description
<station_type>	Same as the station types that can be specified when adding a station Example: HIS, FCS, GSGW, SIOS, UGS, UGS2	Station type
<station_name>	Same as the station name Leave this blank if there is no domain number and no station number. When importing, the domain number, station number, and redundant station settings are read from the station name. Example: HIS0164, FCS0101, BCVU0163(UGS)(Peer)	Station name
<computer name>	The values specified in the station properties This value is set for the Peer station if the station name ends with (Peer).	Station properties
<station_alias> <station_comment>	The values specified in the station properties This value is ignored if the station name ends with (Peer).	Station properties
<paid_flag>	By default, Paid P is specified If the paid flag for the imported package list is blank, it is considered paid.	
<expiration>	No expiry date: Blank Expiry date: YYYY/MM/DD YYYY Year MM Month DD Day Example: 2015/12/22	License expiry date
<version>	R<version_number > Example: R6	License version number
<number_assigned>	Number of assigned licenses If there are no assigned licenses at the time of exporting, the exported package list will be blank. If the number of assigned licenses at the time of importing is 0 or blank, the number of assigned licenses is set to 0.	Number of licenses assigned for each station

The permitted capacity for the package list is shown in the following table.

Table 3.9.1-3 Permitted capacity for package list

Specified items	Permitted capacity
Maximum number of stations	256
Maximum number of rows of packages	200

Importing a package list

Follow these steps to import a package list:

1. On the license management station, start License Manager in Editing mode.
2. From the menu bar, select [File] > [External File] > [Import].
   The file selection dialog box appears.
3. Select the package list that you want to import.
4. Click [Open].
   License Manager automatically checks the license assignments for consistency and checks the package lists, and updates its window with information from the imported package list.
5. From the menu bar, select [File] > [Save] .
   The imported package list is saved.

Any errors and warnings appear in the message display area. Find out the cause and resolve the problem.

Import process

The process of importing a package list is as follows:

- Station information
  If the imported package list contains stations that were not in the license project, the stations and their assignment information are added.

  If the imported package list contains stations that are already in the license project, the properties of those stations are overwritten.

  The station properties consist of information from the package list, such as <computer name>, <alias of station>, and <station comment>.

  The information related to stations not included in the imported package list remains the same when performing the import.
- Assignment information
  If the imported package list includes assignment information for stations that are already in the license project, the assignment information is overwritten.

  If the imported package list does not include assignment information for stations that are already in the license project, the current assignment information remains the same.

  If the license project includes redundant stations, specify the assignment information for both stations in the package list.
- Information on licensed software packages (package type, version)
  If the imported package list contains information on software packages that were not in the license project, set the number of licenses to 0 and add a row.

Items checked when importing

When you import a package list, License Manager automatically checks the license assignments for consistency and checks the package lists. If an error is detected, details of the error appear in the message display area and the import process is terminated.

The following package list items are checked.

Table 3.9.1-4 Items checked in the package list

Checked item	Description
File type	Checks whether the file is in CSV format.
Entry	Checks whether the following mandatory items have been entered: Project ID Product name Station type Station name Computer name
Product name	Checks whether the product name is the same as that of the license project.
Project ID	Checks whether the project ID is the same as that of the license project.
Packages that can be assigned	Checks that there are no package types that cannot be assigned to the station type.
Redundant station settings	Checks that the assignment details for the first and second station are the same.

Exporting a package list

Follow these steps to export a package list:

1. Start License Manager.
2. From the menu bar, select [File] > [External File] > [Export].
   A dialog box appears to confirm whether you want to save the file.
3. Specify the folder to which the package list needs to be exported and a file name for the package list.
4. Click [Save].
   The package list for the license information is exported to the specified folder using the specified file name.

3.9.2 Searching for characters in the license project window

You can search for character strings in the license project window.

Performing a search

Follow these steps to use the License Manager search function:

1. Open the license project in which you want to search for text.
2. From the License Manager menu bar, select [Edit] > [Find].
   The Find dialog box appears.
3. In the Find string box, enter the search text and click [Find next].
   The search starts from the upper-left part of the license project window and moves towards the right. It continues downward when the row is completed.
   The cursor moves to a result that matches the search text.

   If there are no matches, a message appears.

3.9.3 Folding the display of a license project

In the license project package information area, there is a list of software packages for each station type.

You can display or hide the package type by expanding or folding the license project rows.

Collapsing the display

In the license project window, click the [+] and [-] collapse buttons on the left of the package type.

The rows are collapsed so that only the applicable package type appears.

Click the [+] and [-] buttons to switch between the normal display and collapsed display.

3.9.4 Filtering information that appears in the license project window

You can filter the view to show only the station columns and software package rows that match the conditions selected in the license project window.

You can select the following conditions:

- Filtering by station type
- Filtering by domain number
- Filtering by station status
- Filtering by license paid/free, expiry date (time-limited/open-ended), and version

You can specify multiple filtering conditions independently. If you are filtering using multiple filtering conditions, only the columns and rows that match all of the conditions appear.

For example, if you filter by FCS, all station types other than FCS stations are collapsed and only the FCS packages appear.

Filtering contents

Follow these steps to filter the display:

1. In the license project window, click the Filter button for attributes that you want to filter by.
2. From the drop-down menu that appears, select the filter conditions.
   Only the station columns and license rows that match the selected conditions appear.

3.9.5 Deleting software package licenses from a license project

You can delete licenses for software packages from a license project if the software packages meet both of the following conditions:

- Software packages that do not have licenses assigned to a station
- The number of available licenses is zero (*1), or the software packages cannot be used as they have expired.

*1: When creating a license project, if you imported a package list that contains software packages whose license quantity is zero, a row is added for that software package indicating zero license quantity.

TIP

After upgrading the licenses, the licenses of software packages that are no longer needed should be deleted from the license project.

SEE ALSO

For more information about importing package lists, refer to:

3.9.1, “Importing and exporting package lists” on page 3-27

Deleting software package licenses

Follow these steps to delete licenses for a software package:

IMPORTANT

Deleted software package licenses cannot be restored. You must delete software package licenses very carefully.

1. On the license management station, start License Manager in Editing mode.
2. In the license project window, select the software package that you want to delete.
   You can only select one software package.
3. From the menu bar, select [License] > [Delete license].
   The Delete license dialog box appears.
4. Click [Yes].
   The license of the software package is deleted.

3.9.6 Creating an assigned licenses status file

In License Manager, you can create the license assignment status as a text file. Follow these steps to create a file:

1. On the license management station, from the License Manager menu bar, click [View] and select one of the following export modes:
   - Editing mode
   - Monitoring mode

   You do not need to select a mode for a license-assigned station.
2. From the menu bar, select [Tool] > [Output report].
3. In the file selection dialog box, specify the following items:
   - Folder in which the file should be created
   - File name
4. Click [Save].
   A text file is saved to the specified folder.

Structure of the assigned licenses status file

The following tables describe the structure of the file containing information about assigned licenses.

Header

The following information is saved in the Header section:

Table 3.9.6-1 Information in the Header section

Title	Description
License Manager Report [Station name] ([Mode])	[Station name] ([Mode]) The name of the station that generated the file and the mode of the license project Example: HIS0164 (Monitoring mode)
Date	The local date on which the file was generated

Project Information

License project information is saved in the Project Information section. The following table shows the items that are saved in the Project Information section.

Table 3.9.6-2 Information in the Project Information section

Title	Description
Product	Product name
Project ID No	Project ID number
Project name	License project name
Comment	Comments about the license project
License Admin	License management flag 1: License management station 0: License-assigned station
Back up folder	The backup folder for the license project

The information that is saved changes according to the license project mode. The information that is saved in each mode is as follows:

- Editing mode

Table 3.9.6-3 Information saved in Editing mode

Title	Description
Edit	Number of licenses with an Editing status
Edit(NG)	Number of stations that returned an error in the consistency check
AckWait	Number of stations waiting for license acceptance
RtnWait	Number of stations waiting for licenses to be returned
Expired	Number of stations with expired licenses
DueToExpire	Number of stations with licenses that will expire in 30 days or less

- Monitoring mode

Table 3.9.6-4 Information saved in Monitoring mode

Title	Description
Error	Number of stations with license errors
Expired	Number of stations with expired licenses
DueToExpire	Number of stations with licenses that will expire in 30 days or less
Unknown	Number of stations for which the status cannot be tracked
AckWait	Number of stations waiting for license acceptance
RtnWait	Number of stations waiting for licenses to be returned

- Assigned station mode

Table 3.9.6-5 Information saved in Assigned Station mode

Title	Description
Error	Number of stations with license errors
Expired	Number of stations with expired licenses
DueToExpire	Number of stations with licenses that will expire in 30 days or less
AckWait	Number of stations waiting for license acceptance

Package List

License package information is saved in the Package List section. The following table shows the items that are saved in the Package List section.

For each package, items in the Package List section are assigned a consecutive number starting from one, and each item is saved in a new line.

Table 3.9.6-6 Information in the Package List sections

Title	Description
No	A consecutive number starting from one is automatically saved for each license
PackageType	Package type

Continues on the next page

Table 3.9.6-6 Information in the Package List sections (Table continued)

Title	Description
InternalPackage	CENTUM VP R5 package model corresponding to the CENTUM VP R6 package model, or ProSafe-RS R3 package model corresponding to the ProSafe-RS R4 package model
PackageName	Package name
Paid	Shows whether it is paid or free Paid: P Free: F
Expiry	Validity duration Time-limited: Expiry date and time Non-time-limited: -
Ver.	version
Qty	Number of licenses
Unused	Number of unused licenses

Station Information, Station Information-Package

Information about stations is saved in the Station Information section. Information about licenses assigned to a station is saved in the Station Information-Package section.

The following information is saved in the Station Information section:

Table 3.9.6-7 Information in the Station Information section

Title	Description
StationType	Station type
Domain,Station	[Domain number][Station number] Example: 1, 63 Empty if there is no domain or station
StnName	Station name
Alias	Alias of station
Comment	Comment
Computer	Computer name
Status	The status that appears in the license window.(*1)

*1: The text that appears is different in Editing mode and Monitoring mode.

The following items are saved in the Station Information-Package section:

Table 3.9.6-8 Information in the Station Information-Package section

Title	Description
No	A consecutive number starting from one is automatically saved for each license
PackageType	Package type
InternalPackage	CENTUM VP R5 package model corresponding to the CENTUM VP R6 package model, or ProSafe-RS R3 package model corresponding to the ProSafe-RS R4 package model
PackageName	Package name
Paid	Shows whether it is paid or free Paid: P Free: F

Continues on the next page

Table 3.9.6-8 Information in the Station Information-Package section (Table continued)

Title	Description
Expiry	Validity duration Time-limited: Expiry date and time Non-time-limited: -
Ver.	version
Assign	Number of licenses assigned to the displayed station(*1)

*1: The number may be different in Editing mode and Monitoring mode.

4. Upgrading the Licenses from CENTUM VP R5 to R6, or from ProSafe-RS R3 to R4

This section describes how to upgrade the licenses from CENTUM VP R5 to R6, or from ProSafe-RS R3 to R4. Before starting upgrading of the licenses, you must install CENTUM VP R6 or ProSafe-RS R4 software packages on the computers to which you want to distribute the upgraded licenses.

CENTUM VP is not affected by the ProSafe-RS license upgrading, and vice versa.

4.1 Process for License Upgrading

This section describes the basic procedures about how to upgrade licenses that are assigned in all stations within a license project.

As for how to upgrade the licenses for some HISs, it is described in the other section.

The following figure shows the procedures of upgrading licenses.

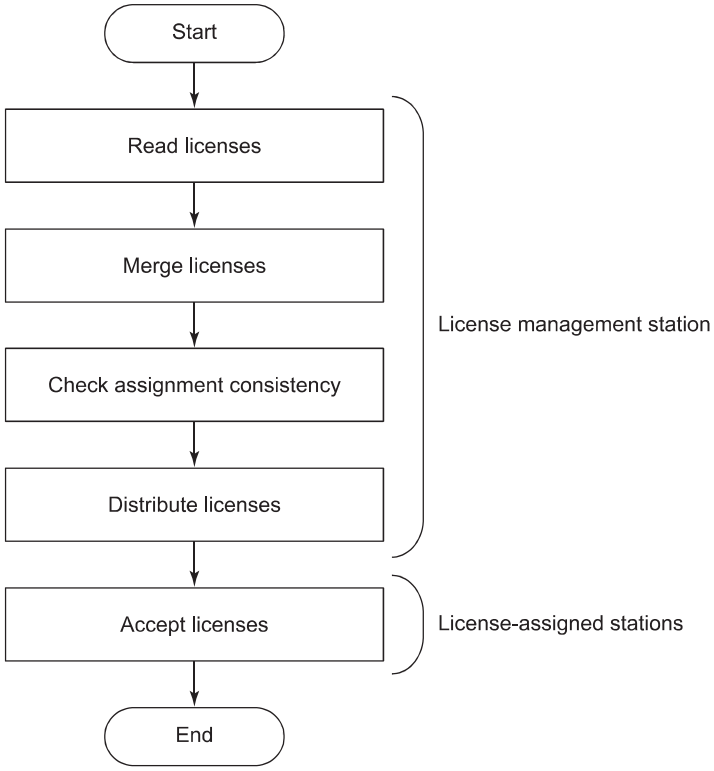


Figure 4.1-1 Procedures for Upgrading Licenses

SEE ALSO For more information about Upgrading the Licenses for Some HISs, refer to:

4.2, “Upgrading the Licenses for Some HISs” on page 4-5

Reading Licenses

Read the license key file to upgrade the license in the license management station that is upgraded to CENTUM VP R6 or ProSafe-RS R4.

The procedure to read the license key file into the license management station is same as the procedure to read the new license.

The following line is added to the package type in the license management. In the following explanation, we call the added line as a version upgrade license.

<old package type> => <new package type>

example: LHS1100-V10/N0099 => VP6H1100-V10N09

IMPORTANT

Retain the following license media after you upgrade licenses because you need it when you restore the licenses.

- The license medium that contains the old license key file.
- The license medium that contains the license key file to upgrade the old licenses

SEE ALSO For more information about reading licenses, refer to:

"■ Reading a license" on page 2-6

■ Merging Licenses

You need to merge licenses because version upgrade licenses cannot be distributed independently.

IMPORTANT

Licenses cannot be divided after they have been merged. Perform merging licenses very carefully.

To merge licenses, perform following procedures.

1. Run the license manager on the license management station as editing mode.
2. Assign the version upgrade licenses to the all stations that have been assigned with old licenses. The procedures to assign a version upgrade license is same as the procedures to assign a license.
3. From the menu bar, select [License] > [Merge version upgrade licenses].
   A dialog box to confirm packages appears.
4. Click [Yes].
   The old license and the version upgrade license is merged. You can confirm the merged license by package type.

A sample image of the license manager

Package type	Ver.	Qty	HIS1	HIS2	HIS3
LHS1100-V10/N0099	R5	3	1	1	1
LHS1100-V10/N0099 => VP6H1100-V10N09	R6	3			

Assigning the license

The image of the license manager that appears after assigning the license

Package type	Ver.	Qty	HIS1	HIS2	HIS3
LHS1100-V10/N0099	R5	3	1	1	1
LHS1100-V10/N0099 => VP6H1100-V10N09	R6	3	1	1	1

Merging the license

The image of the license manager that appears after merging the license

Package type	Ver.	Qty	HIS1	HIS2	HIS3
VP6H1100-V10N09	R6	3	1	1	1

Figure 4.1-2 Merging operation to upgrade licenses

TIP

If there are more than one licenses that is available to merge, you can merge only one group by one merging operation.

SEE ALSO

For more information about assigning licenses, refer to:

"■ Assigning licenses" on page 2-11

■ Assignment Consistency Check

Check the assignment consistency on the licenses that are upgraded.

The procedures to check the assignment consistency on the upgraded license is same as the checking on the license assignment.

IMPORTANT

Do not assign the different version of licenses on the same licenses-assigned station. If you assign a different version of license and check the consistency of assignment, an error message appears in the message display area on the license manager. Modify the assignment of licenses if an error message appears.

SEE ALSO

For more information about license assignment consistency check, refer to:

2.6, "Checking license assignment consistency" on page 2-12

■ Distributing Licenses

Distribute the upgraded licenses to the license-assigned stations.

The procedures to distribute the upgraded license is same as the procedures to distribute new licenses.

SEE ALSO

For more information about distributing licenses to license-assigned stations through a network, refer to:

"■ Distributing a license to license-assigned stations through a network" on page 2-13

For more information about distributing license by using external storage media, refer to:

"■ Distributing licenses by using external storage media" on page 2-16

■ Accepting Licenses

Accept upgraded licenses on the license-assigned stations.

The procedures to accept the upgraded license is same as the procedures to accept new licenses.

SEE ALSO

For more information about accepting licenses, refer to:

"■ Accepting a license and activating a software package on a license-assigned station" on page 2-15

For more information about accepting licenses by using external storage media, refer to:

"■ Activating a software package using external storage media" on page 2-17

4.2 Upgrading the Licenses for Some HISs

This section describes how to upgrade the licenses for some HISs.

For example, if you want to mix HISs with CENTUM VP R5 and R6 in a license project, upgrade the license to R6 for the number of the stations that have been upgraded to CENTUM VP V6. And distribute the upgraded licenses to HISs that are upgraded to CENTUM VP R6.

IMPORTANT

With CENTUM VP, one license project cannot have mixed non-HIS stations to which R5 and R6 licenses are assigned. With ProSafe-RS, one license project cannot have mixed SENGs to which R3 and R4 licenses are assigned.

Upgrading the Licenses for Some HISs

The procedures to upgrade license for some HISs is same as the procedure to upgrade whole licenses. However, note that the version upgrade license must be assigned to the station whose license is to be upgraded.

The following figure shows an example of upgrading the licenses for some HISs.

A sample image of the license manager

Package type	Ver.	Qty	HIS1	HIS2	HIS3
LHS1100-V10/N0099	R5	3	1	1	1
LHS1100-V10/N0099 => VP6H1100-V10N09	R6	2			

↓ Assigning the license to HIS1 and HIS2

The image of the license manager that appears after assigning the license

Package type	Ver.	Qty	HIS1	HIS2	HIS3
LHS1100-V10/N0099	R5	3	1	1	1
LHS1100-V10/N0099 => VP6H1100-V10N09	R6	2	1	1	

↓ Merging the license

The image of the license manager that appears after merging the license

Package type	Ver.	Qty	HIS1	HIS2	HIS3
LHS1100-V10/N0099	R5	1			1
VP6H1100-V10N09	R6	2	1	1	

Figure 4.2-1 Upgrading partial licenses

If you upgrade the licenses for some HISs, the available license number to be upgraded is up to the quantity of the version upgrade licenses.

After upgrading the licenses for some HISs, continue working on the procedure from "Assignment Consistency Check" according to the procedure of upgrading the license.

SEE ALSO

For more information about the process for license upgrading, refer to:

4.1, “Process for License Upgrading” on page 4-2

For more information about the version upgrade license, refer to:

“■ Reading Licenses” on page 4-2

5. Working with upgrade licenses

An upgrade license is required to upgrade a product. You can install the issued product medium before the expiry date of upgrade licenses.

The following operations differs from the software license operations:

- Addition
- Distribution and acceptance
- Deletion
- Moving

  You cannot move upgrade licenses across license projects.

■ Adding upgrade licenses

You should add an upgrade license when reading a new upgrade license or when extending the expiry date of an upgrade license.

TIP

When installing a software that was issued after the upgrade license is expired, first make sure to add an upgrade license with a new expiry date. Expiry date is extended.

SEE ALSO

For more information about adding upgrade licenses, refer to:

"■ Reading a license" on page 2-6

■ Distributing and accepting upgrade licenses

When you upgrade the following products, distribute and accept the upgrade licenses before you install the new revision of the software:

- CENTUM VP R6.04 or later
- ProSafe-RS R4.03 or later

TIP

- When you distribute only the upgrade licenses through a network, the licenses are accepted automatically.
- Upgrade licenses can be distributed even after the expiry date.

SEE ALSO

For more information about distributing and accepting licenses through a network, refer to:

2.7, "Distributing and accepting licenses through a network" on page 2-13

For more information about distributing and accepting licenses using external storage media, refer to:

2.8, "Distributing and accepting licenses using external storage media" on page 2-16

■ Deleting upgrade licenses from a license project

You can delete upgrade licenses from the license project if they are not assigned to any stations.

The procedure is the same as that for deleting software package licenses.

SEE ALSO

For more information about deleting software package licenses, refer to:

3.9.5, "Deleting software package licenses from a license project" on page 3-34

Appendix 1. Items checked in the license assignment consistency check

The following tables list and describe the items checked for each license or station.

Table Appendix 1-1 Items checked for each license

Checked item	Description
Excess assignment	Checks that the total number of licenses assigned to each station does not exceed the number of licenses available in the license project.
PJTCOM definition	Checks whether PJTCOM has been defined if a Project I/O License is assigned.
Quantity of assigned Project I/O License	Checks whether the quantity of the Project I/O License that is assigned to PJTCOM matches the quantity of the Project I/O License that is provided.

Table Appendix 1-2 Items checked for each station

Checked item	Description
Station properties	Checks whether there are any mistakes in the following station properties: Input range Setting category Station identification conditions
Dependency	Checks that all required package types have been assigned to software packages that need to be assigned together at the same time.
Exclusion	Checks that package types with exclusion relationships have not been assigned to the same station.
Packages that can be assigned	Checks that there are no package types that cannot be assigned to the station type.
Expired licenses	Checks that expired licenses have not been assigned.
Merge license	Checks that any upgrade installation license, version upgrade license, or replacement license has not been assigned independently.
Exceeded assignment limit	Checks whether the number of assigned licenses has exceeded the number of licenses that can be assigned to one station.
Redundant station	Checks that the assignment details are the same on the first station and the second station.
Version number identification	Checks that no license that has inconsistent version number has been assigned in a station

SEE ALSO

For more information about PJTCOM, refer to:

"■ Station name and computer name default values" on page 2-9

For more information about upgrade installation license, refer to:

3.5, "Increasing the software package capacity" on page 3-17

For more information about version upgrade license, refer to:

"■ Reading Licenses" on page 4-2

For more information about replacement licenses, refer to:

Appendix 4., "Upgrading licenses of CENTUM VP R5 software packages" on page App.4-1

Appendix 2. Displaying the status of assigned licenses on a license-assigned station

Displaying the status of assigned licenses on a License Manager

When you open License Manager on a license-assigned station, the license project window for the local station appears.
The status of the local station appears in the summary information area. The displayed items and corresponding responses are as follows:

Table Appendix 2-1 Status and response

Status	Description	Response
Error	Number of stations with a license error	Check the details of the license error.
Expired	Number of stations with an expired license	Check the expired licenses.
DueToExpire	Number of stations with licenses that will expire in 30 days or less	Check the licenses that will expire in 30 days or less.
AckWait	Number of stations waiting for license acceptance	Accept the distributed licenses.

Displaying the status of assigned licenses in the task tray

An icon that indicates the status of assigned licenses for the local station appears in the task tray.
The icons displayed in the task tray and the corresponding responses are as follows:

Table Appendix 2-2 Icons and responses

Icon	Description	Response
	Licenses have been assigned successfully (The status in Monitoring mode is OK).	—
	There is an error in the license. (a status of either Error, Expired, or NoLicense in Monitoring mode)	Check the details of the license error.
	The licenses will expire in 30 days or less (the status in Monitoring mode is DueToExpire).	Check the licenses that will expire in 30 days or less.
	Licenses have been distributed and are waiting to be accepted. Licenses have currently been assigned successfully (The status in Monitoring mode is OK).	Accept the distributed licenses.
	Licenses have been distributed and are waiting to be accepted. There is currently an error in the license. (a status of either Error, Expired, or NoLicense in Monitoring mode)	Accept the distributed licenses.
	Licenses have been distributed and are waiting to be accepted. The licenses will expire in 30 days or less (the status in Monitoring mode is DueToExpire).	Accept the distributed licenses.

Displaying the status of assigned licenses in the HIS system message banner

The status of assigned licenses for the local station appears in the system status icon display area of the HIS system message banner. If there is a license error or warning, or if a license is waiting for acceptance, an icon appears.
The following example shows the status of assigned licenses displayed in the HIS system message banner.

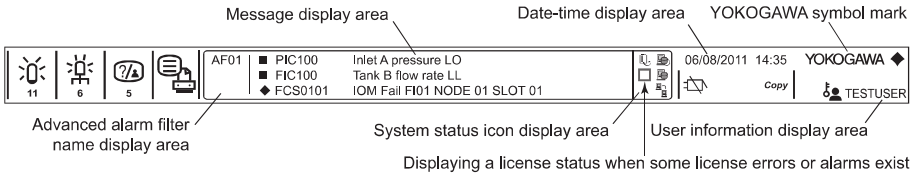


Figure Appendix 2-1 Example of the HIS system message banner display

The icons displayed in the system status icon display area and the corresponding responses are as follows:

Table Appendix 2-3 Icons and responses

Icon	Description	Response
No display	Licenses have been assigned successfully.	-
	There is an error in the license.	Check the details of the license error.
	The licenses will expire in 30 days or less.	Check the licenses that will expire in 30 days or less.
	Licenses have been distributed and are waiting to be accepted. Licenses have currently been assigned successfully.	Accept the distributed licenses.
	Licenses have been distributed and are waiting to be accepted. There is currently an error in the license.	Accept the distributed licenses.
	Licenses have been distributed and are waiting to be accepted. The licenses will expire in 30 days or less.	Accept the distributed licenses.

Appendix 3. Messages

The format for messages is as follows:

Station name (STNddss) message

Example: STN0164 License is not Accepted

The messages that appear on the station and the corresponding responses are as follows:

Table Appendix 3-1 Messages and corresponding responses

Message	Meaning	Action
STNddss License is not Accepted	A distributed license is not accepted.	Start the license manager and accept the license.
STNddss Cannot Restart. License Expired (VP6H1100, VP6H1120)	The license expired. If you restart the station, the correspondent package will not work.	Renew the license or remove the station assignment.
STNddss Cannot Restart from 2015/12/22. License will Expire (VP6H1100, VP6H1120)	If you restart the station on 2015/12/22 or after, the correspondent package will not work. The warning message appears 30 days before the license expiration date.	Renew the license or remove the station assignment.
STNddss License Error (License is Invalid)	The license information is not correct.	Redistribute the license.
STNddss License Error (Different from License Manager)	The license information on local station and on license management station is not consistent.	Redistribute the license.
STNddss License Error (Duplication with STNxxxx)	The license for STNddss station is distributed to multiple stations.	Redistribute the license.
STNddss License Error (ProjectID1 and ProjectID2(STNxxxx) are detected)	Licenses with different project IDs were assigned to stations (*1)in the same system. For example, STNddss was assigned with licenses for ProjectID1, while STNxxxx was assigned with licenses for ProjectID2. ProjectID1: The project ID of the license project for the local station. ProjectID2: The project ID of the license project for the other station. STNxxxx: Name of the station (or computer) that uses a different project ID from the local station.	Check whether the licenses in the same project have the same project ID.

*1: This refers to all computer-based stations that are defined in System View as well as in license projects.

Appendix 4. Upgrading licenses of CENTUM VP R5 software packages

This section describes how to upgrade licenses of CENTUM VP R5 software packages. For example, if you want to replace LHM1101 Standard Operation and Monitoring Functions (for CENTUM VP Small) to LHS1100 Standard Operation and Monitoring Functions, you need to upgrade the license LHM1101 to LHS1100. The basic workflow to upgrade the license is same as the workflow to upgrade the license. However, after having accepted the license on the license-assigned station, restart the station.

On the license management station of CENTUM VP R6, read the license key file from the license medium to upgrade the licenses. The following line is added to the package type in the license management. In the following explanation, we call the added line as a replacement license.

<old package type> => <new package type>

Example: LHM1101-V10/N0064 => LHS1100-V10/N0099

Merge the old license and replacement license to upgrade the license. Distribute the upgraded licenses to the license-assigned stations.

IMPORTANT

Retain the following license media after you upgrade licenses because you need it when you restore the licenses.

- The license medium that contains the old license key file.
- The license medium that contains the license key file to upgrade the old licenses

SEE ALSO For more information about basic workflow for license upgrading, refer to:

4.1, “Process for License Upgrading” on page 4-2

Upgrading licenses

When you upgrade licenses by merging old licenses and replacement licenses, perform following procedures.

IMPORTANT

Licenses cannot be divided after they have been merged. Perform merging licenses very carefully.

1. On the license management station of CENTUM VP R6, read the license key file from the license medium to upgrade the licenses. The procedure to read the license key file into the license management station is same as the procedure to read the new license.
2. Run the license manager on the license management station as editing mode.

3. Assign a replacement license to the station in which the license needs to be upgraded. The procedures to assign a replacement license is same as the procedures to assign a license.
4. From the menu bar, select [License] > [Merge version upgrade licenses]. A dialog box to confirm packages appears.
5. Click [Yes]. The old license and the replacement license are merged. You can confirm the merged license by package type.

A sample image of the license manager

Package type	Ver.	Qty	HIS1	HIS2	HIS3
LHM1101-V10/N0064	R5	3	1	1	1
LHM1101-V10/N0064 => LHS1100-V10/N0099	R5	2			

Assigning the license to HIS1 and HIS2

The image of the license manager that appears after assigning the license

Package type	Ver.	Qty	HIS1	HIS2	HIS3
LHM1101-V10/N0064	R5	3	1	1	1
LHM1101-V10/N0064 => LHS1100-V10/N0099	R5	2	1	1	

Merging the license

The image of the license manager that appears after merging the license

Package type	Ver.	Qty	HIS1	HIS2	HIS3
LHM1101-V10/N0064	R5	1			1
LHS1100-V10/N0099	R5	2	1	1	

Figure Appendix 4-1 Upgrading licenses

6. Check the assignment consistency on the licenses that are upgraded. The procedures to check the assignment consistency on the upgraded license is same as the checking on the license assignment.
7. Distribute the upgraded licenses to the license-assigned stations.

SEE ALSO

For more information about reading licenses, refer to:

"■ Reading a license" on page 2-6

For more information about assigning licenses, refer to:

"■ Assigning licenses" on page 2-11

For more information about license assignment consistency check, refer to:

2.6, "Checking license assignment consistency" on page 2-12

For more information about distributing modified licenses, refer to:

3.2.2, "Distributing modified licenses" on page 3-7

For more information about accepting modified licenses, refer to:

3.2.3, "Accepting modified licenses" on page 3-9

Revision information

Document name : License Management Guide

Document no. : IM 32P01C60-01EN

Dec. 2023/8th Edition/R4.10 or later

3.6	Updated steps in “■ Restoring a license project on another license management station.”

Feb. 2021/7th Edition/R4.06

2.2	Updated descriptions and added information about switching method of license project display.
2.4	Updated description of when using virtual test functions.

Dec. 2019/6th Edition/R4.05

Introduction	Updated description of registered trademarks and trademarks.
1.1.2, 2.4	Added UACS station.

Aug. 2018/5th Edition/R4.04

Introduction	Changed descriptions of registered trademarks of YOKOGAWA.
1.1.1	Added information about PRM.
5	Added information about additional methods of upgrade licenses.

Oct. 2017/4th Edition/R4.03.10

Entire manual	Updated expressions of the products managed in license management.
1.1	Updated descriptions.
1.2.4	Added information about upgrade licenses.
3.9.5	Updated expressions.
5	Added information about upgrade licenses.

May 2017/3rd Edition/R4.03

Introduction	Deleted Windows Vista from Trademark Acknowledgments.
1.1, 1.2	Added information about upgrade licenses.
3	Added information about software licenses.
4	Added information about version upgrade licenses.
5	Added information about application of upgrade licenses.

Oct. 2016/2nd Edition/R4.02

Entire manual	Changed the symbols that indicate warning and caution.
Introduction	Updated descriptions in "■ Safety, Protection, and Modification of the Product," "■ Symbols," and "■ Trademark Acknowledgments." Added a new term in "■ Full Names and Simplified Terms."
1.1.1	Added descriptions related to license management for iDefine.
2.4	Added information about UGS2.
2.11	Newly added.
2.12	Changed the section number from 2.11. Changed "redundant station" to "network switchover type redundant UGS."
3.9.1	Added information about UGS2.

Appendix 3 Corrected an error.

Dec. 2015/1st Edition/R4.01

Newly published

■ For Questions and More Information Online Query: A query form is available on the following URL for online query. http://www.yokogawa.com/iss
■ Written by Yokogawa Electric Corporation
■ Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Attachment 9.6 ProSafe-RS Security Guide

IM32P01C70-01EN

User's
Manual

ProSafe-RS
ProSafe-RS Lite

ProSafe-RS
Security Guide

IM 32P01C70-01EN

YOKOGAWA
Yokogawa Electric Corporation

IM 32P01C70-01EN
10th Edition

Introduction

This manual is a guide for implementing security measures in the ProSafe-RS system from a viewpoint of information technology (IT).

It explains security models and setting details of ProSafe-RS. Please read this manual to learn about the details of security settings.

The intended readers of this manual are engineers who examine construction and operation of the ProSafe-RS system.

10th Edition : Dec. 2023 (YK)
All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Safety Precautions for Use

Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Be sure to confirm the specifications and required settings of the devices that are used in combination with the Product by referring to the instruction manual or other documents of the devices.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:



Indicates that caution is required. This symbol for the Product indicates the possibility of dangers such as electric shock on personnel and equipment, and also indicates that the user must refer to the User’s Manuals for necessary actions. In the User’s Manuals, this symbol is used together with a word “CAUTION” or “WARNING” at the locations where precautions for avoiding dangers are described.

<French> Signale qu’il faut faire preuve de prudence. Ce symbole pour le produit signale la possibilité d’un danger pour le personnel et l’équipement comme un choc électrique, et signale également que l’utilisateur doit se référer au Manuel de l’utilisateur afin de prendre les mesures nécessaires. Dans le Manuel de l’utilisateur, ce symbole est utilisé conjointement avec la mention «CAUTION» ou «WARNING» aux endroits où sont décrites les précautions pour éviter les dangers.



Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.

<French> Signale qu'il faut faire preuve de prudence avec la surface brûlante. Les appareils sur lesquels est apposé ce symbole risquent de devenir brûlants. Tout contact physique ou matériel avec ces appareils risque de provoquer des brûlures ou des dommages.



Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.



Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.

~ Indicates an AC supply.

⎓ Indicates a DC supply.

| Indicates that a component such as a power supply switch is turned ON.

○ Indicates that a component such as a power supply switch is turned OFF.

Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

Warning and Disclaimer

- Except as specified in the warranty terms, YOKOGAWA shall not provide any warranty for the Product.
- YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Product.

Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the Software Product's merchantability or suitability for any particular purpose, except as specified in the warranty terms.
- Purchase the appropriate number of licenses of the Software Product according to the number of computers to be used.
- No copy of the Software Product may be made for any purpose other than backup; otherwise, it is deemed as an infringement of YOKOGAWA's Intellectual Property rights.
- Keep the software medium of the Software Product in a safe place.
- No reverse engineering, reverse compiling, reverse assembling, or converting the Software Product to human-readable format may be performed for the Software Product.
- No part of the Software Product may be transferred, converted, or sublet for use by any third-party, without prior written consent from YOKOGAWA.

Documentation Conventions

Symbols

The following symbols are used in the User's Manuals.

 WARNING	Indicates precautions to avoid a danger that may lead to death or severe injury.
 CAUTION	Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.
IMPORTANT	Indicates important information required to understand operations or functions.
TIP	Indicates additional information.
	Indicates referenced content. In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

Typographical Conventions

The following typographical conventions are used throughout the User's Manuals.

Commonly Used Conventions throughout the User's Manuals

- Δ Mark
  Indicates that a space must be entered between character strings.
  Example:

  ```
  .ALΔPIC010Δ-SC
  ```

- Character string enclosed by braces { }
  Indicates character strings that may be omitted.

  Example:

  ```
  .PRΔTAG{Δ.sheet name}
  ```

Conventions Used to Show Key or Button Operations

- Characters enclosed by brackets [ ]
  When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a button name in a window, or an item in a list box displayed in a window.

  Example:

  To alter the function, press the [ESC] key.

Conventions of a User-defined Folder

- User-defined folder name enclosed by parenthesis ( )
  User definable path is written in a pair of parentheses.

  Example:

  ```
  (RS Project Folder)\SCS0101
  ```

If the RS Project Folder is `C:\MYRSPJT`, the above path becomes `C:\MYRSPJTSCS0101`.

Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.
If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

Definitions of Node and Module Terms

In the User's Manuals, nodes and modules are referred to by using collective terms, another terms, or abbreviations based on the following definitions:

- Definitions of nodes
  - Node: A node is a collective term for an FIO node and an N-IO node.
  - FIO node: This is a collective term for a safety control unit, a safety node unit, and a unit for optical ESB bus repeater module.
  - CPU node: This is another term for a safety control unit. The abbreviation of safety control unit is SCU.
  - I/O node: This is another term for a safety node unit. The abbreviation of safety node unit is SNU.
  - N-IO node: This is a collective term for a node interface unit and an N-IO I/O unit. The abbreviation of node interface unit is NIU.
- Definitions of modules
  - I/O module: This is a collective term for an FIO I/O module and an N-IO I/O module.
  - FIO I/O module: This is a collective term for an analog I/O module and a digital I/O module for FIO, and a communication module.
  - N-IO I/O module: This is a collective term for the modules that can be mounted on an N-IO I/O unit.
  - AIO/DIO module: This is a collective term for an analog I/O module, a digital I/O module, and a universal type I/O module.
  - Analog I/O module: This is a collective term for an analog input module and an analog output module.
  - Digital I/O module: This is a collective term for a digital input module and a digital output module.
  - Universal type I/O module: This is a collective term for the I/O modules for which the channel signal category can be changed by software.

- Input module: This is a collective term for an analog input module, digital input module, and a universal type I/O module with defined input channels.
- Output module: This is a collective term for an analog output module, digital output module, and a universal type I/O module with defined output channels.
- Communication module: This is a collective term for a serial communication module, an Ethernet communication module, and a fire and gas communication module.

Full Names and Simplified Terms

In the User's Manuals, simplified terms listed in the following table are used.

Table Info-1 Full Names and Simplified Terms

Full Name	Simplified Term
Automation Design Suite	AD Suite
Automation Design Organizer	AD Organizer
Automation Design Server	AD Server
Automation Design project	AD project
Automation Design Master Database	ADMDB
Automation Design Suite Administration Tool	ADS Administration Tool
iDefine for ProSafe-RS	iDefine
Modification Package	ModPack
SCSV1-S (SCS supporting the SSC10S/SSC10D safety control units)	SCSV1
SCSP1-S (SCS supporting the SSC50S/SSC50D safety control units)	SCSP1
SCSP2-S (SCS supporting the SSC60S/SSC60D safety control units)	SCSP2
SCSP3-S (SCS supporting the S2SC70S/S2SC70D safety control units)	SCSP3
SCSL2-S (SCS supporting the L1SC70S/L1SC70D safety control units)	SCSL2
SCSU1-S (SCS supporting the SSC57S/SSC57D safety control units)	SCSU1

Copyright and Trademark Notices

All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, PRM, Exaopc, FieldMate Validator, and STARDOM are registered trademarks or trademarks of Yokogawa Electric Corporation.
- The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

ProSafe-RS Security Guide

IM 32P01C70-01EN 10th Edition

CONTENTS

1. Overview....1-1
   - 1.1 Security Threats to be Handled....1-3
   - 1.2 Security Measures....1-4
2. Security Models....2-1
   - 2.1 Overview of Security Models....2-2
   - 2.2 User/Group Management....2-14
     - 2.2.1 User Management Methods....2-15
     - 2.2.2 User Authentication Modes....2-16
     - 2.2.3 User/Group Management....2-17
3. Details of Security Measures....3-1
   - 3.1 Access Control....3-2
     - 3.1.1 Access Permissions to Files and Folders....3-3
     - 3.1.2 Package Configuration and Users/Groups....3-7
     - 3.1.3 Registry Configuration and User/Group....3-11
     - 3.1.4 DCOM (OPC) and User/Group....3-13
     - 3.1.5 Local Security and User/Group....3-14
   - 3.2 Personal Firewall Tuning....3-15
   - 3.3 Stopping Unused Window Services....3-18
   - 3.4 IT Environment Settings Common to IT Security Versions 2.0 and 1.0....3-22
     - 3.4.1 Disabling NetBIOS over TCP/IP....3-23
     - 3.4.2 HDD Password Function by BIOS....3-24
   - 3.5 Group Policy Settings Common to IT Security Versions 2.0 and 1.0....3-25
     - 3.5.1 Disabling the Built-in Administrator Account or Changing its User Name....3-26
     - 3.5.2 Applying the Software Restriction Policies....3-27
     - 3.5.3 Applying the Audit Policy....3-29
     - 3.5.4 Applying the StorageDevicePolicies Function....3-30
     - 3.5.5 Disabling USB Storage Devices....3-31
     - 3.5.6 Applying the Account Lockout Policy....3-33
     - 3.5.7 Windows Update Delivery Optimization....3-34
     - 3.5.8 Disabling Windows Defender....3-35
     - 3.5.9 Disabling Shared experiences....3-36

3.5.10 Enabling SMB Signing....3-37
3.5.11 Prevent illegal dll from loading....3-38
3.6 Group Policy Settings in IT Security Version 2.0....3-39
3.6.1 Applying the Password Policies....3-40
3.6.2 User Rights Assignment....3-41
3.6.3 Security Options....3-42
3.6.4 Advanced Audit Policy Configuration....3-44
3.6.5 Administrative Template....3-47
3.6.6 User Configuration - Administrative Template....3-55
3.7 Group Policy Settings in IT Security Version 1.0....3-56
3.7.1 Hiding the Last Logon User Name....3-57
3.7.2 Applying AutoRun Restrictions....3-58
3.7.3 Changing the LAN Manager Authentication Level....3-59
3.7.4 Applying the Password Policies....3-60
4. Selection of Security Functions....4-1
4.1 Items to be Considered Before Setting Security Functions....4-2
5. Precautions on Operations....5-1
5.1 Windows Account Management....5-2
5.1.1 Common Account Management....5-3
5.1.2 Individual Account Management....5-4
5.1.3 Common Precautions for Common Account Management/Individual Account Management....5-5
5.2 Related Programs....5-6
5.3 Measures for Secure Use....5-7
6. Utility Programs for Security Settings....6-1
6.1 IT Security Tool....6-2
6.2 Domain Link Management Tool....6-5
6.3 Setting the IT security....6-10
6.4 Changing the IT Security Settings....6-11
6.4.1 SENG PC, Computer Installed with Only AD Server, or Computer Dedicated to License Management....6-12
6.4.2 For File Server or Domain Controller....6-19
6.4.3 Applying the IT Security Version 2.0 Settings to a File Server or Domain Controller....6-27
6.5 Saving the IT Security Settings....6-28
6.5.1 SENG PC, Computer Installed with Only AD Server, or Computer Dedicated to License Management....6-29
6.5.2 Procedure for a File Server or Domain Controller....6-32
6.6 Restoring the IT Security Settings....6-33
6.6.1 SENG PC, Computer Installed with Only AD Server, or Computer Dedicated to License Management....6-34
6.6.2 Procedure for a File Server or Domain Controller....6-36
6.7 Changing the Security Setting File Password....6-37

6.7.1 SENG PC, Computer Installed with Only AD Server, or Computer Dedicated to License Management....6-38
6.7.2 Procedure for a File Server or Domain Controller....6-40
6.8 Exporting/Importing the IT Security Setting File....6-41
6.8.1 Procedure to Export by Using the IT Security Tool....6-42
6.8.2 Procedure to Export by Using the ITSecuritySettingItemExport Tool....6-43
6.8.3 Procedure to Import by Using the IT Security Tool....6-44
6.9 Viewing the Information Configured by the IT Security Tool....6-45
6.10 Active Directory-Based Consolidated Management of IT Security Settings....6-46
6.10.1 Creating Group Policy Objects....6-47
6.10.2 Applying Group Policy Objects to an Organizational Unit....6-49
6.11 Other Utility Programs....6-51
6.11.1 CreateProSafeProcess....6-52
6.11.2 CreateLicenseProcess....6-53
6.11.3 CreateAdsProcess....6-54
6.11.4 CreateAdsAgent....6-55
6.11.5 YWVNETCreateVNTUser....6-56
6.11.6 CreateTISService....6-58
6.11.7 StorageDeviceCTL....6-59
6.11.8 ITSecuritySettingItemExport....6-61

ProSafe-RS Security Guide

IM 32P01C70-01EN 10th Edition

CONTENTS

Appendix

Appendix 1. IT Security Setting Items..... App.1-1

Appendix 1.1 IT Security Version 2.0.....App.1-2

Appendix 1.1.1 Setting Items for a Computer with ProSafe-RS Software Installed..... App.1-3

Appendix 1.1.2 Setting Items for a File Server or Domain Controller..... ..... App.1-12

Appendix 1.2 IT Security Version 1.0.....App.1-25

Appendix 1.2.1 Setting Items for a Computer with ProSafe-RS Software Installed..... App.1-26

Appendix 1.2.2 Setting Items for a File Server or Domain Controller..... ..... App.1-28

1. Overview

This manual is a guide for implementing security measures on the product and for its operation.

By operating the system with security measures implemented, the product is protected from existing and future security threats.

The security models described in this manual are based on general configuration of the product. You must consider engineering and operation practices when applying these models to the actual systems.

Security-related Terms Used in the Manual

The following table describes the security-related terms.

Table 1-1 Security-related Terms

Term	Explanation
IT security	Security measures considered based on given IT environment, in order to protect the system and fight against current and future security threats including cyber terrorism.
User authentication mode	A scheme that prescribes the method of managing Windows users and ProSafe-RS users. Two modes are available: Windows authentication mode and ProSafe authentication mode.
ProSafe authentication mode	One of user authentication modes. This mode manages ProSafe-RS users and their access permissions independently of the Windows management functions.
Windows authentication mode	One of user authentication modes. This mode links credentials of Windows users and ProSafe-RS users.
Kerberos authentication	The default authentication method of Windows domain and it is used in a domain environment where the server and client PCs are mixed for single sign on. Once a user is authenticated; the authentication will be valid for entire system.
Personal firewall	Firewall operating on PC and domain controller, including firewalls other than the Windows standard firewall.

Overview of ProSafe-RS

SENG/HMI and SCS are connected by Vnet/IP, and SENG/HMI is connected to Ethernet as needed.

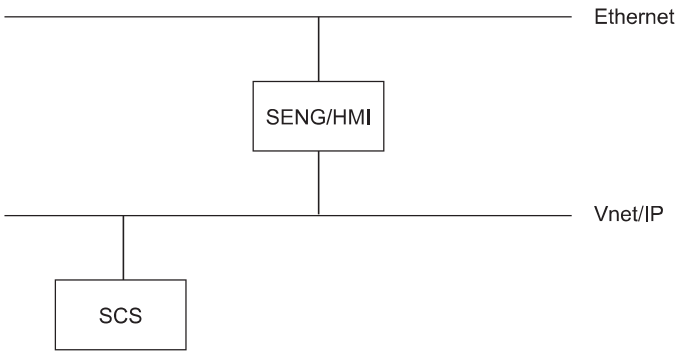


Figure 1-1 Overview of ProSafe-RS

Authentication and Access Control are performed on the SENG/HMI connected to the SCS. For this reason, SENG/HMI must have the security settings in this document. Also, take

measures such as using a switch or other device to prevent the computer from being inadvertently connected to the Ethernet or Vnet/IP to which the SENG/HMI is connected.

SEE ALSO For more information about the details of security measures, refer to:

Security Standard of System Product (TI 33Y01B30-01E)

1.1 Security Threats to be Handled

This section describes the security threats that the security functions of the product should deal with.

Security Threats

The security threats that can harm the ProSafe-RS system are as follows:

1. Attacks over the network
   Threats from individuals without any rights to the ProSafe-RS system via networks such as intranets, as well as the resultant threats of leakage of important data of the ProSafe-RS system.
2. Direct attacks through operation of SENG
   Threats where individuals without any rights to the ProSafe-RS system directly operate an SENG to affect the system and steal important data.
3. Theft of SENG or data.
   Threats where an SENG or data is stolen and important data is analyzed.

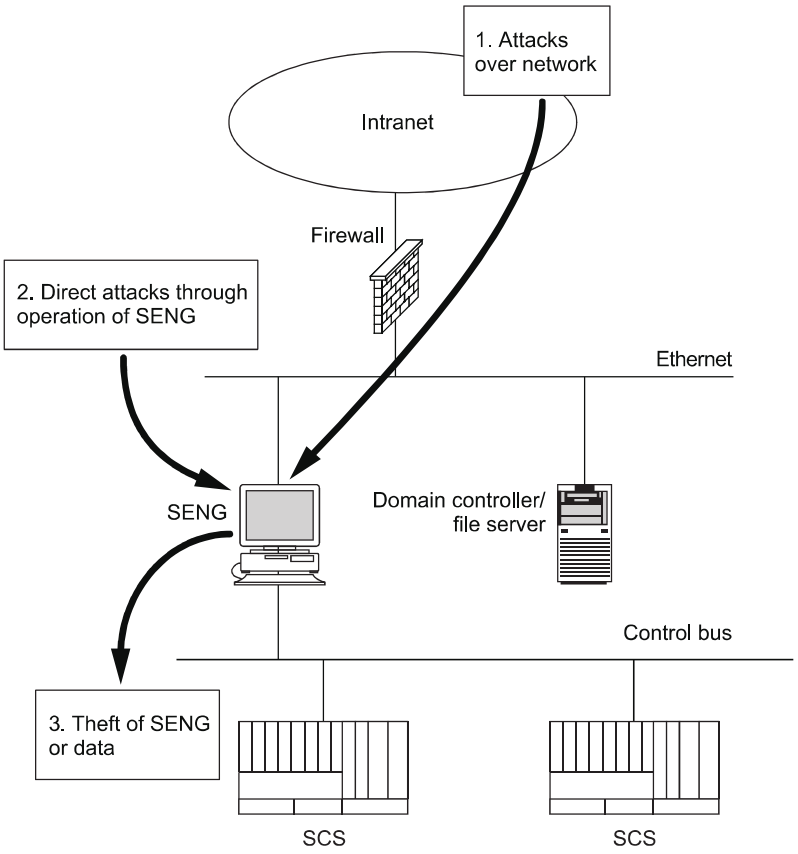


Figure 1.1-1 Security Threats

1.2 Security Measures

This section describes the security measures against security threats. Identify security measure items required for the product and, from among them, select the required security measures according to the level of security strength.

Security Measures and Handled Security Threats

In order to fight against security threats, we arranged security measures applied in security guides for each OS issued by Microsoft and general business network environment and optimized as a set of security measures for the product. Two IT security versions, 2.0 and 1.0, are available, which provide security measures that cover different ranges. These two versions are described as follows.

- IT security version 2.0
  This version was designed after reconsidering the IT security version 1.0 and includes more security measures. It supports the Standard and Strengthened security models.
- IT security version 1.0
  It supports the Legacy, Standard, and Strengthened security models.

IT security version 2.0 and IT security version 1.0 can coexist in the same project.

The following tables show the security measures and the threats that each measure handles for each security version.

[1]: Attacks over the network

[2]: Direct attacks by operation of SENG

[3]: Theft of SENG or data.

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0

Security measure	Threat handled		
	[1]	[2]	[3]
Password Policy-[Minimum password length]	Yes	Yes	No
Password Policy-[Minimum password age]	Yes	Yes	No
Password Policy-[Maximum password age]	Yes	Yes	No
Password Policy-[Enforce password history]	Yes	Yes	No
Disable ‘Password Policy-[Store passwords using reversible encryption]'	Yes	Yes	No
Password Policy-[Password must meet complexity requirements]	Yes	Yes	No
Access control for files and folders	Yes	Yes	No
Access control for product registry	Yes	Yes	No
Access control for DCOM (OPC) objects	Yes	Yes	No
Personal firewall tuning	Yes	No	No
Disable 'Personal Firewall-[Allow unicast response]’	Yes	No	No
Stopping unused Windows services	Yes	No	No
Account Lockout Policy-[Account lockout threshold]	Yes	Yes	No
Account Lockout Policy-[Reset account lockout counter after]	Yes	Yes	No
Account Lockout Policy-[Account lockout duration]	Yes	Yes	No
Disabling NetBIOS over TCP/IP	Yes	No	No

Continues on the next page

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0 (Table continued)

Security measure	Threat handled		
	[1]	[2]	[3]
Applying the StorageDevicePolicies function	No	Yes	Yes
Disabling USB storage devices	No	Yes	Yes
Applying the software restriction policies	Yes	Yes	No
User Rights Assignment-[Access this computer from the network]	No	Yes	No
User Rights Assignment-[Add workstations to domain]	Yes	Yes	No
User Rights Assignment-[Allow log on locally]	No	Yes	No
User Rights Assignment-[Deny log on locally]	No	Yes	No
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Yes	Yes	No
Security Options-[Devices: Prevent users from installing printer drivers]	No	Yes	No
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Yes	No	No
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Yes	No	No
Disable 'Security Options-[Domain controller: Allow server operators to schedule tasks]'	No	Yes	No
Disable 'Security Options-[Domain controller: Refuse machine account password changes]'	No	Yes	No
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Yes	No	No
Do not display user information 'Security Options-[Interactive logon: Display user information when the session is locked]'	No	Yes	No
Security Options-[Interactive logon: Do not display last user name]	No	Yes	No
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]'	No	Yes	No
Security Options-[Interactive logon: Machine inactivity limit]	No	Yes	No
Security Options-[Interactive logon: Prompt user to change password before expiration]	Yes	Yes	No
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Yes	No	No
Security Options-[Microsoft network server: Server SPN target name validation level]	Yes	No	No
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Yes	No	No
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Yes	No	No
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Yes	No	No
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Yes	No	No

Continues on the next page

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0 (Table continued)

Security measure	Threat handled		
	[1]	[2]	[3]
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Yes	No	No
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Yes	No	No
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Yes	No	No
Disable 'Security Options-[Network security: Allow LocalSystem NULL session fallback]'	Yes	No	No
Security Options-[Network security: Force logoff when logon hours expire]	No	Yes	No
Security Options-[Network security: LAN Manager authentication level]	Yes	No	No
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Yes	No	No
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Yes	No	No
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	No	Yes	No
Security Options-[User Account Control: Admin Approval Mode for the Built-in Administrator account]	No	Yes	No
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	No	Yes	No
Advanced Audit Policy Configuration-[Audit Credential Validation]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Security Group Management]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit User Account Management]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Process Creation]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Directory Service Access]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Directory Service Changes]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Account Lockout]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Logoff]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Logon]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Other Logon/Logoff Events]	Yes	Yes	No

Continues on the next page

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0 (Table continued)

Security measure	Threat handled		
	[1]	[2]	[3]
Advanced Audit Policy Configuration-[Audit Special Logon]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Removable Storage]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit IPsec Driver]	No	Yes	No
Advanced Audit Policy Configuration-[Audit Other System Events]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Security State Change]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Security System Extension]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit System Integrity]	Yes	Yes	No
Personalization-[Prevent enabling lock screen camera]	No	Yes	No
Personalization-[Prevent enabling lock screen slide show]	No	Yes	No
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services]	Yes	No	No
SCM-[Enable LSA Protection]	Yes	Yes	No
SCM-[Lsass.exe audit mode]	Yes	Yes	No
Group Policy-[Configure registry policy processing]	Yes	Yes	No
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Yes	No	No
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Yes	No	No
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Yes	No	No
Internet Communication settings-[Turn off printing over HTTP]	Yes	No	No
Internet Communication settings-[Turn off Search Companion content file updates]	Yes	No	No
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Yes	No	No

Continues on the next page

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0 (Table continued)

Security measure	Threat handled		
	[1]	[2]	[3]
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Yes	No	No
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Yes	No	No
Logon-[Do not display network selection UI]	Yes	Yes	No
Logon-[Do not enumerate connected users on domain-joined computers]	No	Yes	No
Logon-[Do not process the legacy run list]	No	Yes	No
Logon-[Do not process the run once list]	No	Yes	No
Disable 'Logon-[Enumerate local users on domain-joined computers]'	No	Yes	No
Logon-[Turn off app notifications on the lock screen]	No	Yes	No
Mitigation Options-[Untrusted Font Blocking]	Yes	Yes	No
Remote Procedure Call-[Enable RPC Endpoint Mapper Client Authentication]	Yes	Yes	No
User Profiles-[Turn off the advertising ID]	Yes	No	No
App Privacy-[Let Windows apps access account information]	Yes	No	No
App Privacy-[Let Windows apps access call history]	Yes	No	No
App Privacy-[Let Windows apps access contacts]	Yes	No	No
App Privacy-[Let Windows apps access email]	Yes	No	No
App Privacy-[Let Windows apps access location]	Yes	No	No
App Privacy-[Let Windows apps access messaging]	Yes	No	No
App Privacy-[Let Windows apps access motion]	Yes	No	No
App Privacy-[Let Windows apps access the calendar]	Yes	No	No
App Privacy-[Let Windows apps access the camera]	Yes	No	No
App Privacy-[Let Windows apps access the microphone]	Yes	No	No
App Privacy-[Let Windows apps access trusted devices]	Yes	No	No
App Privacy-[Let Windows apps control radios]	Yes	No	No
App Privacy-[Let Windows apps sync with devices]	Yes	No	No
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Yes	No	No
AutoPlay Policies-[Turn off Autoplay]	No	Yes	No
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	No	Yes	No
Data Collection and Preview Builds-[Allow Telemetry]	Yes	No	No
Data Collection and Preview Builds-[Do not show feedback notifications]	Yes	No	No
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Yes	Yes	No

Continues on the next page

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0 (Table continued)

Security measure	Threat handled		
	[1]	[2]	[3]
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Yes	Yes	No
Event Log Service(System)-[Specify the maximum log file size (KB)]	Yes	Yes	No
File Explorer-[Turn off heap termination on corruption]	No	Yes	No
HomeGroup-[Prevent the computer from joining a homegroup]	Yes	No	No
OneDrive-[Prevent the usage of OneDrive for file storage]	Yes	No	No
OneDrive-[Save documents to OneDrive by default] (Save documents to the local PC by default)	Yes	No	No
Remote Desktop Connection Client-[Do not allow passwords to be saved]	Yes	No	No
Device and Resource Redirection-[Do not allow drive redirection]	Yes	No	No
Security-[Always prompt for password upon connection]	Yes	No	No
Security-[Require secure RPC communication]	Yes	No	No
Security-[Require user authentication for remote connections by using Network Level Authentication]	Yes	No	No
Session Time Limits-[Set time limit for active but idle Remote Desktop Services sessions]	Yes	No	No
Sync your settings-[Do not sync Apps]	Yes	No	No
Sync your settings-[Do not sync start settings]	Yes	No	No
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Yes	No	No
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	No	Yes	No
Notifications-[Turn off toast notifications on the lock screen]	No	Yes	No
Disabling the built-in Administrator account or changing its user name	Yes	Yes	No
HDD password function by BIOS	No	No	Yes
Disabling Shared experiences	No	No	Yes
Enabling SMB signing	Yes	No	No
Prevent illegal dll from loading	Yes	No	No

Table 1.2-2 Security Measures and Handled Threats - IT security version 1.0

Security measure	Threat handled		
	[1]	[2]	[3]
Access control	Yes	Yes	No
Personal firewall tuning	Yes	No	No
Stopping unused Windows services	Yes	No	No

Continues on the next page

Table 1.2-2 Security Measures and Handled Threats - IT security version 1.0 (Table continued)

Security measure	Threat handled		
	[1]	[2]	[3]
Disabling the built-in Administrator account or changing its user name	Yes	Yes	No
Hiding the last logon user name	Yes	Yes	No
Applying the software restriction policies	Yes	Yes	No
Applying AutoRun restrictions	No	Yes	No
Applying the StorageDevicePolicies function	No	Yes	Yes
Disabling USB storage devices	No	Yes	Yes
Disabling NetBIOS over TCP/IP	Yes	No	No
Changing the LAN Manager authentication level	Yes	No	No
Applying the password policy	Yes	Yes	No
Applying the audit policy	Yes	Yes	No
Applying the account lockout policy	Yes	Yes	No
HDD password function by BIOS	No	No	Yes
Disabling Shared experiences	No	No	Yes
Enabling SMB signing	Yes	No	No
Prevent illegal dll from loading	Yes	No	No

2. Security Models

The product provides three types of security models, Legacy model, Standard model, and Strengthened model, according to the required security strength, in order to flexibly accommodate system configuration and operation. Required security measure items are incorporated in the security models.

2.1 Overview of Security Models

This section describes the features of security models and the relationship between security models and their corresponding security measures.

Security Models

The features of the three security models, Legacy model, Standard model, and Strengthened model, are as follows:

- Legacy model
  This model does not strengthen security. Use this model when you connect the system with YOKOGAWA products that do not support security measures.
- Standard model
  This model places importance on operation of the product and collaboration with other systems (Exaopc, CENTUM VP, and so on) and guards against "attacks over the network" and "direct attacks through operation of SENG." The Standard model does not guard against "theft of SENG or data" because this threat is considered not likely to happen to the product.
- Strengthened model
  This model takes all measures against any security treats. If all security measures are taken, operation and so on may be affected. Take measures according to the characteristics of each system for non-mandatory items.

IMPORTANT

Please consult YOKOGAWA if IT security of the Strengthened model is required.

Security Models and Security Measures

As a security measure for ProSafe-RS, the IT Security Tool is provided. Using the IT Security Tool, you can implement security measures on each computer.

If you want to implement consolidated security measures under a domain environment, you can also use the group policy objects (referred to as GPOs in this chapter) provided by YOKOGAWA together.

IMPORTANT

Even if you are intending to implement GPO file based security measures, you must configure the security settings by running the IT Security Tool in advance. Note that the security configuration by the GPO file overrides the security configuration by the IT Security Tool.

With security configuration using the IT Security Tool, settings of some security measure items differ, depending on the differences in the IT Security Tool version and the security model. In addition, some security measure items are configured for the purpose to match the product specification rather than to fight against security threats.

SEE ALSO For more information about security measures, refer to:

3., “Details of Security Measures” on page 3-1

For more information about creating a GPO file, refer to:

6.10.1, “Creating Group Policy Objects” on page 6-47

For more information about applying the GPO file, refer to:

6.10.2, “Applying Group Policy Objects to an Organizational Unit” on page 6-49

Security Measures to Fight Against Security Threats

The following table shows the security measure items against security threats and their configuration in IT security version 2.0.

“Defined/Not defined” in the Configuration by GPO file column indicates whether the security measure item is defined to be configured in the GPO file that is created based on the group policy provided by YOKOGAWA.

- Defined
  The security measure, which is adopted by YOKOGAWA, is defined in the GPO file.
- Not defined
  The security measure is not defined in the GPO file.

“Applied/Not applied” in the Configuration by IT Security Tool column indicates whether the security measure item is configured by the IT Security Tool, applying the predefined setting, for each security model.

- Applied
  The security measure, which is adopted by YOKOGAWA, is configured by the IT Security Tool so that it is applied.
- Not applied
  Because YOKOGAWA decided not to adopt the security measure, it is configured by the IT Security Tool so as not to be applied.

TIP The setting values set by the IT Security Tool can be changed by the user for some security measure items and cannot be changed for others. To find out which security measure items can be changed, refer to the appendix.

Table 2.1-1 Security Measures in IT Security Version 2.0

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Password Policy-[Minimum password length]	Defined	Not applied	Applied
Password Policy-[Minimum password age]	Defined	Not applied	Applied
Password Policy-[Maximum password age]	Defined	Not applied	Applied
Password Policy-[Enforce password history]	Defined	Not applied	Applied
Disable ‘Password Policy-[Store passwords using reversible encryption]'	Defined	Not applied	Applied
Password Policy-[Password must meet complexity requirements]	Defined	Not applied	Applied
Access control for files and folders (*1)	Not defined	Applied	Applied
Access control for product registry (*1)	Not defined	Applied	Applied
Access control for DCOM (OPC) objects (*1)	Not defined	Applied	Applied

Continues on the next page

Table 2.1-1 Security Measures in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Personal Firewall tuning (*2)	Not defined	Applied	Applied
Disable 'Personal Firewall-[Allow unicast response]'	Not defined	Applied	Applied
Stopping unused Windows services (*2)	Not defined	Not applied	Applied
Account Lockout Policy-[Account lockout threshold]	Defined	Not applied	Applied
Account Lockout Policy-[Reset account lockout counter after]	Defined	Not applied	Applied
Account Lockout Policy-[Account lockout duration]	Defined	Not applied	Applied
Disabling NetBIOS over TCP/IP (*1)	Not defined	Applied	Applied
Applying the StorageDevicePolicies function	Defined	Applied	Applied
Disabling USB storage devices	Defined	Applied	Applied
Applying the software restriction policies	Not defined	Applied	Applied
User Rights Assignment-[Add workstations to domain] (*3)	Not defined	Applied	Applied
User Rights Assignment-[Allow log on locally]	Not defined	Not applied	Applied
User Rights Assignment-[Deny log on locally]	Not defined	Applied	Applied
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Defined	Applied	Applied
Security Options-[Devices: Prevent users from installing printer drivers]	Defined	Applied	Applied
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Defined	Applied	Applied
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Defined	Applied	Applied
Disable 'Security Options-[Domain controller: Allow server operators to schedule tasks]' (*3)	Not defined	Applied	Applied
Disable 'Security Options-[Domain controller: Refuse machine account password changes]' (*3)	Not defined	Applied	Applied
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Defined	Applied	Applied
Do not display user information 'Security Options-[Interactive logon: Display user information when the session is locked]'	Defined	Not applied	Applied
Security Options-[Interactive logon: Do not display last user name]	Defined	Applied	Applied
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]'	Defined	Applied	Applied
Security Options-[Interactive logon: Prompt user to change password before expiration]	Defined	Applied	Applied
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Defined	Applied	Applied
Security Options-[Microsoft network server: Server SPN target name validation level]	(*4)	Applied	Applied
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Not defined	Applied	Applied

Continues on the next page

Table 2.1-1 Security Measures in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Not defined	Applied	Applied
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Not defined	Applied	Applied
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Defined	Applied	Applied
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Defined	Applied	Applied
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Defined	Applied	Applied
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Defined	Applied	Applied
Disable 'Security Options-[Network security: Allow Local System NULL session fallback]'	Defined	Applied	Applied
Security Options-[Network security: Force logoff when logon hours expire] (*3)	Not defined	Applied	Applied
Security Options-[Network security: LAN Manager authentication level]	Defined	Applied	Applied
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Defined	Applied	Applied
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Defined	Applied	Applied
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Defined	Applied	Applied
Security Options-[User Account Control: Admin Approval Mode for the Built-in Administrator account]	Defined	Applied	Applied
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Credential Validation]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Security Group Management]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit User Account Management]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Process Creation]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Directory Service Access] (*3)	Not defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Directory Service Changes] (*3)	Not defined	Applied	Applied

Continues on the next page

Table 2.1-1 Security Measures in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Advanced Audit Policy Configuration-[Audit Account Lockout]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Logoff]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Logon]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Other Logon/Logoff Events]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Special Logon]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Removable Storage]	Not defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit IPsec Driver] (*3)	Not defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Other System Events]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Security State Change]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Security System Extension]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit System Integrity]	Defined	Applied	Applied
Personalization-[Prevent enabling lock screen camera]	Defined	Applied	Applied
Personalization-[Prevent enabling lock screen slide show]	Defined	Applied	Applied
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services] (*5)	Defined	Applied	Applied
SCM-[Enable LSA Protection] (*5)	Defined	Not applied	Applied
SCM-[Lsass.exe audit mode] (*5)	Defined	Not applied	Applied
Group Policy-[Configure registry policy processing]	Defined	Applied	Applied
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Defined	Applied	Applied
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Defined	Applied	Applied

Continues on the next page

Table 2.1-1 Security Measures in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Defined	Applied	Applied
Internet Communication settings-[Turn off printing over HTTP]	Defined	Applied	Applied
Internet Communication settings-[Turn off Search Companion content file updates]	Defined	Applied	Applied
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Defined	Applied	Applied
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Defined	Applied	Applied
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Defined	Applied	Applied
Logon-[Do not display network selection UI]	Defined	Applied	Applied
Logon-[Do not enumerate connected users on domain-joined computers]	Defined	Applied	Applied
Logon-[Do not process the legacy run list]	Defined	Not applied	Applied
Logon-[Do not process the run once list]	Defined	Not applied	Applied
Disable 'Logon-[Enumerate local users on domain-joined computers]'	Defined	Applied	Applied
Logon-[Turn off app notifications on the lock screen]	Defined	Applied	Applied
Mitigation Options-[Untrusted Font Blocking]	Defined	Applied	Applied
Remote Procedure Call-[Enable RPC Endpoint Mapper Client Authentication]	Defined	Not applied	Applied
User Profiles-[Turn off the advertising ID]	Defined	Applied	Applied
App Privacy-[Let Windows apps access account information]	Defined	Applied	Applied
App Privacy-[Let Windows apps access call history]	Defined	Applied	Applied
App Privacy-[Let Windows apps access contacts]	Defined	Applied	Applied
App Privacy-[Let Windows apps access email]	Defined	Applied	Applied
App Privacy-[Let Windows apps access location]	Defined	Applied	Applied
App Privacy-[Let Windows apps access messaging]	Defined	Applied	Applied
App Privacy-[Let Windows apps access motion]	Defined	Applied	Applied
App Privacy-[Let Windows apps access the calendar]	Defined	Applied	Applied
App Privacy-[Let Windows apps access the camera]	Defined	Applied	Applied
App Privacy-[Let Windows apps access the microphone]	Defined	Applied	Applied
App Privacy-[Let Windows apps access trusted devices]	Defined	Applied	Applied
App Privacy-[Let Windows apps control radios]	Defined	Applied	Applied
App Privacy-[Let Windows apps sync with devices]	Defined	Applied	Applied
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Defined	Applied	Applied
AutoPlay Policies-[Turn off Autoplay]	Defined	Applied	Applied
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Defined	Applied	Applied

Continues on the next page

Table 2.1-1 Security Measures in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Data Collection and Preview Builds-[Allow Telemetry]	Defined	Applied	Applied
Data Collection and Preview Builds-[Do not show feedback notifications]	Defined	Applied	Applied
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Defined	Applied	Applied
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Defined	Applied	Applied
Event Log Service(System)-[Specify the maximum log file size (KB)]	Defined	Applied	Applied
File Explorer-[Turn off heap termination on corruption]	Defined	Applied	Applied
HomeGroup-[Prevent the computer from joining a homegroup]	Defined	Applied	Applied
OneDrive-[Prevent the usage of OneDrive for file storage]	Defined	Applied	Applied
OneDrive-[Save documents to OneDrive by default] (Save documents to the local PC by default)	Defined	Applied	Applied
Remote Desktop Connection Client-[Do not allow passwords to be saved]	Defined	Applied	Applied
Device and Resource Redirection-[Do not allow drive redirection]	Defined	Applied	Applied
Security-[Require secure RPC communication]	Defined	Applied	Applied
Security-[Require user authentication for remote connections by using Network Level Authentication]	Defined	Applied	Applied
Sync your settings-[Do not sync Apps]	Defined	Applied	Applied
Sync your settings-[Do not sync start settings]	Defined	Applied	Applied
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Defined	Applied	Applied
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Defined	Applied	Applied
Notifications-[Turn off toast notifications on the lock screen]	Defined	Applied	Applied
Disabling the built-in Administrator account or changing its user name	Not defined	Not applied	The IT Security Tool does not configure this setting. You must configure it manually.
HDD password function by BIOS (*1)	Not defined	Not applied	The IT Security Tool does not configure this setting. You must configure it manually.
Disabling Shared experiences	(*6)	Applied	Applied

Continues on the next page

Table 2.1-1 Security Measures in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Enabling SMB signing	Not defined	The IT Security Tool does not configure this setting. You must configure it manually.	The IT Security Tool does not configure this setting. You must configure it manually.
Prevent illegal dll from loading	Not defined	Configured by the installer.	Configured by the installer.

*1: This security setting item is not affected by group policy
*2: This setting can be controlled by group policy but can also be configured for each computer using the IT Security Tool.
*3: This setting is for domain controllers.
*4: This setting is not included in the GPO file which is provided for consolidated management using Active Directory because problems may occur on the computer in use depending on the OS and update application status.
*5: If you want to change the setting value in Active Directory-based consolidated management, select either “Enabled” or “Disabled” for this item.
*6: This setting is not included in the GPO file which is provided for consolidated management using Active Directory because the setting differs depending on the OS.

TIP

With IT security version 2.0, different security setting items are configured among stations, file server, and domain controller.

Security Measures to Match the Product Specification

The following table shows the security measure items to match the product specification and their configuration in IT security version 2.0.

“Defined/Not defined” in the Configuration by GPO file column indicates whether the security measure item is defined to be configured in the GPO file that is created based on the group policy provided by YOKOGAWA.

- Defined
  The security measure, which is adopted by YOKOGAWA, is defined in the GPO file.
- Not defined
  The security measure is not defined in the GPO file.

“Applied/Not applied” in the Configuration by IT Security Tool column indicates whether the security measure item is configured by the IT Security Tool, applying the predefined setting, for each security model.

- Applied
  The security measure, which is adopted by YOKOGAWA, is configured by the IT Security Tool so that it is applied.
- Not applied
  Because YOKOGAWA decided not to adopt the security measure, it is configured by the IT Security Tool so as not to be applied.

Table 2.1-2 Security Measures Configured to Match the Product Specification in IT Security Version 2.0

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
User Rights Assignment-[Create global objects]	Not defined	Applied	Applied
User Rights Assignment-[Log on as a batch job]	Not defined	Applied	Applied

Continues on the next page

Table 2.1-2 Security Measures Configured to Match the Product Specification in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
User Rights Assignment-[Log on as a service]	Not defined	Applied	Applied
[MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)]	Not defined	Applied	Applied
Security Options-[Network access: Let Everyone permissions apply to anonymous users]	Not defined	Applied	Applied
Security Options-[Network security: Do not store LAN Manager hash value on next password change]	Not defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit RPC Events]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Application Generated]	Defined	Applied	Applied
Disable 'Audit Process Creation-[Include command line in process creation events]'	Defined	Applied	Applied
Internet Communication settings-[Turn off access to the Store]	Defined	Applied	Applied
Video and Display Settings-[Turn Off the Display (On Battery)]	Defined	Applied	Applied
Video and Display Settings-[Turn Off the Display (Plugged In)]	Defined	Applied	Applied
Cloud Content-[Do not show Windows Tips]	Defined	Applied	Applied
Cloud Content-[Turn off Microsoft consumer experiences]	Defined	Applied	Applied
Data Collection and Preview Builds-[Disable pre-release features or settings]	Defined	Applied	Applied
Data Collection and Preview Builds-[Toggle user control over Insider builds]	Defined	Applied	Applied
Disable 'Search-[Allow Cortana]'	Defined	Applied	Applied
Search-[Don't search the web or display web results in Search]	Defined	Applied	Applied
Search-[Don't search the web or display web results in Search over metered connections]	Defined	Applied	Applied
Software Protection Platform-[Turn off KMS Client Online AVS Validation]	Defined	Applied	Applied
Store-[Turn off Automatic Download and Install of updates]	Defined	Applied	Applied
Store-[Turn off Automatic Download of updates on Win8 machines]	Defined	Applied	Applied
Store-[Turn off the offer to update to the latest version of Windows]	Defined	Applied	Applied
Store-[Turn off the Store application]	Defined	Applied	Applied
Windows Defender - [Turn off Windows Defender]	Defined	Applied	Applied
Delivery Optimization - [Download Mode]	(*1)	Applied	Applied

*1: This setting is not included in the GPO file which is provided for consolidated management using Active Directory because the setting differs depending on the OS.

Security Measures to Fight Against Security Threats

The following table shows the security measure items against security threats and their configuration in IT security version 1.0.

“Defined/Not defined” in the Configuration by GPO file column indicates whether the security measure item is defined to be configured in the GPO file that is created based on the group policy provided by YOKOGAWA.

- Defined
  The security measure, which is adopted by YOKOGAWA, is defined in the GPO file.
- Not defined
  The security measure is not defined in the GPO file.

“Applied/Not applied” in the Configuration by IT Security Tool column indicates whether the security measure item is configured by the IT Security Tool, applying the predefined setting, for each security model.

- Applied
  The security measure, which is adopted by YOKOGAWA, is configured by the IT Security Tool so that it is applied.
- Not applied
  Because YOKOGAWA decided not to adopt the security measure, it is configured by the IT Security Tool so as not to be applied.

TIP

The setting values set by the IT Security Tool can be changed by the user for some security measure items and cannot be changed for others. To find out which security measure items can be changed, refer to the appendix.

Table 2.1-3 Security Measures in IT Security Version 1.0

Security measure	Configuration by GPO file	Configuration by IT Security Tool		
		Legacy model	Standard model	Strengthened model
Access control (*1)	Not defined	Not defined	Applied	Applied
Personal firewall tuning	Not defined	Not applied	Applied	Applied
Stopping unused Windows services	Not defined	Not applied	Not applied	Applied
Disabling the built-in Administrator account or changing its user name	Not defined	Not applied	Not applied	The IT Security Tool does not configure this setting. You must configure it manually.
Hiding the Last Logon User Name	Defined	Applied	Applied	Applied
Applying the software restriction policies	Not defined	Not applied	Applied	Applied
Applying AutoRun restrictions	Defined	Applied	Applied	Applied
Applying the StorageDevicePolicies function	Defined	Not applied	Applied	Applied
Disabling USB storage devices	Defined	Not applied	Applied	Applied
Disabling NetBIOS over TCP/IP (*1)	Not defined	Not applied	Applied	Applied
Changing the LAN Manager authentication level	Defined	Not applied	Applied	Applied
Applying the password policy	Defined	Not applied	Not applied	Applied
Applying the audit policy	Defined (*2)	Not applied	Not applied	Applied
Applying the account lockout policy	Defined	Not applied	Not applied	Applied

Continues on the next page

Table 2.1-3 Security Measures in IT Security Version 1.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool		
		Legacy model	Standard model	Strengthened model
HDD password function by BIOS (*1)	Not defined	Not applied	Not applied	The IT Security Tool does not configure this setting. You must configure it manually.
Disabling Shared experiences	(*3)	Applied	Applied	Applied
Enabling SMB signing	Not defined	Not applied	The IT Security Tool does not configure this setting. You must configure it manually.	The IT Security Tool does not configure this setting. You must configure it manually.
Prevent illegal dll from loading	Not defined	Configured by the installer.	Configured by the installer.	Configured by the installer.

*1: This security setting item is not affected by group policy
*2: "Audit object access" is not included in the GPO file which is provided for consolidated management using Active Directory.
*3: This setting is not included in the GPO file which is provided for consolidated management using Active Directory because the setting differs depending on the OS.

Security Measures to Match the Product Specification

The following table shows the security measure items to match the product specification and their configuration in IT security version 1.0.

"Defined/Not defined" in the Configuration by GPO file column indicates whether the security measure item is defined to be configured in the GPO file that is created based on the group policy provided by YOKOGAWA.

- Defined
  The security measure, which is adopted by YOKOGAWA, is defined in the GPO file.
- Not defined
  The security measure is not defined in the GPO file.

"Applied/Not applied" in the Configuration by IT Security Tool column indicates whether the security measure item is configured by the IT Security Tool, applying the predefined setting, for each security model.

- Applied
  The security measure, which is adopted by YOKOGAWA, is configured by the IT Security Tool so that it is applied.
- Not applied
  Because YOKOGAWA decided not to adopt the security measure, it is configured by the IT Security Tool so as not to be applied.

Table 2.1-4 Security Measures Configured to Match the Product Specification in IT Security Version 1.0

Security measure	Configuration by GPO file	Configuration by IT Security Tool		
		Legacy model	Standard model	Strengthened model
Windows Defender - [Turn off Windows Defender]	Defined	Applied	Applied	Applied
Delivery Optimization - [Download Mode]	(*1)	Applied	Applied	Applied

*1: This setting is not included in the GPO file which is provided for consolidated management using Active Directory because the setting differs depending on the OS.

2.2 User/Group Management

This section describes the relationship between Windows user management types and the product. Access control is set for each user group explained in this section.

2.2.1 User Management Methods

Windows provides two methods of managing users: standalone management and domain management.

This product provides four methods of managing users: standalone management, domain management, combination management, and linked domain management. The following table shows the required configuration, operation, and feature of the user management methods for this product.

Table 2.2.1-1 User Management Methods

User management type	Required configuration	Operation	Feature
Standalone management	Configuration of the system built up with the product only.	Operated by registering user accounts used in each of all SENGs.	• Simple configuration not requiring domain controller. • Since account management is required for each PC, all PCs must be maintained at user account maintenance, making this method not suited for large-scale systems.
Domain management	Construction of domain controller is required in addition to the system built up with the product.	Operated by registering user accounts used to the domain controller.	Centralized management of users is possible, resulting in fewer human errors.
Combination management	Construction of domain controller is required in addition to the system built up with the product.	Operated the same way as for the domain management in normal operation.	Even if a domain controller is not available, continuous operation is possible by managing accounts of each computer.
Linked domain management	Construction of domain controller is required in addition to the system built up with the product.	Operated the same way as for the domain management in normal operation.	• Even if a domain controller is not available, continuous operation is possible by managing accounts of each computer. • IT security can be configured in two stages, before and after building the domain environment. (*1)

*1: After applying IT security of standalone management and joining the computer to the domain, add the corresponding domain groups to the members of the local groups for the products installed on the computer.

TIP

- The combination management and the linked domain management have the convenience that domain users or local users can access this product depending on the situation. A domain user can perform normal operation of the system configured with this product, and a local user can also perform system configuration and maintenance for each computer. Note that the domain user account is created by the domain administrator, and the local user account is created by the administrator of the computer on which this product is installed.
- The linked domain management is recommended when installing new software for this product because it is convenient to easily migrate from stand-alone management after adding to the domain. The domain management or the combination management is recommended when upgrading or performing additional installation without changing the management method.

2.2.2 User Authentication Modes

When the Access Control and Operation History Management package is used, two user authentication modes, Windows authentication and ProSafe authentication, are available in a ProSafe-RS system. These modes are called user authentication modes.

- Windows authentication mode
  Users are authenticated using Windows functions.
- ProSafe authentication mode
  Users are authenticated using specific functions of ProSafe-RS.

SEE ALSO For more information about user authentication mode setting, refer to:

- "■ ProSafe authentication mode and Windows authentication mode" in E2.1.1, "Overview of access control for engineers" in Engineer's Reference Manual (IM 32P04B10-01EN)
- "■ Specifying the user authentication mode" in E2.2.1, "Settings for access control" in Engineer's Reference Manual (IM 32P04B10-01EN)

2.2.3 User/Group Management

Users and groups are described as follows:

Combination of User Management and Security Model for Windows

Five types of method for creating a user/group are available, depending on the combination of the Windows user management and the security model.

- Type 1: Legacy Model
- Type 2: Standard Model / Strengthened Model - Standalone Management
- Type 3: Standard Model / Strengthened Model - Domain Management
- Type 4: Standard Model / Strengthened Model - Combination Management
- Type 5: Standard Model / Strengthened Model - Linked Domain Management

TIP

No matter what security model is applied, the ProSafe-RS installer creates a PSF_MAINTENANCE group and add the user who installed the ProSafe-RS software as a member of this group. Moreover, if domain management type, combination management type, or linked domain management type is used for user management, the PSF_MAINTENANCE group in the domain should be used.

IMPORTANT

When you create users or groups, do not use the following group names, which are reserved by the ProSafe-RS system:

- ADS_SERVICE
- ADS_SERVICE_LCL

IMPORTANT

- The initial password is set by default for the following predefined user accounts in this product. Be sure to change the password because operating with the initial password may increase the security risk.
  - PSF_PROCESS
  - LIC_PROCESS
  - ADS_PROCESS
  - CTM_PROCESS
  - ADS_AGENT
- The password for the above user accounts is reset to the default password when this product is installed for upgrading its version or revision. Be sure to change the password before operating. The password is not reset to the default password by configuring with the IT Security Tool.
- To change the password of the user account, use the utilities described in SEE ALSO at the end of this topic.

SEE ALSO For more information about changing the password of a user account, refer to:

6.11, “Other Utility Programs” on page 6-51

For more information about security of AD projects, refer to:

C1.2.2, “Controlling access to AD projects” in Engineer's Reference Manual (IM 32P04B10-01EN)

For more information about changing the password of CTM_PROCESS, refer to:

6.11., “Other Utility Programs” in CENTUM VP Security Guide (IM 33J01C30-01EN)

Type 1: Legacy Model

After running the IT Security Tool, the following users and user groups will be automatically created.

Table 2.2.3-1 Legacy Model

User name/group name	Type	Created location	Member of	Explanation
LIC_PROCESS	User	Local PC	Users	User account for running license management processes (Windows services) that does not have Windows logon rights.
EXAUSER (*1)	User	Local PC	Users	User account for running the SCS SOE OPC server that does not have Windows logon rights.
ADS_PROCESS	User	Local PC	Users	User account for running Automation Design Server processes (Windows services) that does not have Windows logon rights.
CTM_PROCESS	User	Local PC	Users	User account that is created on a computer with the license for the Engineering Server Function and used when backing up a project. This user account does not have Windows logon rights.
ADS_AGENT	User	Local PC	• Users • Performance Monitor Users	User account for running station information management processes that does not have Windows logon rights.

*1: EXAUSER is used only in the Legacy model and thus the password change procedure is not provided.

IMPORTANT

Use these user accounts only for running ProSafe-RS products.

SEE ALSO For more information about Automation Design Server, refer to:

A., “Overview of Automation Design Suite” in Engineer's Reference Manual (IM 32P04B10-01EN)

Type 2: Standard Model/Strengthened Model - Standalone Management

After running the IT Security Tool, the following users and user groups will be automatically created.

Table 2.2.3-2 Standard Model/Strengthened Model - Standalone Management

User name/group name	Type	Created location	Member of	Explanation
PSF_OPERATOR	Group	Local PC	Users (*1)	Group of users for enabling CENTUM VP operators to access ProSafe-RS when the system is integrated with CENTUM VP.
PSF_ENGINEER	Group	Local PC	Users (*1)	Group of users who perform ProSafe-RS system engineering by using SCS Manager and other programs.
PSF_OPC	Group	Local PC	Users (*1)	Group of users who perform OPC communication with ProSafe-RS.
PSF_MAINTENANCE	Group	Local PC	Administrators (*1)	Group of users who perform system installation and ProSafe-RS maintenance.
PSF_UTL	Group	Local PC	Users (*1)	Group of users who use tools for analyzing ProSafe-RS project data. Safe operation of the tools is ensured because the members of this group cannot write to project folders.
ADS_MANAGER	Group	Local PC	Users (*1)	Group of users who use the Automation Design Suite Administration Tool to manage Automation Design Server.
PSF_PROCESS	User	Local PC	Users	User account for running ProSafe-RS processes (Windows services) that does not have Windows logon rights.
LIC_PROCESS	User	Local PC	Users	User account for running license management processes (Windows services) that does not have Windows logon rights.
ADS_PROCESS	User	Local PC	Users	User account for running Automation Design Server processes (Windows services) that does not have Windows logon rights.
CTM_PROCESS	User	Local PC	Users	User account that is created on a computer with the license for the Engineering Server Function and used when backing up a project. This user account does not have Windows logon rights.
ADS_AGENT	User	Local PC	• Users • Performance Monitor Users • PSF_OPC	User account for running station information management processes that does not have Windows logon rights.

*1: You need to add the users who belong to the created group to the group shown in the “Member of” column.

IMPORTANT

- Use these user accounts and groups only for running ProSafe-RS products.
- If you change the security model, existing user groups may be deleted or their names may be modified without confirmation.

SEE ALSO For more information about Automation Design Server, refer to:

A., “Overview of Automation Design Suite” in Engineer's Reference Manual (IM 32P04B10-01EN)

Type 3: Standard Model/Strengthened Model - Domain Management

After running the IT Security Tool, the following users and user groups will be automatically created.

Table 2.2.3-3 Standard Model/Strengthened Model - Domain Management

User name/group name	Type	Created location	Member of	Explanation
PSF_OPERATOR	Group	Domain controller	Domain Users (*1)	Group of users for enabling CENTUM VP operators to access ProSafe-RS when the system is integrated with CENTUM VP.
PSF_ENGINEER	Group	Domain controller	Domain Users (*1)	Group of users who perform ProSafe-RS system engineering by using SCS Manager and other programs.
PSF_OPC	Group	Domain controller	Domain Users (*1)	Group of users who perform OPC communication with ProSafe-RS.
PSF_OPC_LCL	Group	Local PC	Users (*1)	Supplementary group of users with the same rights as PSF_OPC but do not support Domain management, such as users embedded in the EXA package. This group is not used in normal operations.
PSF_MAINTENANCE	Group	Domain controller	Domain Admins (*1)	Group of users who perform system installation and ProSafe-RS maintenance.
PSF_MAINTENANCE_LCL	Group	Local PC	Administrators (*1)	Group of users with the same rights as PSF_MAINTENANCE that is used only for emergency situations when the domain environment is abnormal. This group is not used in normal operations. The user who installed the ProSafe-RS software becomes a member of this group.
PSF_UTL	Group	Local PC	Users (*1)	Group of users who use tools for analyzing ProSafe-RS project data. Safe operation of the tools is ensured because the members of this group cannot write to project folders.
ADS_MANAGER	Group	Domain controller	Domain Users (*1)	Group of users who use the Automation Design Suite Administration Tool to manage Automation Design Server.
PSF_PROCESS	User	Local PC	Users	User account for running ProSafe-RS processes (Windows services) that does not have Windows logon rights.

Continues on the next page

Table 2.2.3-3 Standard Model/Strengthened Model - Domain Management (Table continued)

User name/group name	Type	Created location	Member of	Explanation
LIC_PROCESS	User	Local PC	Users	User account for running license management processes (Windows services) that does not have Windows logon rights.
ADS_PROCESS	User	Local PC	Users	User account for running Automation Design Server processes (Windows services) that does not have Windows logon rights.
CTM_PROCESS	User	Local PC	Users	User account that is created on a computer with the license for the Engineering Server Function and used when backing up a project. This user account does not have Windows logon rights.
ADS_AGENT	User	Local PC	• Users • Performance Monitor Users • PSF_OPC_LCL	User account for running station information management processes that does not have Windows logon rights.

*1: You need to add the users who belong to the created group to the group shown in the “Member of” column.

IMPORTANT

- Use these user accounts and groups only for running ProSafe-RS products.
- If you change the security model, existing user groups may be deleted or their names may be modified without confirmation.

SEE ALSO

For more information about Automation Design Server, refer to:

A., “Overview of Automation Design Suite” in Engineer's Reference Manual (IM 32P04B10-01EN)

Type 4: Standard Model/Strengthened Model - Combination Management

After running the IT Security Tool, the following users and user groups will be automatically created.

Table 2.2.3-4 Standard Model/Strengthened Model - Combination Management

User name/group name	Type	Created location	Member of	Explanation
PSF_OPERATOR	Group	Domain controller	Domain Users (*1)	Group of users for enabling CENTUM VP operators to access ProSafe-RS when the system is integrated with CENTUM VP.
PSF_OPERATOR_LCL	Group	Local PC	Users (*1)	Group of users for operators that is used in a PC where standalone management is performed.

Continues on the next page

Table 2.2.3-4 Standard Model/Strengthened Model - Combination Management (Table continued)

User name/group name	Type	Created location	Member of	Explanation
PSF_ENGINEER	Group	Domain controller	Domain Users (*1)	Group of users who perform ProSafe-RS system engineering by using SCS Manager and other programs.
PSF_ENGINEER_LCL	Group	Local PC	Users (*1)	Group of users who perform ProSafe-RS system engineering by using SCS Manager and other programs. This group is used in a PC where standalone management is performed.
PSF_OPC	Group	Domain controller	Domain Users (*1)	Group of users who perform OPC communication with ProSafe-RS.
PSF_OPC_LCL	Group	Local PC	Users (*1)	Supplementary group of users with the same rights as PSF_OPC but do not support Domain management, such as users embedded in the EXA package. This group is not used in normal operations.
PSF_MAINTENANCE	Group	Domain controller	Domain Admins (*1)	Group of users who perform system installation and ProSafe-RS maintenance.
PSF_MAINTENANCE_LCL	Group	Local PC	Administrators (*1)	Group of users with the same rights as PSF_MAINTENANCE that is used only for emergency situations when the domain environment is abnormal. This group is not used in normal operations. The user who installed the ProSafe-RS software becomes a member of this group.
PSF_UTL	Group	Local PC	Users (*1)	Group of users who use tools for analyzing ProSafe-RS project data. Safe operation of the tools is ensured because the members of this group cannot write to project folders.
ADS_MANAGER	Group	Domain controller	Domain Users (*1)	Group of users who use the Automation Design Suite Administration Tool to manage Automation Design Server.
ADS_MANAGER_LCL	Group	Local PC	Users (*1)	Group of users who use the Automation Design Suite Administration Tool on a PC where standalone management is applied to manage Automation Design Server.
PSF_PROCESS	User	Local PC	Users	User account for running ProSafe-RS processes (Windows services) that does not have Windows logon rights.

Continues on the next page

Table 2.2.3-4 Standard Model/Strengthened Model - Combination Management (Table continued)

User name/group name	Type	Created location	Member of	Explanation
LIC_PROCESS	User	Local PC	Users	User account for running license management processes (Windows services) that does not have Windows logon rights.
ADS_PROCESS	User	Local PC	Users	User account for running Automation Design Server processes (Windows services) that does not have Windows logon rights.
CTM_PROCESS	User	Local PC	Users	User account that is created on a computer with the license for the Engineering Server Function and used when backing up a project. This user account does not have Windows logon rights.
ADS_AGENT	User	Local PC	• Users • Performance Monitor Users • PSF_OPC_LCL	User account for running station information management processes that does not have Windows logon rights.

*1: You need to add the users who belong to the created group to the group shown in the “Member of” column.

IMPORTANT

- Use these user accounts and groups only for running ProSafe-RS products.
- If you change the security model, existing user groups may be deleted or their names may be modified without confirmation.

SEE ALSO

For more information about Automation Design Server, refer to:

A., “Overview of Automation Design Suite” in Engineer's Reference Manual (IM 32P04B10-01EN)

Type 5: Standard Model/Strengthened Model - Linked Domain Management

After applying IT security of standalone management with IT Security Tool, the following users and local computer groups will be automatically created. The domain controller groups shown in the following table must be created in the domain before running Domain Link Management Tool.

Table 2.2.3-5 Standard Model/Strengthened Model - Linked Domain Management

User name/group name	Type	Created location	Member of	Explanation
PSF_OPERATOR	Group	Domain controller	Domain Users (*1)	Group of users for enabling CENTUM VP operators to access ProSafe-RS when the system is integrated with CENTUM VP.

Continues on the next page

Table 2.2.3-5 Standard Model/Strengthened Model - Linked Domain Management (Table continued)

User name/group name	Type	Created location	Member of	Explanation
PSF_OPERATOR	Group	Local computer	Users (*1)	Group of users for operators that is used in a computer where standalone management is performed.
PSF_ENGINEER	Group	Domain controller	Domain Users (*1)	Group of users who perform ProSafe-RS system engineering by using SCS Manager and other programs.
PSF_ENGINEER	Group	Local computer	Users (*1)	Group of users who perform ProSafe-RS system engineering by using SCS Manager and other programs. This group is used in a PC where standalone management is performed.
PSF_OPC	Group	Domain controller	Domain Users (*1)	Group of users who perform OPC communication with ProSafe-RS.
PSF_OPC	Group	Local computer	Users (*1)	Supplementary group for users not supporting domain management, such as users embedded in the EXA package, having the same rights as PSF_OPC created in the domain controller. It is not used in normal operation.
PSF_MAINTENANCE	Group	Domain controller	Domain Admins (*1)	Group of users who perform system installation and ProSafe-RS maintenance.
PSF_MAINTENANCE	Group	Local computer	Administrators (*1)	Emergency group used when the domain environment has problems, having the same rights as PSF_MAINTENANCE created in the domain controller. It is not used in normal operation. The user who installed the ProSafe-RS software becomes a member of this group.
PSF_UTL	Group	Local computer	Users (*1)	Group of users who use tools for analyzing ProSafe-RS project data. Safe operation of the tools is ensured because the members of this group cannot write to project folders.
ADS_MANAGER	Group	Domain controller	Domain Users (*1)	Group of users who use the Automation Design Suite Administration Tool to manage Automation Design Server.
ADS_MANAGER	Group	Local computer	Users (*1)	Group of users who use the Automation Design Suite Administration Tool on a PC where standalone management is applied to manage Automation Design Server.

Continues on the next page

Table 2.2.3-5 Standard Model/Strengthened Model - Linked Domain Management (Table continued)

User name/group name	Type	Created location	Member of	Explanation
PSF_PROCESS	User	Local computer	Users	User account for running ProSafe-RS processes (Windows services) that does not have Windows logon rights.
LIC_PROCESS	User	Local computer	Users	User account for running license management processes (Windows services) that does not have Windows logon rights.
ADS_PROCESS	User	Local computer	Users	User account for running Automation Design Server processes (Windows services) that does not have Windows logon rights.
CTM_PROCESS	User	Local computer	Users	User account that is created on a computer with the license for the Engineering Server Function and used when backing up a project. This user account does not have Windows logon rights.
ADS_AGENT	User	Local computer	• Users • Performance Monitor Users • PSF_OPC	User account for running station information management processes that does not have Windows logon rights.

*1: You need to add the users who belong to the created group to the group shown in the “Member of” column.

IMPORTANT

- Use these user accounts and groups only for running ProSafe-RS products.
- If you change the security model, existing user groups may be deleted or their names may be modified without confirmation.

SEE ALSO For more information about Automation Design Server, refer to:

A., “Overview of Automation Design Suite” in Engineer's Reference Manual (IM 32P04B10-01EN)

The Users and User Groups Added by the Vnet/IP Interface Package

When Vnet/IP Interface Package is installed, the users and user groups in the following table are automatically created.

The users and user groups other than LIC_PROCESS are used only for Vnet/IP Interface Package. They do not affect the ProSafe-RS software.

Table 2.2.3-6 Added Users and Groups

User name/group name	Type	Created location	Member of	Explanation
VNT_ALL	Group	Local PC	-	Group of users who can read/write in the directory of Vnet/IP Interface Package Do not include the users who can sign-in to Windows in this group.
VNT_ VNET_VVIF	Group	Local PC	-	Group of users for running the processes (like Windows services) of Vnet/IP Interface Package. Do not include the users who can sign-in to Windows in this group.
VNT_NVP_ CMDIF	Group	Local PC	-	
VNT_NVP_MNGIF	Group	Local PC	-	
VNT_COMMON	User	Local PC	VNT_ALL	Users who can read/write in the directory of Vnet/IP Interface Package. Windows sign-in rights are not granted.
VNT_NVP_CORE	User	Local PC	• VNT_VNET_VVIF • VNT_NVP_CMDIF • VNT_NVP_MNGIF • VNT_ALL • Performance Monitor Users	Users for running the processes (like Windows services) of Vnet/IP Interface Package. Windows sign-in rights are not granted.
VNT_BKNET	User	Local PC	• VNT_VNET_VVIF • VNT_NVP_MNGIF • VNT_ALL	
LIC_PROCESS	User	Local PC	• VNT_ALL • Users	LIC_PROCESS is a common user for products which support License Manager. It is used for accepting licenses. When installing Vnet/IP Interface Package, if LIC_PROCESS is not present, LIC_PROCESS user is created and configured.

IMPORTANT

The users and user groups that are automatically created when Vnet/IP Interface Package is installed are valid only on local PCs. Do not manage the users and user groups in the domain controller. And, do not include the users who can sign-in to Windows in this group.

The users for using iDefine in a virtualization environment

TIS_SERVICE user is necessary for using iDefine in a virtualization environment.

TIS_SERVICE user is reserved as a user to run Dongle Gateway. When the Dongle Gateway which is provided by Trinity Integrated Systems is installed, TIS_SERVICE user is created.

IMPORTANT

- The default initial password is set for the TIS_SERVICE user. Be sure to change the password because operating with the initial password may increase the security risk.
- The password for the TIS_SERVICE user is reset to the default password when Dongle Gateway is installed for upgrading its version or revision. Be sure to change the password before operating. The password is not reset to the default password by configuring with the IT Security Tool.
- To change the password of the TIS_SERVICE user, use the utilities described in SEE ALSO at the end of this topic.

Table 2.2.3-7 Users and Groups

User name/group name	Type	Created location	Member of	Explanation
TIS_SERVICE	User	Local PC	Users	User account for running the Dongle Gateway of iDefine that does not have Windows logon rights.

SEE ALSO For more information about changing the password of a user account, refer to:

6.11, “Other Utility Programs” on page 6-51

3. Details of Security Measures

This section describes the security measures for each security type in detail.

3.1 Access Control

By minimizing the access rights of the users of the product, you can prevent unauthorized access, leakage, tampering, and destruction of important data in the product. Access permissions to files, folders, registries, DCOM modules, and local security policy are controlled by using the Windows access control functions.

Access control is performed for each user or group. Users have only the rights that are granted to them or to the group they belong to.

3.1.1 Access Permissions to Files and Folders

In the product, accesses to files and folders are controlled for each file or folder. Access to files and folders by users is restricted by controlling the permissions to execute, read, write, and delete in user or group units. In the product, access permissions are granted for each folder.

TIP If a file in a folder requires different access permissions, the access permissions for the file can be separately granted.

Target Folders

The following table describes the main target folders with controlled access, showing examples where the system drive is drive C.

Table 3.1.1-1 Target Folders

Name	Target folder	Description
ProSafe-RS folder 1	C:\Program Files (x86)\ProSafe-RS	The folder in which ProSafe-RS programs are installed.
ProSafe-RS folder 2	C:\Program Files (x86)\Yokogawa\IA\iPCS\Products\ProSafe-RS	The folder in which ProSafe-RS programs are installed.
ProSafe-RS folder 3	C:\ProgramData\Yokogawa\IA\iPCS\Products\ProSafe-RS	The folder in which ProSafe-RS data such as log files are stored.
ProgramFiles Platform folder	C:\Program Files (x86)\Yokogawa\IA\iPCS\Platform	The folder in which IT Security Tool, Domain Link Management Tool, and license management programs are installed.
AD Suite folder 1	C:\Program Files\Yokogawa\IA\iPCS\Products\ADSuite	The folder in which programs that are related to Automation Design Server are installed.
AD Suite folder 2	C:\Program Files (x86)\Yokogawa\IA\iPCS\Products\ADSuite	The folder in which programs that are related to Automation Design Server are installed.
ADMDB folder	C:\ProgramData\Yokogawa\IA\iPCS\Products\ChronusENG	The folder in which data that are related to Automation Design Server are installed.
ProgramData Platform folder	C:\ProgramData\Yokogawa\IA\iPCS\Platform	The folder in which data files such as the setting files for IT Security Tool and license management data files are installed.
iDefine folder 1	C:\Program Files (x86)\Trinity Integrated Systems\iDefine x.xx.x Yokogawa	The folder in which iDefine-related programs are installed. The folder shown in the left column is the default setting (x.xx.x is the version number of iDefine). You can specify a different folder at installation.
iDefine folder 2	C:\Program Files (x86)\Common Files\Aladdin Shared	The folder in which iDefine-related programs are installed.
PROFINET Configurator folder 1	C:\Program Files (x86)\Yokogawa\PROFIBUS_Configurator	The folder in which PROFINET Configurator is installed.
PROFINET Configurator folder 2	C:\Program Files (x86)\Common Files\Hilscher	The folder for use by PROFINET Configurator.
PROFINET Configurator folder 3	C:\Program Files (x86)\Common Files\Hilscher GmbH	The folder for use by PROFINET Configurator.
PROFINET Configurator folder 4	C:\ProgramData\Yokogawa\SYCONnet	The folder in which PROFINET Configurator data files are stored.
Station information checking function folder 1	C:\Program Files\Yokogawa\IA\iPCS\Products\CIMAgent	The folder in which programs related to station information management processes are installed.

Continues on the next page

Table 3.1.1-1 Target Folders (Table continued)

Name	Target folder	Description
Station information checking function folder 2	C:\ProgramData\Yokogawa\IA\iPCS\Products\CIMAgent	The folder in which data related to station information management processes is installed.
Windows folder	C:\Windows\system32	The folder in which Windows maintenance tools are installed.(*1)
Project Data folder	The folder for storing ProSafe-RS project files.	The folder to which a share name, RS-Projects, is assigned. Note: You can assign the share name only to a user-created folder. Do not assign to a folder created by the installer or ProSafe-RS system. Exceptionally, however, you can assign the share name to the C:\RS-Projects folder.
RS-Share folder	The folder for storing data shared by ProSafe-RS stations.	The folder to which a share name, RS-Share, is assigned. Note: You can assign the share name only to a user-created folder. Do not assign to a folder created by the installer or ProSafe-RS system.
ForcedIO folder	The folder for storing data of Forced I/O Viewer function	The folder to which a share name, RS-ForcedIO, is assigned.
iDefine project folder	The folder for storing iDefine projects shared by ProSafe-RS stations.	The folder to which a share name, iDefineProjects, is assigned. Note: Assign the share name iDefineProjects to the C:\iDefineProjects folder, which is created by the iDefine installer. If you want to place the iDefine project folder in a different location, create a folder and assign the share name iDefineProjects. Do not assign the share name to a folder created by the ProSafe-RS installer or ProSafe-RS system.
VnetIPSoftStack folder 1	C:\ProgramData\Yokogawa\IA\iPCS\Products\AccessRef\VnetIPSoftStack	The folder in which Vnet/IP Interface Package related files and data are stored.
VnetIPSoftStack folder 2	C:\Program Files\Yokogawa\IA\iPCS\Platform\VnetIPSoftStack	The folder in which Vnet/IP Interface Package related files and data are stored.
VnetIPSoftStack folder 3	C:\ProgramData\Yokogawa\IA\iPCS\Platform\VnetIPSoftStack	The folder in which Vnet/IP Interface Package related files and data are stored.

*1: Access permissions are set for certain files in the folder.

Access Permissions to Programs

Functions that each user can use are restricted by setting access permissions to each ProSafe-RS function (program) for each user or group.

The following table shows the access permissions to run programs registered in the Start menu that are granted to each user and group . Only the users or users of a group to which the access permission is granted can run the program.

Table 3.1.1-2 Access Permissions to Programs that are Started from the Start Menu

Items on Start Menu	User/group (*1)										
	[1]	[2]	[3]	[4]	[5]	[6] (*2)	[7]	[8]	[9]	[10]	[11]
[YOKOGAWA License]											
License Manager	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No	No
[YOKOGAWA Security]											
IT Security Tool	No	No	No	No	Yes	No	No	Yes	No	No	No
Domain Link Management Tool	No	No	No	No	Yes	No	No	Yes	No	No	No
[ProSafe]											
Workbench	Yes	Yes	No	No	Yes (*3)	No	No	Yes	No	No	No
Version Control Tool	No	Yes	No	No	Yes	No	No	Yes	No	No	No
Test Project Creating Tool	No	Yes	No	No	Yes	No	No	Yes	No	No	No
Software Configuration Viewer	No	Yes	No	No	Yes	No	No	Yes	No	No	No
SOE Viewer	Yes	Yes	No	No	Yes	No	No	Yes	No	No	No
SOE OPC Parameter Setting	No	Yes	No	No	Yes	No	No	Yes	No	No	No
SCS Status Overview	Yes	Yes	No	No	Yes	No	No	Yes	No	No	No
Project Attribute Tool	No	Yes	No	No	Yes	No	No	Yes	No	No	No
Message Cache Tool	No	Yes	No	No	Yes	No	No	Yes	No	No	No
Operation History Database Viewer	Yes	Yes	No	No	Yes	No	No	Yes	No	No	No
Operation History Management Set-up Tool	No	No	No	No	Yes	No	No	Yes	No	No	No
Project Comparing Tool	No	Yes	No	No	Yes	No	No	Yes	No	No	No
Domain Properties Setting Tool	No	Yes	No	No	Yes	No	No	Yes	No	No	No
YFGW-PROFINET Configuration Support Tool	No	Yes	No	No	Yes	No	No	Yes	No	No	No
Forced IO Viewer Setup Tool	No	Yes	No	No	Yes	No	No	Yes	No	No	No
Forced IO Viewer	Yes	Yes	No	No	Yes	No	No	Yes	No	No	No
[YOKOGAWA AD Suite]											
AD Organizer	No	Yes	No	No	Yes	No	No	No	No	Yes	No
ADS Administration Tool	No	No	No	No	No	No	No	No	Yes	Yes	No
[ProSafe Online Manual]											
Document Map	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	No	No
Read Me First	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	No	No
Workbench	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	No	No
[ProSafe Maintenance]											
Logsave for ProSafe-RS	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	No	No
SCS master DB recover	No	Yes	No	No	Yes	No	No	Yes	No	No	No
[Trinity Integrated Systems]											
Dongle Manager	Yes	Yes	No	No	Yes	No	No	No	No	No	No
Dongle Utility	Yes	Yes	No	No	Yes	No	No	No	No	No	No
Enterprise License Tool (*4)	Yes	Yes	No	No	Yes	No	No	No	No	No	No
iDefine	Yes	Yes	No	No	Yes	No	No	No	No	No	No

Continues on the next page

Table 3.1.1-2 Access Permissions to Programs that are Started from the Start Menu (Table continued)

Items on Start Menu	User/group (*1)										
	[1]	[2]	[3]	[4]	[5]	[6] (*2)	[7]	[8]	[9]	[10]	[11]
iDefine - License User Guide	Yes	Yes	No	No	Yes	No	No	Yes	No	No	No
iDefine - User Guide	Yes	Yes	No	No	Yes	No	No	Yes	No	No	No
Uninstall iDefine	No	No	No	No	Yes	No	No	No	No	No	No
[YOKOGAWA Virtualization]											
VnetIP interface management tool	(*5)										

*1: User/Group
[1]: PSF_OPERATOR/PSF_OPERATOR_LCL
[2]: PSF_ENGINEER/PSF_ENGINEER_LCL
[3]: LIC_PROCESS
[4]: PSF_OPC/PSF_OPC_LCL
[5]: PSF_MAINTENANCE/PSF_MAINTENANCE_LCL
[6]: PSF_PROCESS
[7]: PSF_UTL
[8]: Local System Account (System account for programs used by Windows)
[9]: ADS_MANAGER/ADS_MANAGER_LCL
[10]: ADS_PROCESS
[11]: CTM_PROCESS/ADS_AGENT
*2: The PSF_PROCESS user cannot start programs from the start menu because it is not a logon user.
*3: SCS simulator can be started only by the built-in Administrator account.
*4: The customer cannot use this tool.
*5: The Vnet/IP interface management tool starts. Access permission is set for the Administrators group, Users group, and VNT_ALL group, and users who belong to Administrators group and Users group can be executed. The users in the Administrators group can configure the Vnet station address and monitor the Vnet/IP interface package. Other users can only monitor the Vnet/IP interface package.

IMPORTANT

The users of PSF_MAINTENANCE and PSF_MAINTENANCE_LCL belonging to the Administrators group cannot start SCS simulator. However, the built-in Administrator account user is an exception, and can start SCS simulator.

3.1.2 Package Configuration and Users/Groups

You can control access rights of each user and group for the folders related to the installed packages to prevent tampering and destruction of the installed modules.

Access Permissions to Package Folders

The following table shows the types of access permissions to package folders.

Table 3.1.2-1 Types of Access Permissions to Package Folders

Package-related folder	Target folder	User/group (*1)											
		[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
ProSafe-RS folder 1	The folder in which ProSafe-RS programs are installed <ProgramFiles32>\ProSafe-RS	RW	RW	-	RW	RWD	RW	R	RWD	R	-	-	-
ProSafe-RS folder 2	The folder in which ProSafe-RS programs are installed <ProgramFiles32>\Yokogawa\IA\iPCS\Products\ProSafe-RS	R	R	-	R	RWD	R	R	RWD	-	-	-	-
ProSafe-RS folder 3	The folder in which ProSafe-RS data such as log files are stored <ProgramData>\Yokogawa\IA\iPCS\Products\ProSafe-RS	R	R	-	R	RWDP	R	R	RWD	-	-	-	-
Project Data folder	The folder in which project data are saved (Share name "RS-Projects" is assigned)	RWD	RWD	RWD	RWD	RWD	RWD	R	RWD	-	-	-	-
RS-Share folder	The folder in which data of the Access Control and Operation History Management Package or data managed by Version Control Tool are saved (Share name "RS-Share" is assigned)	RWD	RWD	RWD	RWD	RWD	RWD	R	RWD	-	-	-	-
ForcedIO folder	The folder in which data of Forced I/O Viewer function are saved (Share name “RS-ForcedIO” is assigned)	R	RWD	-	-	RWDP	-	-	RWD	-	-	-	-
AD Suite folder 1	The folder in which programs that are related to Automation Design Server are installed <ProgramFiles64>\Yokogawa\IA\iPCS\Products\ADSuite	-	R	-	-	RWD	-	-	RWD	R	R	R	-

Continues on the next page

Table 3.1.2-1 Types of Access Permissions to Package Folders (Table continued)

Package-related folder	Target folder	User/group (*1)											
		[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
AD Suite folder 2	The folder in which programs that are related to Automation Design Server are installed <ProgramFiles32>\Yokogawa\IA\iPCS\Products\ADSuite	-	R	-	-	RWDP	-	-	RWD	R	R	R	-
ADMDB folder	The folder in which data that are related to Automation Design Server are installed <ProgramData>\Yokogawa\IA\iPCS\Products\ChronusENG	-	R	-	-	RWD	R	-	RWD	R	RWD	RWD	-
iDefine folder 1	The folder in which iDefine-related programs are installed <ProgramFiles32>\Trinity Integrated Systems\iDefine x.xx.x Yokogawa	RX	RX	-	-	F	-	-	RWD	-	-	-	-
iDefine folder 2	The folder in which iDefine-related programs are installed <ProgramFiles32>\Common Files\Aladdin Shared	RWD	RWD	-	-	RWDP	-	-	RWDX	-	-	-	-
iDefine project folder	The folder in which iDefine project data is saved (Share name “iDefineProjects” is assigned)	RWD	RWD	-	-	RWDP	-	-	RWD	-	-	-	-
PROFINET Configurator folder 1	The folder in which PROFINET Configurator-related programs are installed <ProgramFiles32>\Yokogawa\PROFIBUS_Configurator	-	RX	-	-	F	-	-	RWD	-	-	-	-
PROFINET Configurator folder 2	The folder in which PROFINET Configurator-related programs are installed <ProgramFiles32>\Common Files\Hilscher	-	RX	-	-	F	-	-	RWDX	-	-	-	-
PROFINET Configurator folder 3	The folder in which PROFINET Configurator-related programs are installed <ProgramFiles32>\Common Files\Hilscher GmbH	-	RX	-	-	F	-	-	RWDX	-	-	-	-

Continues on the next page

Table 3.1.2-1 Types of Access Permissions to Package Folders (Table continued)

Package-related folder	Target folder	User/group (*1)											
		[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
PROFINET Configurator folder 4	The folder in which PROFINET Configurator-related data files are stored <ProgramData>\Yokogawa\SYCONnet	-	RW	-	-	RW DP	-	-	RW D	-	-	-	-
Station information checking function folder 1	The folder in which programs for running station information management processes (Windows services) are installed <ProgramFiles64>\Yokogawa\IA\iPCS\Products\CIMAgent)	-	-	-	-	RW DP	-	-	RW DX	-	-	-	RX
Station information checking function folder 2	The folder in which data for running station information management processes (Windows services) is installed <ProgramData>\Yokogawa\IA\iPCS\Products\CIMAgent)	-	-	-	-	RW DP	-	-	RW D	-	-	-	RW D
VnetIP-SoftStack folder 1 (*2)	The folder in which Vnet/IP Interface Package related files and data are stored <ProgramData> \Yokogawa\IA\iPCS\Products\AccessRef\VnetIPSoftStack	R	R	-	R	RW DP	R	R	RW D	-	-	-	R
VnetIP-SoftStack folder 2	The folder in which Vnet/IP Interface Package related files and data are stored <ProgramFiles64>\Yokogawa\IA\iPCS\Platform\VnetIPSoftStack	(*3)											
VnetIP-SoftStack folder 3	The folder in which Vnet/IP Interface Package related files and data are stored <ProgramData>\Yokogawa\IA\iPCS\Platform\VnetIPSoftStack	(*3)											

*1: User/group
[1]: PSF_OPERATOR/PSF_OPERATOR_LCL
[2]: PSF_ENGINEER/PSF_ENGINEER_LCL
[3]: LIC_PROCESS
[4]: PSF_OPC/PSF_OPC_LCL
[5]: PSF_MAINTENANCE/PSF_MAINTENANCE_LCL
[6]: PSF_PROCESS
[7]: PSF_UTL
[8]: Local System Account (System account for executing programs used by Windows)
[9]: ADS_MANAGER/ADS_MANAGER_LCL
[10]: ADS_PROCESS
[11]: CTM_PROCESS
[12]: ADS_AGENT
Types of access permission

F:Full access control
R: Read files and view a list of folder details
X: Read and execute
W: Write
D: Delete
P: Change permissions (rights to set and change access permissions to files and registries)
C: Change access permission
-: No permission

*2: In addition to the users / groups listed in the table, F is set for the Administrators group, and R is set for the Users group.

*3: Set access permissions for users and groups defined in the Vnet/IP interface package and Windows standard users and groups. User and group access permissions defined for each product are not set. RWXDC is set for the Administrators group, RWX is set for the VNT_ALL group, and RX is set for the User group.

3.1.3 Registry Configuration and User/Group

You can control access to the registries used by ProSafe-RS to prevent tampering and destruction of them.

Access Permissions to Registries

The following table shows the types of permissions to the registry keys corresponding the target registries.

With ProSafe-RS software release number R3.01 or later, only a read permission is granted to Everyone of the user or group that can access the registries.

Table 3.1.3-1 Types of Access Permissions to Registries

Registry key	User/group (*1)											
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\EXA (*2)	F	F	F	F	F	F	F	F	R	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\EXAOPC (*2)	F	F	F	F	F	F	F	F	R	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\PKGCOM (*2)	F	F	F	F	F	F	F	F	R	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\PROSAFE-RS	F	F	F	F	F	F	F	F	R	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\VHFD (*2)	F	F	F	F	F	F	F	F	R	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA Prosafe	F	F	F	F	F	F	F	F	R	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\Alter sys	F	F	F	F	F	F	F	F	R	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\Trinity Integrated Systems\iDefine for Yokogawa	R	R	–	–	F	–	–	F	–	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin Knowledge Systems	R	R	–	–	F	–	–	F	–	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\Hilscher GmbH	–	F	–	–	F	–	–	F	–	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\PROFIBUS International	–	F	–	–	F	–	–	F	–	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\DTMs	–	F	–	–	F	–	–	F	–	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\GenericSlaveDTM	–	F	–	–	F	–	–	F	–	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\SyCon_net	–	F	–	–	F	–	–	F	–	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{1229e510-2cd5-11d4-a174-0050da59a2ed}	F	F	F	F	F	F	F	F	F	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{12413-1229e511-2cd5-11d4-a174-0050da59a2ed}	F	F	F	F	F	F	F	F	F	–	–	–
HKEY_LOCAL_MACHINE\SOFTWARE\ODBC (*2)	F	F	F	F	F	F	F	F	R	–	–	–

Continues on the next page

Table 3.1.3-1 Types of Access Permissions to Registries (Table continued)

Registry key	User/group (*1)											
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\VLNIC\Config (*2)	F	F	F	F	F	F	F	F	R	–	–	–
HKEY_USERS\DEFAULT\SOFTWARE\YOKOGAWA (*2)	F	F	F	F	F	F	F	F	R	–	–	–

*1: User/group
[1]: PSF_OPERATOR/PSF_OPERATOR_LCL
[2]: PSF_ENGINEER/PSF_ENGINEER_LCL
[3]: LIC_PROCESS
[4]: PSF_OPC/PSF_OPC_LCL
[5]: PSF_MAINTENANCE/PSF_MAINTENANCE_LCL
[6]: PSF_PROCESS
[7]: PSF_UTL
[8]: Local System Account (System account for executing programs used by Windows)
[9]: Everyone
[10]: ADS_MANAGER/ADS_MANAGER_LCL
[11]: ADS_PROCESS
[12]: CTM_PROCESS/ADS_AGENT
Types of access permission
F: Full access control
R: Read
-: No permission

*2: For these registry keys, permissions are added as shown in the table without changing the existing permissions.

3.1.4 DCOM (OPC) and User/Group

Considering software packages (including third party packages) that communicate with ProSafe-RS by using DCOM, you can set access permissions on DCOM applications that perform OPC communication to prevent tampering, destruction, and theft of data through OPC communication.

By running the IT Security Tool, permission settings of local and/or remote access to OPC applications are configured for the following users and groups.

User/group

[1]: PSF_OPERATOR/PSF_OPERATOR_LCL

[2]: PSF_ENGINEER/PSF_ENGINEER_LCL

[4]: PSF_OPC/PSF_OPC_LCL

[5]: PSF_MAINTENANCE/PSF_MAINTENANCE_LCL

[6]: PSF_PROCESS

[7]: PSF_UTL

[8]: ADS_MANAGER/ADS_MANAGER_LCL

[9]: ADS_PROCESS

[10]: CTM_PROCESS

With this configuration, only the users who belong to the user group for OPC communication ([4]: PSF_OPC/PSF_OPC_LCL) are allowed to start such DCOM applications or make connection through the DCOM applications. In addition, port numbers of the ports used by DCOM is restricted.

3.1.5 Local Security and User/Group

The following local security policies, in addition to Windows standard securities, are set for each user and group.

Table 3.1.5-1 Permissions Set as Local Security Policies

Policy	User/group (*1)												
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]
Create global objects	No	No	No	No	No	Yes	No	No	No	No	No	No	No
Debug programs	No	Yes	No	Yes	No	Yes	No	No	No	No	No	No	No
Log on as a batch job	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Log on as a service	No	No	Yes	No	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes
Deny log on locally	No	No	Yes	No	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes

*1: User/group
[1]: PSF_OPERATOR/PSF_OPERATOR_LCL
[2]: PSF_ENGINEER/PSF_ENGINEER_LCL
[3]: LIC_PROCESS
[4]: PSF_OPC/PSF_OPC_LCL
[5]: PSF_MAINTENANCE/PSF_MAINTENANCE_LCL
[6]: PSF_PROCESS
[7]: PSF_UTL
[8]: ADS_MANAGER/ADS_MANAGER_LCL
[9]: ADS_PROCESS
[10]: CTM_PROCESS
[11]: ADS_AGENT
[12]: VNT_COMMON, VNT_NVP_CORE, VNT_BKNET
[13]: TIS_SERVICE

3.2 Personal Firewall Tuning

You can minimize connections from networks to the PCs in the system to fight against attacks by unauthorized persons.

Exception Setting Type

Required communication ports are set as exception so that the functions of ProSafe-RS can operate.

The following table describes the exception settings of the personal firewall.

Table 3.2-1 Exception Setting Types

Name	Description
ProSafe-RS related	Communication ports used by ProSafe-RS related programs
Vnet/IP interface package related	Communication ports used by Vnet/IP Interface Package
DCOM Related	Communication ports used by programs using DCOM communication (including OPC communication)
File Sharing Related	Communication ports used by Windows file sharing functions
Windows Related	Communication ports used by Windows functions (excluding file sharing functions)

ProSafe-RS Related Exceptional Settings

The following table lists the ProSafe-RS related exceptional settings.

Table 3.2-2 ProSafe-RS Related Exceptional Settings

Service name/ execution file name	Protocol : port number	Package name	Remarks
RHHMsCacheSvr.exe	UDP: Dynamic allocation	ProSafe-RS station	Message cache server for ProSafe-RS
Yokogawa.IA.iPCS.Platform.License.LicenseManager.Service	TCP:34417	License management function	-
Yokogawa.IA.iPCS.ChronusENG.Services.Service.exe	Can be specified by the user TCP:34473 (default)	Automation Design Server	-
Yokogawa.IA.iPCS.ChronusENG.Client.RS.ExternalTest.TestManager.exe	TCP:34494	iDefine interface package	-
Yokogawa.IA.iPCS.ChronusENG.CIMAgent.exe	Can be specified by the user TCP:34497 (default)	ProSafe-RS station	Not affected by licenses
DongleGateway.exe	Can be specified by the user TCP:34512 (default)	iDefine for ProSafe-RS	Set Firewall exception by using Dongle Gateway Configurator which is placed when Dongle Gateway is installed.

Vnet/IP Interface Package Related Exceptional Settings

The following table lists the Vnet/IP interface package related exceptional settings.

Table 3.2-3 Vnet/IP Interface Package Related Exceptional Settings

Package name	Protocol : port number	Remarks
Vnet/IP interface package	UDP:520 UDP:5313 UDP:9940	Enable sending/receiving in the UDP ports mentioned on the left that are used in the Vnet/IP interface package

DCOM Related Exceptional Settings

The following table lists the DCOM related exceptional settings.

Table 3.2-4 DCOM Related Exceptional Settings

Service name/ execution file name	Protocol : port number	Assumed package name	Remarks
DCOM service	TCP:135	Programs using OPC communication	Required when using OPC communication.
DCOM service	TCP:20501 to 20550	Programs using OPC communication	Required when using OPC communication.

File Sharing Related Exceptional Settings

The following table lists the file sharing related exceptional settings.

Table 3.2-5 File Sharing Related Exceptional Settings

Service name/execution file name	Protocol : port number	Function name	Remarks
Sharing files and printers	TCP:139 UDP:137 UDP:138	NetBIOS	-
Sharing files and printers	TCP:445	Direct Hosting	If NetBIOS is disabled, separate means of name resolution, such as HOSTS file and registration to DNS, is required.
Sharing files and printers	UDP:5355	LLMNR	-

Windows Related Exceptional Settings

The following table lists the Windows related exceptional settings.

Table 3.2-6 Windows Related Exceptional Settings

Service name/execution file name	Protocol : port number	Server/station
Enable ICMP (*1)	ICMP	Domain controller File server ProSafe-RS station
Kerberos Authentication	TCP:88 UDP:88	Domain controller
LDAP(Active Directory)	TCP:389 UDP:389	Domain controller
DNS	TCP:53 UDP:53	Domain controller

Continues on the next page

Table 3.2-6 Windows Related Exceptional Settings (Table continued)

Service name/execution file name	Protocol : port number	Server/station
Network discovery	UDP:137 UDP:138 UDP:5355 UDP:3702 UDP:1900 TCP:2869 TCP:5358 TCP:5357 UDP:3702	ProSafe-RS station

*1: This item may be ICMPv4 or ICMPv6, depending on the OS.

Allow unicast response

Note the following points:

- With IT security version 2.0, the Allow unicast response option is set to “No.”
- Applications that use multicasting or broadcasting cannot receive the response.

Cautions

In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.3 Stopping Unused Window Services

You can reinforce security by stopping unused Windows services to prevent attacks by unauthorized persons. If vulnerabilities of Windows services are abused, user information in the product may be stolen or important data in the product may be leaked, tampered, or destroyed. In the worst case, attackers may steal the domain administrator rights.

Unused Windows Services When IT Security Version 2.0 Is Applied

The following tables show the Windows services that can be stopped when IT security version 2.0 is applied, one table is for SENG and the other is for file servers and domain controllers.

In this manual, whenever Windows 10, Windows Server 2019, or Windows Server 2022 is mentioned in the explanations hereafter, the IoT versions are also included.

Table 3.3-1 Windows Services That can be Stopped on SENG (with IT Security Version 2.0)

Service	Reason	Windows OS (*1)					
		10 2016 LTSB	10 LTSC 2019	10 LTSC 2021	WS 2016	WS 2019	WS 2022
Delivery Optimization	Unnecessary in the product	Yes (*2)	N/A (*3)	N/A (*3)	–	N/A (*3)	N/A (*3)
Computer Browser	Unnecessary in the product	Yes (*4)	–	–	Yes (*5)	–	–
DHCP Client	Unnecessary because the product does not use DHCP services.	No	No	No	No	No	No
Diagnostic Policy Service	Unnecessary in the product	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)
Connected User Experience and Telemetry	Unnecessary in the product	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)
dmwappushsvc	Unnecessary in the product	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*5)	Yes (*5)
Downloaded Maps Manager	Unnecessary in the product	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*5)	Yes (*5)
IP Helper	Not required because IPv6 is not used in the ProSafe-RS system.	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)
IPsec Policy Agent	Not required because the product does not use IPsec-encrypted communication.	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)
Offline Files	Not required because the product does not use offline services.	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*5)	Yes (*5)	Yes (*5)
Program Compatibility Assistant Service	Unnecessary in the product	Yes (*2)	Yes (*4)	Yes (*4)	Yes (*2)	Yes (*4)	Yes (*6)
Remote Registry	Not required because this feature is not used.	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*2)	Yes (*2)	Yes (*2)
Secondary Logon	Not required because this feature is not used.	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)
Shell Hardware Detection	Not required because this feature is not used.	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)

Continues on the next page

Table 3.3-1 Windows Services That can be Stopped on SENG (with IT Security Version 2.0) (Table continued)

Service	Reason	Windows OS (*1)					
		10 2016 LTSB	10 LTSC 2019	10 LTSC 2021	WS 2016	WS 2019	WS 2022
Themes	Not required because this feature is not used.	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)
WebClient	Not required because this feature is not used.	Yes (*4)	Yes (*4)	Yes (*4)	–	–	–
Windows Error Reporting Service	Not required because this feature is not used.	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)
Windows Push Notifications System Service		Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)

*1: 10 2016 LTSB: Windows 10 Enterprise 2016 LTSB
10 LTSC 2019: Windows 10 Enterprise LTSC 2019
10 LTSC 2021: Windows 10 Enterprise LTSC 2021
WS 2016: Windows Server 2016
WS 2019: Windows Server 2019
WS 2022: Windows Server 2022
Yes: Services that can be stopped
No: Service that must not be stopped
–: Services that do not exist in the OS

*2: Because the Startup type for the Windows service is set to Automatic with the initial OS setting, the Startup type is changed to Disabled by the IT Security Tool.

*3: On the following OS, this service cannot be disabled.
- Windows 10 Enterprise LTSC 2019
- Windows 10 Enterprise LTSC 2021
- Windows Server 2019
- Windows Server 2022

Therefore, as a countermeasure, Windows Update Delivery Optimization prevents updates and applications from being sent or received between the computer in use and the computer on the network.

*4: Because the Startup type for the Windows service is set to Manual with the initial OS setting, the IT Security Tool does not change this setting.

*5: Because the Startup type for the Windows service is set to Disabled with the initial OS setting, the IT Security Tool does not change this setting.

*6: Because the Startup type for the Windows service is set to “Manual” in the initial OS setting, but when the modules required for this product are installed, the Startup type changes to “Automatic”, it is changed to “Disabled” by the IT Security Tool.

Table 3.3-2 Windows Services That can be Stopped on a File Server and Domain Controller (with IT Security Version 2.0)

Service	Reason	Windows OS (*1)		
		WS 2016	WS 2019	WS 2022
DHCP Client	Unnecessary in the product	No	No	No
Diagnostic Policy Service	Unnecessary in the product	Yes (*2)	Yes (*2)	Yes (*2)
Connected User Experiences and Telemetry	Unnecessary in the product	Yes (*2)	Yes (*2)	Yes (*2)
dmwappushsvc	Unnecessary in the product	Yes (*3)	Yes (*4)	Yes (*4)
Downloaded Maps Manager	Unnecessary in the product	Yes (*2)	Yes (*4)	Yes (*4)
IP Helper	Unnecessary in the product	Yes (*2)	Yes (*2)	Yes (*2)
IPsec Policy Agent	Unnecessary in the product	Yes (*3)	Yes (*3)	Yes (*3)
Offline Files	Unnecessary in the product	Yes (*4)	Yes (*4)	Yes (*4)
Program Compatibility Assistant Service	Unnecessary in the product	Yes (*2)	Yes (*3)	Yes (*5)
Remote Registry	Not required because this feature is not used.	Yes (*2)	Yes (*2)	Yes (*2)
Shell Hardware Detection	Not required because this feature is not used.	Yes (*2)	Yes (*2)	Yes (*2)

Continues on the next page

Table 3.3-2 Windows Services That can be Stopped on a File Server and Domain Controller (with IT Security Version 2.0) (Table continued)

Service	Reason	Windows OS (*1)		
		WS 2016	WS 2019	WS 2022
Windows Error Reporting Service	Unnecessary in the product	Yes (*3)	Yes (*3)	Yes (*3)
Windows Push Notifications System Service		Yes (*2)	Yes (*2)	Yes (*2)

*1: WS 2016: Windows Server 2016
WS 2019: Windows Server 2019
WS 2022: Windows Server 2022
Yes: Services that can be stopped
No: Service that must not be stopped
–: Services that do not exist in the OS
*2: Because the Startup type for the Windows service is set to Automatic with the initial OS setting, the Startup type is changed to Disabled by the IT Security Tool.
*3: Because the Startup type for the Windows service is set to Manual with the initial OS setting, the IT Security Tool does not change this setting.
*4: Because the Startup type for the Windows service is set to Disabled with the initial OS setting, the IT Security Tool does not change this setting.
*5: Because the Startup type for the Windows service is set to “Manual” in the initial OS setting, but when the modules required for this product are installed, the Startup type changes to “Automatic”, it is changed to “Disabled” by the IT Security Tool.

Unused Windows Services When IT Security Version 1.0 Is Applied

The following tables show the Windows services that can be stopped when IT security version 1.0 is applied.

Table 3.3-3 Windows Services That can be Stopped on SENG (with IT Security Version 1.0)

Service	Reason	Windows OS (*1)			
		10 2016 LTSB	10 LTSC 2019/ 10 LTSC 2021	WS 2016	WS 2019/ WS 2022
Computer Browser	Unnecessary in the product	Yes (*2)	–	Yes (*3)	–
DHCP Client	Unnecessary in the product	No	No	No	No
Windows Error Reporting Service	Unnecessary in the product	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)
IP Helper	Not required because IPv6 is not used in the ProSafe-RS system.	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)
IPsec Policy Agent	Not required because the product does not use IPsec-encrypted communication.	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)
Offline Files	Not required because the product does not use offline services.	Yes (*2)	Yes (*2)	Yes (*3)	Yes (*3)
Remote Registry	Not required because the functions are not used.	Yes (*3)	Yes (*3)	Yes (*4)	Yes (*4)
Secondary Logon	Not required because the functions are not used.	Yes (*2)	Yes (*2)	Yes (*2)	Yes (*2)
Shell Hardware Detection	Not required because the functions are not used.	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)
Themes	Not required because the functions are not used.	Yes (*4)	Yes (*4)	Yes (*4)	Yes (*4)
WebClient	Not required because the functions are not used.	Yes (*2)	Yes (*2)	-	–

*1: 10 2016 LTSB: Windows 10 Enterprise 2016 LTSB
10 LTSC 2019: Windows 10 Enterprise LTSC 2019

10 LTSC 2021: Windows 10 Enterprise LTSC 2021
WS 2016: Windows Server 2016
WS 2019: Windows Server 2019
WS 2022: Windows Server 2022
Yes: Services that can be stopped
No: Service that must not be stopped
–: Services that do not exist in the OS

*2: Because the Startup type for the Windows service is set to Manual with the initial OS setting, the IT Security Tool does not change this setting.
*3: Because the Startup type for the Windows service is set to Disabled with the initial OS setting, the IT Security Tool does not change this setting.
*4: Because the Startup type for the Windows service is set to Automatic with the initial OS setting, the Startup type is changed to Disabled by the IT Security Tool.

Table 3.3-4 Windows Services That can be Stopped on a File Server and Domain Controller (with IT Security Version 1.0)

Service	Reason	Windows OS (*1)
		WS 2016/WS 2019/WS 2022
DHCP Client	Unnecessary in the product	No
Windows Error Reporting Service	Unnecessary in the product	Yes (*2)
IP Helper	Unnecessary in the product	Yes (*3)
IPsec Policy Agent	Unnecessary in the product	Yes (*2)
Offline Files	Unnecessary in the product	Yes (*4)
Remote Registry	Not required because the functions are not used.	Yes (*3)
Shell Hardware Detection	Not required because the functions are not used.	Yes (*3)

*1: WS 2016: Windows Server 2016
WS 2019: Windows Server 2019
WS 2022: Windows Server 2022
Yes: Services that can be stopped
No: Service that must not be stopped
–: Services that do not exist in the OS

*2: Because the Startup type for the Windows service is set to Manual with the initial OS setting, the IT Security Tool does not change this setting.
*3: Because the Startup type for the Windows service is set to Automatic with the initial OS setting, the Startup type is changed to Disabled by the IT Security Tool.
*4: Because the Startup type for the Windows service is set to Disabled with the initial OS setting, the IT Security Tool does not change this setting.

Caution

In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.4 IT Environment Settings Common to IT Security Versions 2.0 and 1.0

This section describes the IT environment settings that are common to IT security versions 2.0 and 1.0. There may be cases where it is not possible to implement certain security functions depending on the conditions of the individual systems. For this reason, examine whether implementation is possible for each function before the implementation.

3.4.1 Disabling NetBIOS over TCP/IP

It is recommended to disable NetBIOS because attackers may be able to acquire a list of services running on the target computer and a list of users by using NetBIOS.

Cautions

Keep the following points in mind when disabling NetBIOS over TCP/IP.

- The computer name and station name must be the same.
- The computer name must be resolved by the DNS or HOSTS file.

3.4.2 HDD Password Function by BIOS

This function is provided in most PCs and protects HDD by using the ATA command that controls HDD. In normal BIOS password setting, it is possible to refer to data in HDD by removing the hard disk from a PC and connecting it to another PC. A HDD password locks the HDD itself, and it prohibits reading data even if HDD is removed and connected to another computer. Even if a PC is stolen, there is no fear that important data of the product leaks from the stolen PC. It is impossible to recover the data in the HDD once the HDD password is forgotten, and the password is required to enter when starting the computer. For this reason, this function must be introduced with greatest care.

Please contact the PC manufacturer whether or not this function is provided and how to set the function.

3.5 Group Policy Settings Common to IT Security Versions 2.0 and 1.0

Some group policy setting items are common to IT security versions 2.0 and 1.0. This section describes the common setting items. You also need to check the settings that are specific to each of security versions 2.0 and 1.0.

Because some security functions cannot be applied depending on the circumstances of individual systems, consider whether the functions can be applied to your system before you introduce them.

3.5.1 Disabling the Built-in Administrator Account or Changing its User Name

We recommend that you disable the built-in Administrator account or change its user name because the built-in accounts that are created during the installation of windows are easy targets of password cracking.

Cautions (when Disabling the Built-in Administrator Account)

You must consider the following points when you disable the built-in Administrator account:

- Disable the built-in Administrator account after creating a user with administrative rights.
- Be careful not to include root, su, admin, and other words meaning administrator in the name of user with administrator rights.
- Securely control users with administrator rights because they are required for operations.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

Cautions (when Changing the User Name of the Built-in Administrator Account)

You must consider the following points when you change the name of the built-in Administrator account:

- Create a user with administrator rights for normal maintenance.
- Be careful not to include root, su, admin, and other words meaning administrator in the changed user name and in the name of the user with administrator rights you create.
- Securely control users with administrator rights
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.5.2 Applying the Software Restriction Policies

The software restriction policies function of Windows restricts the execution of programs by setting the following types of rules:

- Restriction on path
- Restriction on hash
- Restriction on certificate
- Restriction on the Internet zone

In the product, path rules are applied to provide an environment where users can run only the specified programs. This prevents illegal execution of programs even if harmful programs are copied in a temporary folder or other locations of the computer.

The IT Security Tool supports Restriction on path. If this restriction is applied, other coexisting packages may not run.

Settings

To allow only the specified programs to run, folder paths are added and rules are deleted as follows:

Folder paths to be added

- `%ALLUSERSPROFILE%\Microsoft\Windows\Templates` (*1)
- `%ALLUSERSPROFILE%\Templates` (*1)
- `%ALLUSERSPROFILE%\Yokogawa\IA\iPCS\Products\ChronusENG\Data\Projects` (*1) (*2)
- `%localappdata%\Microsoft\OneDrive\*\FileSyncConfig.exe` (*3)
- `%localappdata%\Microsoft\OneDrive\OneDrive.exe` (*3)
- `%ProgramFiles%` (*4)
- `%ProgramFiles(x86)%`(*5)
- `%ProgramW6432%`(*6)
- `%ProgramFiles%\Yokogawa\IA\iPCS\Platform\Security\PROGRAM` (*4)
- `%ProgramFiles(x86)%\Yokogawa\IA\iPCS\Platform\Security\PROGRAM` (*5)
- `%ProgramFiles(x86)%\YOKOGAWA\IA\iPCS\Products\ProSafe-RS\Program` (*5)
- `%SystemRoot%` (*7)
- ProSafe-RS installation folder
- `%ProgramFiles32%\Trinity Integrated Systems\iDefine x.xx.x Yokogawa` (*8)

Rules to be deleted

- "lnk" and "mdb" are deleted from [Designated File Types Properties].

*1: %ALLUSERSPROFILE% refers to the following folder. This example is when the system drive is drive C.
`C:\ProgramData`
*2: This path is added when the Automation Design Master Database is to be stored in the default location.
*3: Only for Windows 10
*4: %ProgramFiles% refers to the following folder. This example is when the system drive is drive C.
`C:\Program Files`
*5: %ProgramFiles(x86)% refers to the following folder. This example is when the system drive is drive C.
`C:\Program Files(x86)`
*6: %ProgramW6432% refers to the following folder. This example is when the system drive is drive C.
`C:\Program Files`
*7: %SystemRoot% refers to the following drive. This example is when the system drive is drive C.
`C:\Windows`

*8: This is the folder path when iDefine is installed in the default folder. %ProgramFiles32% refers to the following folder. This example is when the system drive is drive C.
`C:\ProgramFiles(x32)`
`x.xx.x` is the version number of iDefine.

Cautions

IMPORTANT

When software restriction policies are applied, observe the following points: To start the installer from the ProSafe-RS software medium, right-click the icon of the installer and select [Run as Administrator]. To run a non-ProSafe-RS program, you also need to run it by selecting [Run as Administrator].

In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.5.3 Applying the Audit Policy

Collected account logon conditions and events related to security serve as data useful in detecting abnormal system conditions in early stages and to trace causes of troubles when problems related to security occur. It is recommended to set appropriate audit policies.

With the Windows default setting, audit data is not collected.

Settings

The following table shows the settings.

Table 3.5.3-1 Settings

Policy	Settings
Audit account logon events	Both the Success and Failure check boxes are selected.
Audit account management	Both the Success and Failure check boxes are selected.
Audit object access	The Failure check box is selected.
Audit system events	Both the Success and Failure check boxes are selected.
Audit directory service access	Both the Success and Failure check boxes are selected.
Audit process tracking	The Success check box is selected.
Audit policy change	Both the Success and Failure check boxes are selected.
Audit logon events	Both the Success and Failure check boxes are selected.
Audit privilege use	Both the Success and Failure check boxes are selected.

Cautions

Keep the following points in mind when applying the audit policies.

- If the number of event types collected is increased, the system performance is affected.
- The number of generated events varies depending on the types of collected events and system operations. Determine the event collection size appropriate for the system operation conditions.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.5.4 Applying the StorageDevicePolicies Function

By using the StorageDevicePolicies function of Windows, you can set removable storage media connected on USB ports as read-only devices. You can use this function to prevent theft of data by unauthorized users. You can use the StorageDeviceCTL utility of the product to temporarily grant write permissions to users.

SEE ALSO For more information about StorageDeviceCTL, refer to:

6.11, “Other Utility Programs” on page 6-51

Setting

The following table shows the setting when IT security version 2.0 is applied.

Table 3.5.4-1 Setting

Policy	Setting
Removable Disks: Deny write access	Enabled

Cautions

Keep the following points in mind when applying the StorageDevicePolicies function.

In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.5.5 Disabling USB Storage Devices

This function disables the use of USB storage devices such as USB memories. You can use this function to prevent theft of data by unauthorized users.

You can use the StorageDeviceCTL utility of the product to temporarily grant write permissions to users.

SEE ALSO For more information about StorageDeviceCTL, refer to:

6.11, “Other Utility Programs” on page 6-51

Settings

The following table shows the settings when IT security version 2.0 is applied.

Table 3.5.5-1 Settings

Policy	Setting
Floppy Drives: Deny execute access	Enabled
Floppy Drives: Deny read access	Enabled
Floppy Drives: Deny write access	Enabled
Removable Disks: Deny execute access	Enabled
Removable Disks: Deny read access	Enabled
Removable Disks: Deny write access	Enabled
WPD Devices: Deny read access	Enabled
WPD Devices: Deny write access	Enabled

Cautions

Keep the following points in mind when disabling USB storage devices.

- If volumes (partitions) other than the system volume or internal hard disk drives are recognized as portable devices, you may not be able to access them. Before disabling the USB storage devices, or if the problem occurs, follow steps to restore access to the required devices.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

How to Restore Access to the Required Devices

Follow these steps to restore access to the required devices:

1. Start Windows PowerShell and enter `mmc devmgmt.msc`.
   Device Manager appears.
2. Expand the node of [Portable devices] and make sure that no devices other than the connected USB storage device are connected.
3. If devices other than the connected USB storage device are connected, update BIOS or UEFI.

TIP

If BIOS or UEFI cannot be updated, or if the problem still exists even after the update, follow these steps:

1. From the Start menu, right-click the Command Prompt and select [Run as administrator].
2. From the opened command prompt, execute the following command: The command argument n represents the Bus Number.
   - File server or domain controller:
     `<ProSafe-RS installation medium>:\ProSafe-RS\SECURITY\TreatAsNonRemovableDisk.cmd n`
   - A computer on which ProSafe-RS software is installed:
     `<System drive>:\Program Files (x86)\YOKOGAWA\IA\iPCS\Platform\SECURITY\PROGRAM\TreatAsNonRemovableDisk.cmd n`
3. Restart the computer.

Follow these steps if you want to check the Bus Number:

1. From the Start menu, select [Run] and enter `diskmgmt.msc`.

   Disk Management appears.
2. In the framed area of the following figure, right-click and select [Properties].
   The properties of the corresponding disk drive appear.

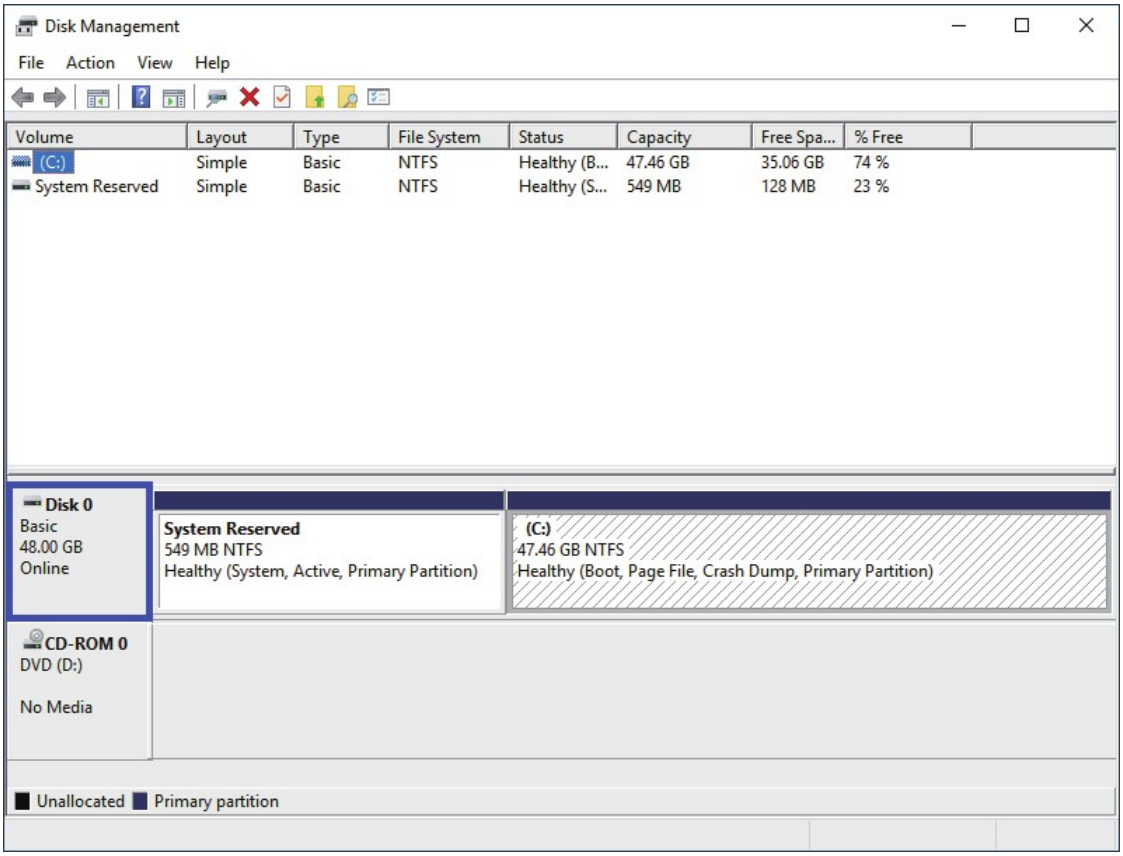


Figure 3.5.5-1 Disk Management

3. On the [General] tab of the displayed properties, check the value of Bus Number displayed in [Location:].
   - If there is only one internal disk drive, or if all internal disk drives have the same Bus Number, use the displayed value.
   - If there are multiple internal disk drives whose Bus Numbers are different from each other, use the IT Security Tool to set disabling USB storage devices. In Explorer, check the inaccessible disk drive, on the Disk Management window, check the Bus Number value of the disk drive and use it. For example, if the F drive is disabled, view and check the properties of the disk drive that contains the F drive.

3.5.6 Applying the Account Lockout Policy

This function is effective to protect the product from attacks such as online cracking.

Settings

The following table shows the settings.

Table 3.5.6-1 Settings

Policy	Setting
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes
Account lockout duration	15 minutes

Cautions

Keep the following points in mind when applying the account lockout policies.

- If this policy is applied and you fail to log on repeatedly, logging on to that user account will be disabled until the time set for "Reset account lockout counter after" elapses.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.5.7 Windows Update Delivery Optimization

Windows Update Delivery Optimization is a feature of Windows 10, Windows Server 2019, and Windows Server 2022. This feature allows Windows updates and Windows store applications to be downloaded from Microsoft servers as well as computers on the network that have the updates and applications installed. In addition, you can send from your computer to other computers on the network.

However, because Windows updates may be applied to your computer or other computers on the network, or a restart may occur unexpectedly, make a setting to prevent updates and applications from being sent or received between your computer and the computer on your network.

The following table shows the setting.

Table 3.5.7-1 Setting

Policy	OS	Setting
Download Mode	Windows 10 Enterprise 2016 LTSB Windows Server 2022	Enabled HTTP only
	Windows 10 Enterprise LTSC 2019 Windows 10 Enterprise LTSC 2021 Windows Server 2019	Enabled Bypass

3.5.8 Disabling Windows Defender

Disable Windows Defender.

The name of Windows Defender displayed in Local Group Policy Editor varies depending on the OS version and language. Please replace it as appropriate. OS version can be checked on the System window calling from the Start menu.

The following table shows the Windows Defender name for each OS version.

Table 3.5.8-1 OS version and Windows Defender name

OS version	Name
1607 or earlier	Windows Defender
1703 to 1909	Windows Defender Antivirus
2004 or later	Microsoft Defender Antivirus

The following table shows the setting.

Table 3.5.8-2 Setting

Policy	Setting
Turn off Windows Defender	Enabled

3.5.9 Disabling Shared experiences

Shared experiences is a feature of Windows 10 Enterprise LTSC 2019 and Windows 10 Enterprise LTSC 2021.

There are two functions: sharing between devices that open applications on devices to send and receive messages, and nearby sharing that shares files and web page URL through Bluetooth or Wi-Fi.

The following table shows the setting.

Table 3.5.9-1 Setting

Policy	OS	Setting
Continue experiences on this device	Windows 10 Enterprise LTSC 2019 Windows 10 Enterprise LTSC 2021	Disabled
	OS other than the above	Not configured

3.5.10 Enabling SMB Signing

By enabling SMB signing, packets sent and received by SMB are digitally signed to prevent tampering and destruction.

The following table shows the setting.

Table 3.5.10-1 Setting

Policy	Setting
Microsoft Network Server: Always digitally sign communications	Enabled

Cautions

Note the following points when enabling SMB signing.

- It is supported for computers on which ProSafe-RS R4.07 or later is installed. In the case of a file server, it is supported for computers built with a server OS supported by ProSafe-RS R4.07 or later.
- The following operations need to be performed on all the above computers which are contained in the ProSafe-RS system.
- In the following cases, set it only if all products support enabling SMB signing.
  - There is software for system products that coexist with ProSafe-RS, or system products that work in linkage.
  - ProSafe-RS of different revisions are mixed in the system.
- Set this item in the Local Group Policy Editor. Follow these steps to set it:

1. Sign in as an administrative user.
2. Start the Command Prompt.
3. Enter `gpedit.msc`.
   Local Group Policy Editor appears.
4. In the left pane, select [Computer Configuration] > [Windows Settings] > [Security Settings] > [Local Policies] > [Security Options.]
5. Enable the setting value of the desired policy.

3.5.11 Prevent illegal dll from loading

The following setting can mitigate attacks of loading illegal dll.

This setting is configured automatically when you install the ProSafe-RS software instead of setting with the IT Security Tool.

The following table shows the setting.

Table 3.5.11-1 Setting

Registry entry	Setting
CWDIllegalInDllSearch	2

Cautions

Loading a dll from the current working directory (current directory) is blocked if all of the following conditions are met:

- The application in a local folder on the local computer is running.
- The current working directory (current directory) of the above application is specified to a folder on the remote computer.

3.6 Group Policy Settings in IT Security Version 2.0

This section describes the group policy settings in IT security version 2.0. There may be cases where it is not possible to implement certain security functions depending on the conditions of the individual systems. For this reason, examine whether implementation is possible for each function before the implementation.

3.6.1 Applying the Password Policies

The strength of security for user authentication changes significantly depending on the set password. It is recommended to secure minimum password strength by applying the password policies.

Settings

The following table shows the settings.

Table 3.6.1-1 Settings

Policy	Setting
Minimum password length	12 characters or more
Minimum password age	One day
Validity period of password	70 days
Enforce password history	2 passwords
Password must meet complexity requirements	Enabled
Store password using reversible encryption	Disabled

Cautions

Keep the following points in mind when applying the password policies.

- If the password policies are made stricter, not only the load of password management on users but also the load of operation administrators to manage user's passwords increases.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.6.2 User Rights Assignment

With this function, only the specified users or groups are allowed to perform a certain operation.

Settings

Table 3.6.2-1 Settings

Policy (*1)	Group to delete	Group to add
Access this computer from the network	All the registered accounts	Administrators Authenticated Users Enterprise Domain Controllers
Add workstations to domain	Authenticated User	Administrators

*1: This setting is for domain controllers only.

3.6.3 Security Options

Various security options are enabled or disabled.

Settings

The following table shows the settings.

Table 3.6.3-1 Settings

Policy	Setting
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Domain controller: Allow server operators to schedule tasks(*1)	Disabled
Domain controller: Refuse machine account password changes(*1)	Disabled
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session is locked	User display name, domain and user names
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Prompt user to change password before expiration	Enabled 14 days
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Server SPN target name validation level	Enabled Accept if provided by client
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)	Disabled
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Enabled Highest protection, source routing is completely disabled
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)	Disabled
MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	Enabled 3
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled

Continues on the next page

Table 3.6.3-1 Settings (Table continued)

Policy	Setting
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network security: Allow Local System to use computer identity for NTLM	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled
Network security: Force logoff when logon hours expire(*1)	Enabled
Network security: LAN Manager authentication level	Enabled Send NTLMv2 response only
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled • Require NTLMv2 session security • Require 128-bit encryption Both check boxes are selected.
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Enabled • Require NTLMv2 session security • Require 128-bit encryption Both check boxes are selected.
Network security: Do not store LAN Manager hash value on next password change	Enabled
Shutdown: Allow system to be shut down without having to log on	Disabled
User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Enabled Prompt for consent on the secure desktop

*1: This setting is for domain controllers only.

Cautions

- You can check the application of the four setting items beginning with MSS: that are set as Security Options by using the gpresult command.
- If you set Interactive logon: Machine inactivity limit, the session will be locked if no operation is made for 900 seconds.
- In Windows Server 2019 and Windows Server 2022, if “User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode” is set to “Prompt for consent on secure desktop”, a User Account Control dialog box appears when you perform the shutdown or restart operation from the Start menu.

3.6.4 Advanced Audit Policy Configuration

Collected account logon conditions and events related to security serve as data useful in detecting abnormal system conditions in early stages and to trace causes of troubles when problems related to security occur. With IT security version 2.0, more detailed audit policy configuration is possible. Each setting item is described as follows.

Account Logon

The following table shows the setting.

Table 3.6.4-1 Setting

Policy	Setting
Audit Credential Validation	Both the Success and Failure check boxes are selected.

Account Management

The following table shows the setting.

Table 3.6.4-2 Setting

Policy	Setting
Audit Computer Account Management	The Success check box is selected.
Audit Other Account Management Events	Both the Success and Failure check boxes are selected.
Audit Security Group Management	Both the Success and Failure check boxes are selected.
Audit User Account Management	Both the Success and Failure check boxes are selected.

Detailed Tracking

The following table shows the setting.

Table 3.6.4-3 Setting

Policy	Setting
Audit Process Creation	The Success check box is selected.
Audit RPC events	Both the Success and Failure check boxes are cleared. (*1)

*1: In the case of domain controller and file server, both the Success and Failure check boxes are selected.

DS Access

These settings are for domain controllers only.

Table 3.6.4-4 Settings

Policy	Setting
Audit Directory Service Access	Both the Success and Failure check boxes are selected.
Audit Directory Service Changes	Both the Success and Failure check boxes are selected.

Logon/Logoff

The following table shows the setting.

Table 3.6.4-5 Setting

Policy	Setting
Audit Account Lockout	The Success check box is selected.
Audit Logoff	The Success check box is selected.
Audit Logon	Both the Success and Failure check boxes are selected.
Audit Other Logon/Logoff Events	Both the Success and Failure check boxes are selected.
Audit Special Logon	The Success check box is selected.

Object Access

The following table shows the setting.

Table 3.6.4-6 Setting

Policy	Setting
Audit Application Generated	Both the Success and Failure check boxes are cleared. (*1)
Audit Removable Storage	Both the Success and Failure check boxes are selected.

*1: In the case of domain controller and file server, both the Success and Failure check boxes are selected.

Policy Change

The following table shows the setting.

Table 3.6.4-7 Setting

Policy	Setting
Audit Policy Change	Both the Success and Failure check boxes are selected.
Audit Authentication Policy Change	Both the Success and Failure check boxes are selected.
Audit Filtering Platform Policy Change	Both the Success and Failure check boxes are selected.
Audit MPSSVC Rule-Level Policy Change	Both the Success and Failure check boxes are selected.
Audit Other Policy Change Events	Both the Success and Failure check boxes are selected.

Privilege Use

The following table shows the setting.

Table 3.6.4-8 Setting

Policy	Setting
Audit Sensitive Privilege Use	Both the Success and Failure check boxes are selected.

System

The following table shows the setting.

Table 3.6.4-9 Setting

Policy	Setting
Audit Other System Events	Both the Success and Failure check boxes are selected.
Audit Security State Change	Both the Success and Failure check boxes are selected.
Audit Security System Extension	Both the Success and Failure check boxes are selected.
Audit System Integrity	Both the Success and Failure check boxes are selected.
Audit IPsec Driver (*1)	Both the Success and Failure check boxes are selected.

*1: This setting is for domain controllers only.

3.6.5 Administrative Template

This section describes the group policy settings that are defined in the administrative template.

Personalization (Control Panel)

Setting

The following table shows the setting.

Table 3.6.5-1 Setting

Policy	Setting
Prevent enabling lock screen camera	Enabled
Prevent enabling lock screen slide show	Enabled

WLAN Settings (Network)

Setting

The following table shows the setting.

Table 3.6.5-2 Setting

Policy	Setting
Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services	Disabled

Audit Process Creation (System)

Setting

The following table shows the setting.

Table 3.6.5-3 Setting

Policy	Setting
Include command line in process creation events	Disabled

TIP

If this option is enabled, the command line information of each process will be recorded to the security event log in text format as part of the Audit Process Creation event 4688, "A new process has been created." For example, if you set a password by using the CreateProSafeProcess tool, the password specified as an argument is recorded in the event log.

Group Policy (System)

Setting

The following table shows the setting.

Table 3.6.5-4 Setting

Policy	Setting
Configure registry policy processing	The check box of Process even if the Group Policy objects have not changed is selected.

Internet Communication Management (System)

Setting

The following table shows the setting.

Table 3.6.5-5 Setting

Policy	Setting
Turn off access to the Store	Enabled
Turn off downloading of print drivers over HTTP	Enabled
Turn off Event Viewer "Events.asp" links	Enabled
Turn off Internet download for Web publishing and online ordering wizards	Enabled
Turn off printing over HTTP	Enabled
Turn off Search Companion content file updates	Enabled
Turn off the "Publish to Web" task for files and folders	Enabled
Turn off the Windows Customer Experience Improvement Program	Enabled
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled

Logon (System)

Settings

The following table shows the settings.

Table 3.6.5-6 Settings

Policy	Setting
Do not display network selection UI	Enabled
Do not enumerate connected users on domain-joined computers	Enabled
Enumerate local users on domain-joined computers	Disabled
Turn off app notifications on the lock screen	Enabled

Mitigation Options (System)

Setting

The following table shows the setting.

Table 3.6.5-7 Setting

Policy	Setting
Untrusted Font Blocking	Enabled Block untrusted fonts and log events

Cautions

If this setting is enabled, fonts that are not installed in %Windir%\Font (normally, C:\Windows \Font) cannot be used. In that case, install the fonts to be used in the above folder. You can install fonts by right-clicking the font and selecting [Install].

Power Management (System)

Settings

The following table shows the settings.

Table 3.6.5-8 Settings

Policy	Setting
Turn Off the Display (On Battery)	Enabled 0
Turn Off the Display (Plugged In)	Enabled 0

User Profile (System)

Setting

The following table shows the setting.

Table 3.6.5-9 Setting

Policy	Setting
Turn off the advertising ID	Enabled

App Privacy (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-10 Setting

Policy	Setting
Let Windows apps access account information	Enabled Force Deny
Let Windows apps access call history	Enabled Force Deny
Let Windows apps access contacts	Enabled Force Deny
Let Windows apps access email	Enabled Force Deny
Let Windows apps access location	Enabled Force Deny
Let Windows apps access messaging	Enabled Force Deny
Let Windows apps access motion	Enabled Force Deny

Continues on the next page

Table 3.6.5-10 Setting (Table continued)

Policy	Setting
Let Windows apps access the calendar	Enabled Force Deny
Let Windows apps access the camera	Enabled Force Deny
Let Windows apps access the microphone	Enabled Force Deny
Let Windows apps access trusted devices	Enabled Force Deny
Let Windows apps control radios	Enabled Force Deny
Let Windows apps sync with devices (*1)	Enabled Force Deny
Let Windows apps communicate with unpaired devices(*2)	Enabled Force Deny

*1: If the OS is Windows 10 Enterprise 2016 LTSB or Windows Server 2016
*2: If the OS is Windows 10 Enterprise LTSC 2019, Windows 10 Enterprise LTSC 2021, or Windows Server 2019 or later server OS

App Runtime (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-11 Setting

Policy	Setting
Block launching Windows Store apps with Windows Runtime API access from hosted content	Enabled

Cautions

This policy disables starting of Windows store applications that are directly accessed by Windows runtime API from Web content.

AutoPlay Policies (Windows Component)

These policies prevent automatic execution of programs from external media. This setting is effective as a measure against viruses that infect computers through USB memory devices (USB worms).

Setting

The following table shows the setting.

Table 3.6.5-12 Setting

Policy	Setting
Turn off Autoplay	Enabled All drives
Disallow Autoplay for non-volume devices	Enabled

Cautions

- If the AutoRun function for the drive is disabled, the installation menu does not start just by inserting the software medium of the product.

- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

Cloud Content (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-13 Setting

Policy	Setting
Do not show Windows tips	Enabled
Turn off Microsoft consumer experiences	Enabled

Data Collection and Preview Builds (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-14 Setting

Policy	Setting
Allow Telemetry (*1)	Enabled 0 - Security [Enterprise Only]
Allow diagnostic data(*2)	Enabled Diagnostic data off (not recommended)
Disable pre-release features or settings	Disabled
Do not show feedback notifications	Enabled
Toggle user control over Insider builds	Disabled

*1: If the OS is one of the following:
- Windows 10 Enterprise 2016 LTSB
- Windows 10 Enterprise LTSC 2019
- Windows 10 Enterprise LTSC 2021
- Windows Server 2016
- Windows Server 2019

*2: If the OS is Windows Server 2022

Cautions

If the OS is Windows 10 Enterprise LTSC 2019, Windows 10 Enterprise LTSC 2021, Windows Server 2019, or Windows Server 2022, the policy “Disable pre-release features or settings” does not appear in the Local Group Policy Editor. Check the current application of the policy by running the `gpresult` command as an alternative measure.

Event Log Service (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-15 Setting

Policy	Setting
Specify the maximum log file size (KB)	Enabled 32768 KB

File Explorer (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-16 Setting

Policy	Setting
Turn off heap termination on corruption	Disabled

HomeGroup (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-17 Setting

Policy	Setting
Prevent the computer from joining a homegroup	Enabled

OneDrive (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-18 Setting

Policy	Setting
Prevent the usage of OneDrive for file storage	Enabled
Save documents to OneDrive by default (Save documents to the local PC by default)	Enabled

Remote Desktop Service (Windows Component)

Settings

The following table shows the settings.

Table 3.6.5-19 Settings

Policy	Setting
[Remote Desktop Connection Client] \ Do not allow passwords to be saved	Enabled
[Remote Desktop Session Host] \ [Device and Resource Redirection] \ Do not allow drive redirection	Enabled
[Remote Desktop Session Host] \ [Security] \ Require secure RPC communication	Enabled
[Remote Desktop Session Host] \ [Security] \ Require user authentication for remote connections by using Network Level Authentication	Enabled

Search (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-20 Setting

Policy	Setting
Allow Cortana	Disabled
Don't search the web or display web results in Search	Enabled
Don't search the web or display web results in Search over metered connections	Enabled

Software Protection Platform (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-21 Setting

Policy	Setting
Turn off KMS Client Online AVS Validation	Enabled

Store (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-22 Setting

Policy	Setting
Turn off Automatic Download of updates on Win8 machines	Enabled
Turn off Automatic Download and Install of updates	Enabled
Turn off the offer to update to the latest version of Windows	Enabled
Turn off the Store application	Enabled

Sync Your Settings (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-23 Setting

Policy	Setting
Do not sync Apps	Enabled
Do not sync start settings	Enabled

Windows Error Reporting (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-24 Setting

Policy	Setting
Automatically send memory dumps for OS-generated error reports	Disabled

Windows Logon Options (Windows Component)

Setting

The following table shows the setting.

Table 3.6.5-25 Setting

Policy	Setting
Sign-in last interactive user automatically after a system-initiated restart	Disabled

3.6.6 User Configuration - Administrative Template

Notifications (Taskbar and Start Menu)

Setting

The following table shows the setting.

Table 3.6.6-1 Setting

Policy	Setting
Turn off toast notifications on the lock screen	Enabled

3.7 Group Policy Settings in IT Security Version 1.0

This section describes the group policy settings in IT security version 1.0. There may be cases where it is not possible to implement certain security functions depending on the conditions of the individual systems. For this reason, examine whether implementation is possible for each function before the implementation.

3.7.1 Hiding the Last Logon User Name

You can hide the last logon user name on the logon dialog box to prevent leakage of valid user names in the system.

Caution

Keep the following points in mind when hiding the last logon user name.

- You must enter a user name on every logon attempt if you apply this security measure.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.7.2 Applying AutoRun Restrictions

This restriction prevents automatic execution of programs when a DVD-ROM or other medium is inserted to the drive or a USB port. This is an effective measure against virus (USB worm) infecting computers via USB memory.

Setting Values

The AutoRun function is disabled for all drives.

Cautions

Keep the following points in mind when applying AutoRun restrictions.

- The installation menu does not start just by inserting the software medium of the product.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.7.3 Changing the LAN Manager Authentication Level

Windows has LM authentication, NTLM authentication and NTLMv2 authentication methods for backward compatibility.

For the environment of the product, use of NTLMv2 authentication is recommended. LM authentication is not recommended since its method of hashing user's password (LM hash algorithm) is very vulnerable.

Setting

The following table shows the setting.

Table 3.7.3-1 Setting

Policy	Setting
Changing the LAN Manager Authentication Level	Send NTLMv2 response only
Do not allow storage of passwords and credentials for network authentication	Enabled
Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security Require 128-bit encryption
Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security Require 128-bit encryption
Let Everyone permissions apply to anonymous users	Disabled

Cautions

- Ensure that the settings of “Minimum session security for NTLM SSP based (including secure RPC) clients” and “Minimum session security for NTLM SSP based (including secure RPC) servers” are consistent on all terminals.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.7.4 Applying the Password Policies

The strength of security for user authentication changes significantly depending on the set password. It is recommended to secure minimum password strength by applying the password policies.

■ Settings

The following table shows the settings.

Table 3.7.4-1 Settings

Policy	Settings
Minimum password length	12 characters or more
Change prohibition period of password	One day
Validity period of password	90 days
Storage of password history	24 passwords stored (25 password types or more are required)
Password must meet complexity requirements	Enabled
Store password using reversible encryption	Disabled

■ Cautions

The cautions for applying the password policies are the same as those of IT security version 2.0.

SEE ALSO For more information about notes on the password policy in IT security version 2.0, refer to:

"■ Cautions" on page 3-40

4. Selection of Security Functions

In order to set security functions, it is necessary to take various items into consideration. This chapter explains the items to be considered and model cases that serve as reference when setting security functions.

4.1 Items to be Considered Before Setting Security Functions

After installing the ProSafe-RS software, you must configure the security settings of the computer to strengthen IT security. Even if the security settings of ProSafe-RS installed computers are controlled collectively by a domain controller, you must perform this configuration at least once on every computer.

When the project database is built on a file server or when user management is consolidated by a Windows domain controller, the configuration of IT security settings is required also on the file server or domain controller.

This section describes the items that you must consider before configuring the security settings.

Considerations on Determining Security Functions

The following items need to be considered according to the actual implementations.

These items should be determined before installing the software of the product.

- IT security version
- Security Model
- Windows user management type
- User authentication mode

Selecting IT Security Version

Select either of the following versions according to the extent of configuration for security measures.

Table 4.1-1 Selecting IT Security Version

IT security version	Selection Criterion
2.0	This version includes more security policies compared to the security measures that had been offered until ProSafe-RS R4.02. In addition, the administrative template for group policies is included as the target of security configuration. The Legacy model is no longer supported in IT security version 2.0.
1.0	This version offers the same security measures as ProSafe-RS R4.02 and earlier versions.

Selecting Security Model

A security model needs to be selected from the following three types.

Table 4.1-2 Selecting Security Model

Security Model	Selection Criterion
Legacy Model	Select this model when upgrading the system from an RS project of ProSafe-RS R4.02 or earlier without changing the existing security settings or when sharing Windows users among multiple operators. The Legacy model can be selected only with IT security version 1.0. If this model is selected, the system remains vulnerable against information leak and attacks by worms and viruses.

Continues on the next page

Table 4.1-2 Selecting Security Model (Table continued)

Security Model	Selection Criterion
Standard Model (Recommended)	It is recommended to select this model unless you have a specific reason not to. This model provides minimum security settings necessary for the product, considering secure operation of the system as well as collaboration with other systems.
Strengthened Model	Select this model when security level higher than the Standard model is required. Consult Yokogawa agent when implementing this model.

● Windows User Management

Select Windows user management type according to the system size and configuration from the following four types.

Table 4.1-3 Selecting User Management Type

User Management Type	Selection Criterion
Standalone Management	This type is suitable for relatively small-scale systems. When this type is selected, the user accounts and passwords of all computers in the system need to be kept consistent.
Domain Management	This type is suitable for systems that implement a centralized user management. When this type is selected, it is recommended to set a new, dedicated domain controller when constructing the system.
Combination Management	This type is suitable for the system where user management is centralized but some users are allowed to be independently managed in local computers.
Linked Domain Management	This type is suitable for the system where user management is centralized but some users are allowed to be independently managed in local computers. When installing new software for this product, it is recommended to use the linked domain management instead of the domain management or the combination management.

● User Authentication Mode

When the Access Control and Operation History Management Package is used, you can select either of the following user authentication modes according to the operation conditions and security policies of the system.

Table 4.1-4 Selecting User Authentication Mode

User Authentication Mode	Selection Criterion
ProSafe Authentication Mode	Select this mode when Windows users and ProSafe-RS users are authenticated separately.
Windows Authentication Mode	Select this mode when Windows users and the users who perform system engineering or maintenance works are authenticated together. This mode is suitable for systems requiring a higher security level.

When Windows authentication mode is selected, only one authentication is performed before operating the SENG.

■ Precautions when Setting Security Functions

The following table lists precautions to be observed when setting security measures.

Table 4.1-5 Precautions when Setting Security Functions

Security function	Item to be considered
Software Restriction Policies	If the software restriction policies are set, programs added for the purpose of collaboration and coexistence may not run. You need to add policies of the programs to the software restriction policies. Follow these steps to add policies. 1. Logon the PC as an administrative user. 2. Open the Administrative Tools. 3. At Local Security Policy, select [Software Restriction Policies] > [Additional Rules]. 4. Add the policy of a newly added program.
PSF_PROCESS Password	Do not change the password of PSF_PROCESS.
StorageDevicePolicies function/ Disabling USB storage devices	If you apply the StorageDevicePolicies function or disable USB storage devices, you cannot back up data into storage devices such as USB memories. When you take a backup of the operation history database or other data into a storage device, use the StorageDeviceCTL command.
Disabling NetBIOS over TCP/IP	If you disable NetBIOS over TCP/IP, you cannot resolve names by broadcasting. Because of this, the following problems arise in environments with standalone management. • When you try to open a file in a file server from SCS Manager, you cannot see the file server. • If the cache file is stored in another PC, you cannot see the cache file. To solve these problems, use the HOSTS file or LMHOSTS file.

5. Precautions on Operations

This section describes the precautions related to security when operating the product.

5.1 Windows Account Management

Two types of Windows account management are assumed, common account management and individual account management, considering sharing of the user accounts often used in the systems that were built before the security functions are introduced.

Common Account Management and Individual Account Management

The following table shows the differences between the common account management and individual account management.

Table 5.1-1 Common Account Management and Individual Account Management

Account management method	Operation form	Convenience of operation		Security strength	
Common account management	A Windows account is shared by multiple users.	High	The same operability as the systems that were built before the security functions are introduced.	Low	Highly anonymous and disadvantageous.
Individual account management	A Windows account is assigned to a single user.	Low	Windows logoff and logon are required at personnel shift, and thus cumbersome compared to the systems that were built before the security functions are introduced.	High	Advantageous because access control of each user is possible.

5.1.1 Common Account Management

The common account management is highly convenient to operate because it is similar to the conventional account management of the systems that were built before the security functions are introduced. However, from the security point of view, anonymity is high and security strength level is low. When applying the common account management, take personnel education and security of operation environment fully into consideration.

Use of Accounts

If the common accounts are used, it is recommended to group accounts by rights of users and use common accounts within a group. By grouping by rights of users, it becomes possible to prohibit operations on the product by users without rights and to narrow down user groups when tracing the trouble occurrence. It is considered that more usable trace data is obtained compared to the case when common accounts are used among all users.

Password Management

Considering security, it is recommended to change passwords periodically. It is possible to handle password cracking attacks by periodically changing passwords. If common accounts are used, it is recommended to change passwords at the timing when members using the common accounts are changed. By changing passwords, illegal access from previously authorized people is prevented.

Automatic Logon Function

Do not use the automatic logon function of Windows unless CENTUM VP coexists on the PC.

Otherwise, persons without rights to the ProSafe-RS system may inadvertently use engineering functions, and so on.

5.1.2 Individual Account Management

With the individual account management, it is possible to minimize rights on accounts by specifying PC users. Moreover, it is possible to trace trouble occurrence more efficiently because users can be identified. However, the individual account management is different from conventional operations on several points, such as Windows logoff/logon becomes necessary at personnel shift. More careful consideration is required when implementing the individual account management.

Account Maintenance

If user rights are changed, it is recommended to promptly change account rights.

By performing account maintenance immediately, it becomes possible to handle illegal access by users who used to have rights before and/or unexpected attacks from attackers.

For example, if a user left the job, delete the account of the user; if the scope of charge of a maintenance personnel is changed, change the group to which the personnel belongs.

Password Management

Considering security, it is recommended to change passwords periodically. Password cracking can be prevented by periodically changing the user passwords.

5.1.3 Common Precautions for Common Account Management/Individual Account Management

This section lists precautions common to the common account management and individual account management.

System Audit

It is recommended to perform system audit periodically. By doing so, it is possible to detect system abnormalities in early stages, which leads to early discovery of signs of troubles and accidents. If any abnormalities are found, consult network administrators or experts to take appropriate measures.

Account Management by Standalone Management

When managing accounts by standalone management, it is not only necessary to create the same user account on all PCs used by users and SENG PCs on which project databases exist, but also unify passwords of registered accounts. Note that, when changing a password, it is also necessary to change the password to the same new password on all the PCs in which the same account is registered.

Account Management by Domain Management

If the time on the domain controller and the time on PCs in the system of the product significantly differ (5 minutes or longer by default), the authentication function does not work properly in the domain environment. Pay attention to the time deviation between the domain controller and each PC.

PSF_MAINTENANCE Group

PSF_MAINTENANCE, which is a group for maintenance, has very powerful rights, including administrator rights. It is desired to treat accounts belonging to PSF_MAINTENANCE as invalid accounts under normal operation and enable the accounts when they are in need. Moreover, setting valid periods for accounts at the timing to enable the accounts is also an effective security measure.

Users who can Use OPC

Users who can use OPC can use the DCOM function on remote sites, so it is desired to minimize the number of registered users who can use OPC to reduce their influences on the system. Moreover, if target users use only programs, deleting the logon right is also an effective measure.

User Creation Method for Groups Having Windows Administrator Rights

When creating a user belonging to PSF_MAINTENANCE or PSF_MAINTENANCE_LCL, it is necessary to add the user to either the Administrators group or the Domain Admins group as well.

5.2 Related Programs

This section explains the following related programs.

- Windows Security Patches
- Antivirus software

Windows Security Patches

It is assumed that security patches are applied according to the customer's security policy.

YOKOGAWA recommends to apply Windows security patches to the product. It is recommended to apply all required security patches before the system goes into operation and also apply security patches that are released after the system went into operation as promptly as possible.

Yokogawa offers security patch application services. Contact Yokogawa Service for more information.

As is noted as zero-day attack, attacks that take advantage of the software vulnerability can occur right after the disclosure of the vulnerability (security hole).

Note that when security patches and service packs are applied to the product, existing security settings (firewall setting and local security setting) may be changed. If security patches and service packs are applied, make sure that the existing security settings are valid.

Antivirus Software

It is recommended to install antivirus software tested by YOKOGAWA on PCs and domain controllers within the system before starting operations. For more information about application of antivirus software, contact YOKOGAWA Service.

If search engines and pattern files of antivirus software are updated, it may have unexpected rebooting or unexpected influence on other operations of PC. Exercise sufficient cautions when updating antivirus software, such as checking the operation beforehand using a test purpose PC.

5.3 Measures for Secure Use

This section describes how to use ProSafe-RS securely. It is recommended to take the measures described here for the secure use of ProSafe-RS.

SEE ALSO For more information about security measures for the entire system such as considerations about network configuration, refer to:

Security Standard of System Product (TI 33Y01B30-01E)

■ Selecting a Security Model

On the computers used in a ProSafe-RS system, select the Standard model or Strengthened model for the security model.

■ Informing Users of Entry to a Security Zone

When a system using ProSafe-RS is installed in a security zone, you can use the following measure so that the user who is trying to log on to the system is informed that he/she is entering a security zone and the subsequent operations will be performed in the security zone. Take this measure if necessary:

For the Windows local security policy under Control Panel, select [Local Policy] > [Security Options] and configure the following policies:

- [Interactive logon: Message title for users attempting to log on]
- [Interactive logon: Message text for users attempting to log on]

TIP A security zone is a physical or logical area where only permitted users can access. Equipment and facilities in a security zone require special management and are insulated from other areas.

■ Measures against Physical Attacks

To protect devices making up a ProSafe-RS system, such as SCS, network switches, and computers, from physical attacks by malicious third parties, take measures such as placing the devices in a lockable rack and strictly controlling the entry to and exit from the area where they are placed.

■ Measures against Connection of Unauthorized Devices

Take measures so as to prevent connection of unauthorized devices brought from the outside to the ProSafe-RS system. Examples of the measure are:

- Disable the free ports of network switches
- Limit the devices allowed to connect to the ports of network switches:
  for example, by assigning the MAC addresses of connectable devices to the ports.

■ Measures against Information Leakage in Communication

To prevent information travelling through the control network from leaking to unauthorized third parties, implement the measures described in “■ Measures against Physical Attacks” and “■ Measures against Connection of Unauthorized Devices” on the network switches.

■ Limiting System Administrators

Ensure that only a few reliable persons are registered in the administrative groups of ProSafe-RS.

If Behavior Suspected to be Resulting from Vulnerability is Found

If you find any behavior of the product suspected to be resulting from the vulnerability of our products, please inform YOKOGAWA by using the form at the following URL.

https://contact.yokogawa.com/cs/gw?c-id=000983

Procedure of product disposal

When disposing of a product, follow these steps to delete product information or sensitive information from the devices composing ProSafe-RS.

- Delete the data from the hard disk of your computer.
- Initialize the information in the processor module
  - For S2CP471/L1CP471
    Set the Operation data reset switch to “RESET” and turn on the power of the processor module.
  - For SCP461
    Set the BATTERY ON/OFF switch to “OFF” and turn off the power of the processor module.

SEE ALSO For more information about the Operation data reset switch and the BATTERY ON/OFF switch, refer to:

“● Front switches of the processor module” in “■ Elements on the processor module” in B4.2, “Processor module” in Hardware User's Guide (IM 32P06C10-01EN)

Port used by SCS Vnet/IP

The SCS ports (protocol: port number) used by Vnet/IP are as follows:

- UDP: 123 (SNTP)
- UDP: 520 (RIP)
- UDP: 5313
- UDP: 6000
- UDP: 9940

6. Utility Programs for Security Settings

This section describes the IT Security Tool, Domain Link Management Tool, and other utility programs for security setting.

6.1 IT Security Tool

The IT Security Tool is the security configuration utility for YOKOGAWA system products. You need to use this tool to provide security measures on the computers where any YOKOGAWA system product is installed.

The IT Security Tool applies security settings on a computer automatically based on the selected IT security version, security model, and user management type.

After installing the ProSafe-RS software, you must configure the security settings of the computer to strengthen IT security.

By using the IT Security Tool, various security settings can be configured automatically, so that you do not need to configure them manually. You can use this tool to configure the security settings on PCs with the ProSafe-RS software installed, file servers, and domain controllers.

The security settings items that can be defined using this tool will be explained below.

You cannot use this tool to configure the security settings on computers where iDefine is installed. When SENG and iDefine are installed together on the same computer, you can configure the security settings by using the IT Security Tool if the Legacy model is to be applied.

IMPORTANT

- When changing the roles of a computer such as changing the SENG in the file servers, you need to reinstall the OS.
- When the IT security configured for a computer is wrong, such as configuring IT security settings for file server in an SENG, you need to reinstall the OS.

SEE ALSO

For more information about how to configure IT security settings, refer to:

"■ Configuring IT Security Settings" in B2.3, "Configuring Security Settings for the Domain Controller" in Installation Guide (IM 32P01C50-01EN)

For more information about how to run the IT Security Tool, refer to:

B3.6.1, "Running the IT Security Tool" in Installation Guide (IM 32P01C50-01EN)

For more information about configuring the security settings that are required for coordination with ProSafe-RS on a computer where iDefine is installed, refer to:

iDefine Security Manual (PR03076-MAN-981_01)

■ Functional Overview of the IT Security Tool

The following table describes the functions of the IT Security Tool.

Table 6.1-1 Functions of the IT Security Tool

Function	Description
Information	Displays the summary of the security settings that were configured by the IT Security Tool.
Setup	According to the selected IT security version, configures the security settings by setting the security model and user management type.
Save	Saves the security settings of the OS. The security settings are encrypted with a specified password (encryption key).
Restore	Restores the security settings of the OS to the saved security settings.

Continues on the next page

Table 6.1-1 Functions of the IT Security Tool (Table continued)

Function	Description
Change Password (Encryption Key)	Changes the password (encryption key) of the saved security settings. This function is used when you want to change the password periodically.
Import or Export	Exports the information configured by the IT Security Tool to a file. Or, imports an exported file.

When IT security version 2.0 is selected, only the Standard model is available for security model. The user management type is selectable from Domain, Combination, and Standalone management. When operating with Linked domain management, select the Standalone management for user management.

When IT security version 1.0 is selected, either the Standard model or Legacy model can be selected for security model. The user management type is selectable from Domain, Combination, and Standalone management. When operating with Linked domain management, select the Standalone management for user management.

The default display of the IT security setup window differs depending on whether the tool is used during new installation or upgrading from an earlier version of the product.

IT Security Version

IT security versions are classified based on the strength of the security settings of each security model and the extent of settings.

IT Security Version 2.0

This version was designed after reconsidering the IT security version1.0 and includes more security measures.

IT Security Version 1.0

This version offers the same security measures as ProSafe-RS R4.02 and earlier versions.

Security Models

You can select from the following security models according to the required security strength.

Standard Model

This model enables access control by user authentication, DCOM setting, and Windows Firewall to guard against direct attacks.

TIP

If you need a higher level of security than what the Standard model provide, the Strengthened model is available. Please consult YOKOGAWA if IT security of the Strengthened model is required.

Legacy Model

This model does not strengthen security. Since this model disables Windows Firewall, you need to consider the possible impact of this model's vulnerability to information leaks, worms, and virus attacks when you select this model.

User Management Types

With the Standard model, you can select Domain, Combination, or Standalone for the user management type. When operating with Linked domain management, select the Standalone management.

With the Legacy model, you can select only Standalone management as the user management type.

- **Domain Management**

  Select this option when managing user and group accounts using the Windows domain controller.

- **Combination Management**

  Select this option when installing the Windows domain controller and using the product with domain users and local users.

- **Standalone Management**

  Select this option when managing user and group accounts for each computer without using the Windows domain controller. Although user accounts are created on each computer in this case, user groups and the user management type must match on all related computers.

  When operating with Linked domain management, select the Standalone management for user management.

Security Model and User Management within a Control Bus Domain

Within a V net domain or a Vnet/IP domain, the security model and user management type must be consistent. As the exception, however, Domain management and Combination management can be mixed. This mixed use of user management is also allowed for file server computers.

Standalone Management and Windows Domain

Even on Windows domain member computers, you can apply the "Standard model with Standalone management" type of security settings.

6.2 Domain Link Management Tool

The Domain Link Management Tool is the security configuration utility for YOKOGAWA system products. You need to use this tool to provide security measures as linked domain management on computers where the product is installed.

The security measures as linked domain management are implemented as follows. First, apply the IT security settings for standalone management with IT Security Tool. After that, join the computer to the domain and run the Domain Link Management Tool to add the corresponding domain groups to the members of the local groups for the products installed on the computer.

Adding a domain group to the members of the local group for the product installed on the computer by using the Domain Link Management Tool is called linking the domain. Conversely, deleting the domain group from the members of the local group is called unlinking the domain.

IMPORTANT

- The domain can be linked if the following conditions are met.
  - All of YOKOGAWA system products installed on the computer support the linked domain management.
  - The IT security settings for standalone management are applied to the installed products with IT Security Tool.
  - The computer is joined to the domain.
- You can link or unlink the domain for all of YOKOGAWA system products installed on the computer at once.
- If you install another YOKOGAWA system products that support linked domain management after linking domains, you must apply IT security settings with IT Security Tool and set them with Domain Link Management Tool. The same applies to upgrading or version upgrading the installed products.
- For the file server for ProSafe-RS, use the Domain Link Management Tool for File Server in the ProSafe-RS software medium. If the file server is shared by CENTUM VP and ProSafe-RS, use the Domain Link Management Tool for File Server in the software medium of each product to set each.

The following figure shows the Domain Link Management Tool.

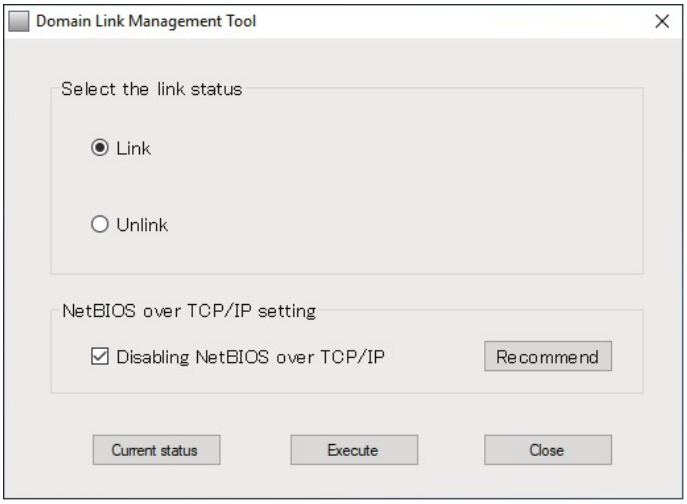


Figure 6.2-1 Domain Link Management Tool

Select the link status

When changing from the standalone management to the linked domain management, select Link. When changing from the linked domain management to the standalone management, select Unlink.

TIP

When you start the Domain Link Management Tool, Link is selected.

SEE ALSO

For more information about changing the user management type, refer to:

- 6.4.1, “SENG PC, Computer Installed with Only AD Server, or Computer Dedicated to License Management” on page 6-12
- 6.4.2, “For File Server or Domain Controller” on page 6-19

NetBIOS over TCP/IP setting

The Disabling NetBIOS over TCP/IP check box switches to the recommended state (Selected/Clear) in conjunction with the Select the link status (Link/Unlink). If you have previously execute the Domain Link Management Tool or separately set the Disabling NetBIOS over TCP/IP by using the IT Security Tool, that configuration is applied to the check box. If you want to change the Disabling NetBIOS over TCP/IP check box setting from the recommended setting or the previous setting, select the link status, and then perform select/clear operation.

When you click the Recommend, the recommended setting according to the Select the link status is applied to the Disabling NetBIOS over TCP/IP check box. If multiple products that support linked domain management are installed on the computer and the recommended settings for Disabling NetBIOS over TCP/IP are different from each other, the Clear setting takes precedence.

TIP

- The setting of Disabling NetBIOS over TCP/IP for products that do not support the linked domain management does not affect the recommended setting.
- If the computer is not in the proper state to use the Domain Link Management Tool, the Disabling NetBIOS over TCP/IP check box remains unchecked and cannot be changed.

Current status

When clicking the Current status, the status related to linked domain management appears.

While the Current status dialog box is displayed, you cannot execute or close the Domain Link Management Tool. Before you execute or close the tool, click the Close button in the upper right corner of the Current Status dialog box.

The following figure shows a display example of the Current status dialog box.

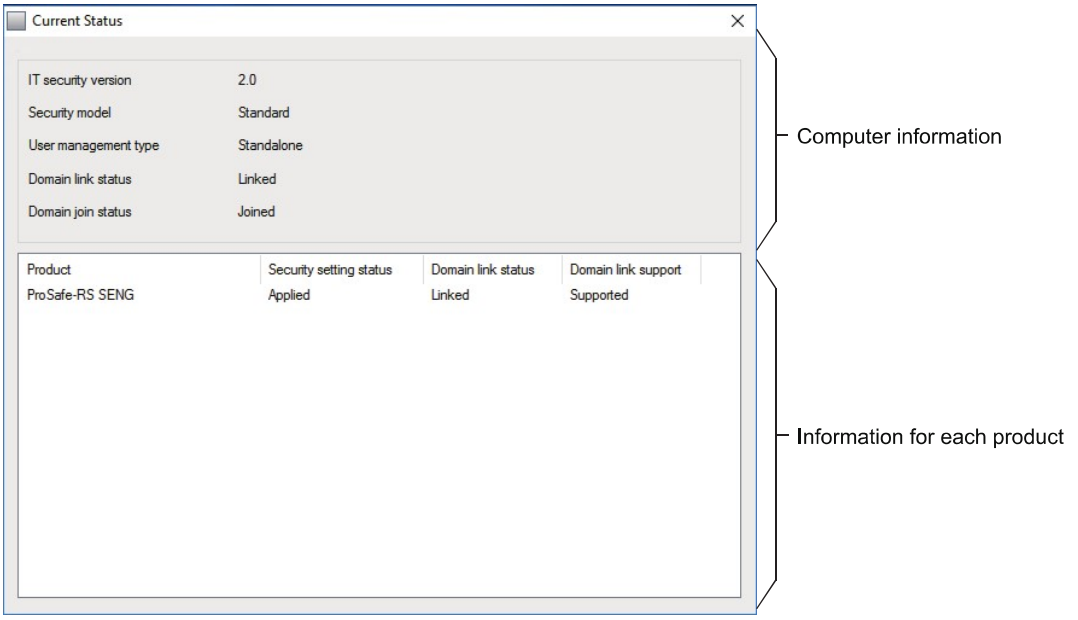


Figure 6.2-2 Display example of the Current Status dialog box

Computer information is displayed at the top of the dialog box, and information for each product is displayed at the bottom. This figure is a display example when the domain linking process by the Domain Link Management Tool is completed properly.

The following table shows the information displayed in the Current status dialog box, divided into computer information and information for each product.

Table 6.2-1 Information displayed in the Current Status dialog box - Computer information

Item	Display example	Description
IT security version	1.0	Items set by the IT Security Tool.
	2.0	
Security model	Standard (*1)	
	Strengthened (*1)	
	Legacy	
User management type	Standalone (*1)	
	Combination	
	Domain	
Domain link status	Linked	The domain is linked for all products installed on the computer.
	Some products are not linked	The domain is not linked for some products installed on the computer.
	Not linked	The domain is not linked for all products installed on the computer.
Domain join status	Joined (*1)	The computer is joined to the domain.
	Not joined	The computer is not joined to the domain.

*1: A condition required for proper processing when you select and execute the Link.

Table 6.2-2 Information displayed in the Current Status dialog box - Information for each product

Item	Display example	Description
Product	ProSafe-RS SENG	The product name and station type are displayed.
Security setting status	Applied (*1)	Both the product installation and the setting by IT Security Tool are complete.
	Not applied	The product installation is complete, but the setting by IT Security Tool is not yet complete.
	Installing	The product installation is not complete.
Domain link status	Linked	Domain linking process has been performed for the product.
	Not linked	Domain linking process has not been performed for the product.
Domain link support	Supported (*1)	The product supports the linked domain management type.
	Not supported	The product does not support the linked domain management type.

*1: A condition required for proper processing when you select and execute the Link.

TIP

The Domain Link Management Tool for File Server in the ProSafe-RS software medium links/unlinks the domain only for the local group related to ProSafe-RS, but the status related to linked domain management of coexisting products can be checked.

Displaying the unusual status

If the combination of the user management type, the domain link status, and the domain join status of computer information is unusual, that area will be displayed in red. The following table shows the unusual combination:

Table 6.2-3 Unusual combination

No.	User management type	Domain link status	Domain join status
1	Standalone	Some products are not linked	Joined
2	Standalone	Linked	Not joined
3	Standalone	Some products are not linked	Not joined
4	Domain	Not linked	Not joined
5	Combination	Not linked	Not joined

The unusual combinations shown in the table are considered transient conditions that occur when trying to set or change any of the user management types. Set correctly so that it does not become unusual combination.

TIP

When attempting to link the domain, the unusual combination shown in No.1 occurs in the following cases.

- While installing YOKOGAWA system products that support the linked domain management
- IT security settings for standalone management is applied, but the domain is not linked.

After installing the product, apply the IT security settings of standalone management with IT Security Tool and link the domain.

SEE ALSO For more information about setting and changing the user management type, refer to:

- 6.1, “IT Security Tool” on page 6-2
- 6.4.1, “SENG PC, Computer Installed with Only AD Server, or Computer Dedicated to License Management” on page 6-12

Execution and error message

When you click Execute, the domain linking process or the process of unlinking the domain occurs for the installed products, depending on the Select the link status. In addition, disabling or enabling NetBIOS over TCP/IP is applied.

When attempting to link the domain, an error message will be displayed and the process will not be performed depending on the conditions. Take the necessary measures.

SEE ALSO For more information about the error messages and countermeasures, refer to:

“■ Error messages and countermeasures” in B3.6.3, “Running Domain Link Management Tool” in Installation Guide (IM 32P01C50-01EN)

6.3 Setting the IT security

When setting the IT security of linked domain management, perform in the order of setting with IT Security Tool, joining computer to domain, and domain linkage with Domain Link Management Tool. For user management types other than linked domain management, the Domain Link Management Tool is not used.

If the IT Security Tool is running, the Domain Link Management Tool cannot be started. When you have finished making settings with the IT Security Tool, close the tool.

SEE ALSO

For more information about running the IT Security Tool, refer to:

B3.6.1, “Running the IT Security Tool” in Installation Guide (IM 32P01C50-01EN)

For more information about running the Domain Link Management Tool , refer to:

B3.6.3, “Running Domain Link Management Tool” in Installation Guide (IM 32P01C50-01EN)

6.4 Changing the IT Security Settings

This section describes how to change the IT security settings that have been applied.

Changes to IT security settings include:

- Change the security model
- Change the IT security version
- Change the user management type
- Change Individual setting items
- Join/leave the computer to/from the domain
- Change the domain link status

When you change the IT security settings, close all running applications before starting the IT Security Tool.

6.4.1 SENG PC, Computer Installed with Only AD Server, or Computer Dedicated to License Management

This section describes the procedure for changing the IT security settings on an SENG PC, a computer installed with only AD Server, or a computer dedicated to license management. The description of the setting procedure of IT Security Tool and Domain Link Management Tool is omitted here. Set it the same way as the first IT security setting.

SEE ALSO For more information about ProSafe-RS applications that can start from Start menu, refer to:

"ProSafe-RS and ProSafe-RS Lite applications that can start from Start menu" in Read Me First (IM 32P01A30-01EN)

For more information about the first configuration by the IT Security Tool, refer to:

B3.6.1, "Running the IT Security Tool" in Installation Guide (IM 32P01C50-01EN)

For more information about adding computers to the domain, refer to:

B2.5, "Adding Computers to the Domain" in Installation Guide (IM 32P01C50-01EN)

For more information about the first configuration by the Domain Link Management Tool, refer to:

B3.6.3, "Running Domain Link Management Tool" in Installation Guide (IM 32P01C50-01EN)

■ Cautions

Precautionary notes on changing IT security settings on a computer installed with the software of the ProSafe-RS software are as follows:

● Note on Changing the Security Model to Legacy Model

When you have changed to the Legacy model for a system using Windows authentication, which is a user authentication mode available with the access control and operation history management functions, you must configure the settings for using ProSafe authentication.

SEE ALSO For more information about the required settings for operation in ProSafe authentication mode, refer to:

- E2.2.1, "Settings for access control" in Engineer's Reference Manual (IM 32P04B10-01EN)
- "■ Settings required when ProSafe authentication mode is selected" in E2.2.1, "Settings for access control" in Engineer's Reference Manual (IM 32P04B10-01EN)
- "■ Tasks required after changing user authentication mode" in E2.3.2, "Operations performed by administrators" in Engineer's Reference Manual (IM 32P04B10-01EN)

● Notes on Changing the User Management Type

For a system using Windows authentication, which is a user authentication mode available with the access control/operation history management function, you need to perform the following tasks:

- When you have changed from Standalone management to Domain/Combination/Linked domain management or vice versa, you need to set up the users who uses SENG again. If you created a new Windows user of SENG, register the user in the Engineers' Account Builder.

■ User Who Can Change IT Security Settings

To be able to change the IT security settings, you need to have the required rights depending on the applied security model and user management type.

Table 6.4.1-1 User Who Can Change IT Security Settings

<table>
<tr><th colspan="2" rowspan="3">Currently applied security model and user management type</th><th colspan="4">Security model and user management type to be applied</th></tr>
<tr><th rowspan="2">Legacy model</th><th colspan="3">Standard model</th></tr>
<tr><th>Standalone management</th><th>Linked domain type</th><th>Domain/Combination management</th></tr>
<tr><td colspan="2">Legacy model</td><td colspan="2">Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer</td><td>Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer</td><td>Domain users who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain (*1)</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td><td>Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*1) (*2) (*3)</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td><td>Domain user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*1)</td></tr>
<tr><td rowspan="5">Standard model</td><td rowspan="2">Standalone management</td><td colspan="2" rowspan="2">Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer</td><td rowspan="2">Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*4)</td><td>Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*1) (*2) (*3)</td></tr>
<tr><td>Domain user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*1)</td></tr>
<tr><td rowspan="2">Linked domain management</td><td rowspan="2">Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer</td><td>Domain users who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain (*4)</td><td>Domain users who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain (*1)</td><td>Domain users who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain (*1)</td></tr>
<tr><td>Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*4)</td><td>Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*1)</td><td>Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*1)</td></tr>
<tr><td rowspan="3">Domain/Combination management</td><td colspan="2" rowspan="3">Local user who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer (*5)</td><td rowspan="3">Local user who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer (*1) (*2)</td><td>Domain users who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain (*1)</td></tr>
<tr><td>Local user who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer (*1) (*2) (*3)</td></tr>
<tr><td>Domain user who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer (*1)</td></tr>
</table>

*1: Log on to the computer when the computer is connected to the domain.
*2: While changing, the user name and password of the domain are required.
*3: When this user applies IT security and uses iDefine interface package, execute the batch file.
*4: Set up in the Domain Link Management Tool. No need to reconfigure the IT Security Tool.
*5: Before you change the IT security settings, remove the computer from the domain.

SEE ALSO For more information about how to execute the batch file when using iDefine interface package, refer to:

"■ User Who Performs Update Installation" in C4.1, "Installation for Upgrading" in Installation Guide (IM 32P01C50-01EN)

Changes related to User Management other than Linked Domain Management

IT Security Tool is used when changing the user management other than linked domain management, but Domain Link Management Tool is not used. Depending on the security model and user management type you are going to change, you may need to join the computer to the domain or remove the computer from the domain.

Follow these steps to change the setting with IT Security Tool:

1. Sign in to the computer as a user who has authority to change IT security settings.
2. From the Start menu, start the IT Security Tool.
3. Click [Setup].
4. Select the security model and user management type you want to change to.
   The rest of the procedure is the same as that for the normal IT security setups.

SEE ALSO For more information about running the IT Security Tool, refer to:

B3.6.1, "Running the IT Security Tool" in Installation Guide (IM 32P01C50-01EN)

For more information about ProSafe-RS applications that can start from Start menu, refer to:

"ProSafe-RS and ProSafe-RS Lite applications that can start from Start menu" in Read Me First (IM 32P01A30-01EN)

Notes on Changing the User Management Type

- When you change from Standalone management to Domain/Combination management, create user groups and user accounts in advance using the domain controller.
- When you change from Standalone management to Domain/Combination management, add the computer to the domain before applying the IT security settings.
- When you change from Domain/Combination management to Standalone management, remove the computer from the domain before you change the IT security settings.

SEE ALSO For more information about how to call up the Current IT security setting information dialog box, refer to:

6.9, "Viewing the Information Configured by the IT Security Tool" on page 6-45

For more information about the required tasks with a domain controller and the procedure to add computers to a domain, refer to:

B2., "Setting Up the Windows Domain Environment" in Installation Guide (IM 32P01C50-01EN)

For more information about registering engineers, refer to:

"■ Registering an engineer's account" in E2.2.3, "Registering engineers" in Engineer's Reference Manual (IM 32P04B10-01EN)

Migrating the standard model (combination/domain management) computer to other domain

Follow these steps to migrate the standard model (combination/domain management) computer to other domain:

1. Sign in to the computer as a local user who has authority to change IT security settings.

2. Remove the computer from the current domain.
3. Change the security model of the computer from combination/domain management to standalone management.
4. Join the computer to the target domain.
5. Sign in to the computer as a local user who has authority to change IT security settings.
6. Change the computer security model from standalone management to combination/domain management.

Changes related to Linked Domain Management

When changing from linked domain management to a user management type other than linked domain management, or vice versa, the tool to be used differs depending on each case.

Reconfiguring IT security during linked domain management operation

IT security needs to be reconfigured in the following cases:

- Installed ProSafe-RS patch version software that requires IT security settings
- Distributed the license for the SOE OPC Interface Package
- Changing the IT Security setting values

To reconfigure IT security during linked domain management operation, use IT Security Tool. Sign in as a local user or a domain user who has authority to change IT security settings, and apply IT security of standalone management by using IT Security Tool.

Changing from standard model with standalone management

When changing from the standard model with standalone management to the standard model with linked domain management, join the computer to the domain, and then link the domain by using the Domain Link Management Tool.

TIP

The domain user authentication dialog box appears because you are linking the domain as a local user who has authority to change IT security settings. Enter the user name and password of the domain user in the authentication dialog box. The user name and password do not have to be those of the domain administrator.

Changing from standard model with combination/domain management or from legacy model

When changing from the standard model with combination management or domain management to the standard model with linked domain management, use both IT Security Tool and Domain Link Management Tool.

Follow these steps to change the user management type:

1. Keep the computer joined to the domain and sign in with a local user who has authority to change IT security settings.
2. From the Start menu, start the IT Security Tool.
3. Click [Setup].
4. Change the user management type to standalone management and complete the IT security settings.
5. Remove the computer from the domain.
6. Sign in to the computer as a local user who has authority to change IT security settings.
7. From the Start menu, start the IT Security Tool.

8. Click [Setup].
9. Complete the IT security settings of standalone management.
10. Join the computer to the domain.
11. Sign in to the computer as a local user who has authority to change IT security settings.
12. Start the Domain Link Management Tool from the Start menu.
13. Complete the settings for linking domain.

TIP

When the domain user authentication dialog box appears, enter the user name and password of the domain user. The user name and password do not have to be those of the domain administrator.

When changing from the legacy model to the standard model with linked domain management, if the computer has joined the domain, perform from step 1 above. If the computer is not joined to the domain, start from step 6 above.

● Changing to standard model with standalone management

When changing from the standard model with linked domain management to the standard model with standalone management, use Domain Link Management Tool.

Follow these steps to change the user management type:

1. Keep the computer joined to the domain and sign in with a local user or a domain user who has authority to change IT security settings.
2. Start the Domain Link Management Tool from the Start menu.
3. Complete the settings for unlinking the domain.
4. Remove the computer from the domain.

● Changing to standard model with combination/domain management

When changing from the standard model with linked domain management to the standard model with combination management or domain management, use both IT Security Tool and Domain Link Management Tool.

Follow these steps to change the user management type:

1. Keep the computer joined to the domain and sign in with a local user or a domain user who has authority to change IT security settings.
2. Start the Domain Link Management Tool from the Start menu.
3. Complete the settings for unlinking the domain.
4. Keep the computer joined to the domain and sign in with a local user or a domain user who has authority to change IT security settings.
5. From the Start menu, start the IT Security Tool.
6. Click [Setup].
7. Complete the IT security settings of combination or domain management.

● Additionally installing the products supporting linked domain management

For the products to be additionally installed, apply IT security of standalone management and link the domain.

To additionally install a product supporting linked domain management, follow these steps:

1. Sign in as a local user who belongs to the Administrators group of the local computer.
2. Install the product supporting linked domain management.

3. Select [Yes, I want to set up IT security now.] on the dialog box that appears after the installation, and click [Finish].
   The IT Security Tool starts.
4. Click Setup.
5. Complete the IT security settings of standalone management.
6. Sign in to the computer as a local user or a domain user who has authority to change IT security settings.
7. Start the Domain Link Management Tool from the Start menu.
8. Complete the settings for linking domain.

TIP

If you start the Domain Link Management Tool as a local user who has authority to change IT security settings, the domain user authentication dialog box appears. The user name and password that you enter in the dialog box do not have to be those of the domain administrator.

Additionally installing the products not supporting linked domain management

When additionally installing products that do not support linked domain management, it is necessary to change the user management type to combination management or domain management in advance.

IMPORTANT

If you install products that do not support linked domain management in a state in which the domain is linked and you select user management other than standalone management in IT Security Tool, a dialog box that prompts you to change to another user management type appears. Unlink the domain, and then set it in IT Security Tool.

To additionally install a product not supporting linked domain management, follow these steps:

1. Keep the computer joined to the domain and sign in with a local user or a domain user who has authority to change IT security settings.
2. Start the Domain Link Management Tool from the Start menu.
3. Complete the settings for unlinking the domain.
4. Sign in as a local user who belongs to the Administrators group of the local computer.
5. Install the product not supporting linked domain management.
6. Select [Yes, I want to set up IT security now.] on the dialog box that appears after the installation, and click [Finish].
   The IT Security Tool starts.
7. Click Setup.
8. Complete the IT security settings of combination or domain management.

Changing to another domain during linked domain management operation

This section describes the procedures assuming a case where a system is constructed using a temporary domain controller and the system is migrated to an official domain controller.

Follow these steps to change to another domain during linked domain management operation:

1. Keep the computer joined to the original domain and sign in with a local user or a domain user who has authority to change IT security settings.

2. Start the Domain Link Management Tool from the Start menu.
3. Complete the settings for unlinking the domain.
4. Remove the computer from the original domain.
5. Join the computer to the target domain.
6. Sign in to the computer as a local user who has authority to change IT security settings.
7. Start the Domain Link Management Tool from the Start menu.
8. Complete the settings for linking domain.

TIP

If you start the Domain Link Management Tool as a local user who has authority to change IT security settings, the domain user authentication dialog box appears. The user name and password that you enter in the dialog box do not have to be those of the domain administrator.

6.4.2 For File Server or Domain Controller

This section describes the procedures for changing the security settings on a computer that serves only as a file server or a domain controller computer. The description of the setting procedure of IT Security Tool and Domain Link Management Tool is omitted here. Set it the same way as the first IT security setting.

IMPORTANT

- When you change the IT security settings on a file server or domain controller computer, prepare the initial security settings that were saved before using the IT Security Tool.
- When operating a file server with linked domain management, use the IT Security Tool for file server/domain controller and the Domain Link Management Tool for File Server for the products that support linked domain management.
- The Domain Link Management Tool for File Server in the ProSafe-RS software medium links/unlinks the domain only for the local group related to ProSafe-RS. If the file server is shared by CENTUM VP and ProSafe-RS, use the Domain Link Management Tool for File Server in the software medium of each product to set each.
- When sharing a file server with a product that does not support linked domain management and using it in a domain environment, operate with domain management or combination management.

SEE ALSO

For more information about restoring the security settings of a file server or domain controller computer without installing the ProSafe-RS software, refer to:

6.6.2, “Procedure for a File Server or Domain Controller” on page 6-36

For more information about how to start the installation menu, refer to:

B3.5, “Installing the ProSafe-RS Software” in Installation Guide (IM 32P01C50-01EN)

For more information about the first time configuring the security settings on a file server with the ProSafe-RS software not installed, refer to:

B5.1, “Setting Up a Computer that Serves Only as a File Server” in Installation Guide (IM 32P01C50-01EN)

For more information about the first time configuring the security settings on a domain controller computer with the ProSafe-RS software not installed, refer to:

B2.3, “Configuring Security Settings for the Domain Controller” in Installation Guide (IM 32P01C50-01EN)

User Who Can Change IT Security Settings on a File Server

To be able to change the IT security settings on a file server, you need to have the required rights depending on the applied security model and user management type.

Table 6.4.2-1 User Who Can Change Security Settings

<table>
<tr><th colspan="2" rowspan="3">Currently applied security model and user management type</th><th colspan="4">Security model and user management type to be applied</th></tr>
<tr><th rowspan="2">Legacy model</th><th colspan="3">Standard model</th></tr>
<tr><th>Standalone management</th><th>Linked domain management</th><th>Domain/Combination management</th></tr>
<tr><td colspan="2" rowspan="3">Legacy model</td><td rowspan="3">Local user who belongs to the Administrators group of the local computer</td><td rowspan="3">Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer</td><td rowspan="3">Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer</td><td>Domain users who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain (*1)</td></tr>
<tr><td>Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*1) (*2)</td></tr>
<tr><td>Domain user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*1)</td></tr>
<tr><td rowspan="6">Standard model</td><td rowspan="2">Standalone management</td><td colspan="2" rowspan="2">Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer</td><td rowspan="2">Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*3)</td><td>Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*2) (*4)</td></tr>
<tr><td>Domain user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer (*2) (*4)</td></tr>
<tr><td rowspan="2">Linked domain management</td><td rowspan="2">Local user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer</td><td>Domain users who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain (*3)</td><td rowspan="2">Local user who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer (*4)</td><td rowspan="2">-</td></tr>
<tr><td>Local user who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer (*3)</td></tr>
<tr><td rowspan="3">Domain/Combination management</td><td colspan="2" rowspan="3">Local user who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer (*5)</td><td rowspan="3">-</td><td>Domain users who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain (*1)</td></tr>
<tr><td>Local user who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer (*1) (*2)</td></tr>
<tr><td>Domain user who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer (*1)</td></tr>
</table>

*1: Log on with your computer joined to the domain.
*2: While changing, entry of the user name and password of the domain user is required.
*3: Set up in the Domain Link Management Tool. No need to reconfigure with the IT Security Tool.
*4: Certain task is required while the computer is not joining the domain and after the computer joined the domain.
*5: Before you change the IT security settings, remove the computer from the domain.

User Who Can Change IT Security Settings on the Domain Controller

When changing the IT security settings on the domain controller computer, sign in to the computer as a user who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain.

Changes related to User Management other than Linked Domain Management

There are the following three types procedures for changing the user management other than linked domain management:

- Basic procedure
- Procedure to change from Standard model (Standalone management) to Standard model (Domain/Combination management) on a file server
- Procedure to change from Standard model (Domain/Combination management) to Standard model (Standalone management) on a file server

Basic Procedure for Changing Security Settings

1. Sign in to the computer as a user who has authority to change IT security settings.

TIP

If the file server is shared with CENTUM VP, the user who has the authority to change IT security settings must also belong to the CTM_MAINTENANCE or CTM_MAINTENANCE_LCL group, depending on the combination of the current security model/user management type and the security model/user management type that you are about to configure. However, this does not apply when reconfiguring IT security settings without changing the model from the legacy model.

2. Start the installation menu from the software medium of the product, and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
3. Click [Restore].
4. Select a file that the previous security settings are saved prior to running the IT Security Setting Tool so as to restore the securities.
   For a file server, if it is not a domain member now, use the file holding the initial security settings that were saved while it was standalone. If it is a domain member now, use the file holding the initial security settings that were saved after it joined the domain.
5. After restoring is completed, restart the computer.
6. For a file server, if its domain membership is to be changed, add to or remove from the domain.
7. Start the installation menu again and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
8. Click [Setup].
9. Select the security model and the user management type you want to change to.
   The rest of steps are the same as the procedure for the first time setup.

TIP

If the file server is shared with CENTUM VP, start the IT Security Tool for file server and domain controller from the installation menu of CENTUM VP R6.04 or later software medium and set IT security for CENTUM VP as well.

SEE ALSO For more information about restoring IT security settings on a file server or a domain controller, refer to:

6.6.2, “Procedure for a File Server or Domain Controller” on page 6-36

For more information about the first configuration of security settings on a file server, refer to:

B5.1, “Setting Up a Computer that Serves Only as a File Server” in Installation Guide (IM 32P01C50-01EN)

For more information about the first configuration of security settings for a domain controller, refer to:

B2.3, “Configuring Security Settings for the Domain Controller” in Installation Guide (IM 32P01C50-01EN)

When Changing from Standard Model (Standalone Management) to Standard Model (Domain/Combination Management) on a File Server

For this change, you need to save the security settings after the file server computer joined a domain because the security settings are changed by joining the domain. Follow these steps to make the change:

1. Sign in to the computer as an administrative user who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer.

TIP If the file server is shared with CENTUM VP, the administrative user must also belong to the CTM_MAINTENANCE group.

2. Start the installation menu from the software medium of this product.
3. Click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
4. Restore the initial security settings saved (while the computer is not a member of a domain) before you fist time used the IT Security Tool to setup security.
5. After restarting, add the computer to the domain.
6. Sign in as the same administrative user you previously signed in in step 1.
7. Start the installation menu and click [Setting IT Security (File server/domain controller use)].
   The IT Security Tool starts.
8. Click [Save].
9. Save the security settings as the initial settings right after it joined a domain.
10. On the IT Security Tool's menu, click [Setup].
11. Select the security model and user management type for the file server, and run the setup.
12. After applying the security settings, restart the computer.

TIP If the file server is shared with CENTUM VP, start the IT Security Tool for file server and domain controller from the installation menu of CENTUM VP R6.04 or later software medium and set IT security for CENTUM VP as well.

When Changing from Standard Model (Domain/Combination Management) to Standard Model (Standalone Management) on a File Server

For this change, the timing of removal from the domain is different from the basic procedure.

1. Sign in to the computer as an administrative user who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer.

TIP

If the file server is shared with CENTUM VP, the administrative user must also belong to the CTM_MAINTENANCE_LCL group.

2. Remove the computer from the domain.
3. Restart the computer, and sign in as the same administrative user that you signed in in step 1.
4. Start the installation menu from the software medium of this product.
5. Click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
6. Click [Restore] to restore the initial security settings that were saved before the IT Security Tool was first used to setup security (before the computer joined a domain).
7. Restart the computer.
8. Sign in as the same administrative user you previously signed in in step 1.
9. Start the installation menu from the software medium of this product.
10. Click [Setting IT Security (File server/domain controller use] to start the IT Security Tool.
11. Click [Setup], select Standard model and Standalone management for the file server, and run the setup.
12. After applying the security settings, restart the computer.

TIP

If the file server is shared with CENTUM VP, start the IT Security Tool for file server and domain controller from the installation menu of CENTUM VP R6.04 or later software medium and set IT security for CENTUM VP as well.

● When migrating the standard model (combination/domain management) computer to other domain on a file server

Follow these steps to migrate the standard model (combination/domain management) computer to other domain:

1. Change the security model of the computer in the migration source domain from combination/domain management to standalone management.
2. Change the computer security model from standalone management to combination/domain management for the migration destination domain.

SEE ALSO

For more information about procedure to change from combination/domain management to standalone management, refer to:

"● When Changing from Standard Model (Domain/Combination Management) to Standard Model (Standalone Management) on a File Server" on page 6-22

For more information about procedure to change from standalone management to combination/domain management), refer to:

"● When Changing from Standard Model (Standalone Management) to Standard Model (Domain/Combination Management) on a File Server" on page 6-22

■ Changes related to Linked Domain Management

When changing from linked domain management to a user management type other than linked domain management, or vice versa, the tool to be used differs depending on each case.

Reconfiguring IT security during linked domain management operation

To reconfigure IT security of the file server during linked domain management operation, use IT Security Tool.

Follow these steps to reconfigure the IT security:

1. Remove the file server from the domain.
2. Sign in to the file server as a local user who has authority to change IT security settings.

TIP If the file server is shared with CENTUM VP, the local user who has authority to change IT security settings must also belong to the CTM_MAINTENANCE group.

3. Start the installation menu from the software medium of this product.
4. Click [Setting IT Security (File server/domain controller use)].
   The IT Security Tool starts.
5. Click [Restore].
6. Select a file that the previous security settings are saved prior to running the IT Security Setting Tool so as to restore the security settings.

TIP Use the file holding the initial security settings that were saved while it was standalone.

7. Restart the file server.
8. Sign in to the file server as a local user who has authority to change IT security settings.

TIP If the file server is shared with CENTUM VP, the local user who has authority to change IT security settings must also belong to the CTM_MAINTENANCE group.

9. Start the installation menu from the software medium of this product.
10. Click [Setting IT Security (File server/domain controller use)].
    The IT Security Tool starts.
11. Click [Setup].
12. Complete the IT security settings of the File Server Standard Model with Standalone Management.

TIP If the file server is shared with CENTUM VP, start the IT Security Tool for file server and domain controller from the installation menu of CENTUM VP R6.08 or later software medium that supports linked domain management, and set IT security of File Server Standard Model with Standalone Management for CENTUM VP as well.

13. Join the file server to the domain.
14. Sign in to the file server as a local user or a domain user who has authority to change IT security settings.

TIP If the file server is shared with CENTUM VP, the local user or domain user who has authority to change IT security settings must also belong to the CTM_MAINTENANCE group.

15. Use Explorer to display the following folder from the software medium of this product.
    `<Drive of software medium>:\ProSafe-RS\SECURITY\`
16. Double click the following program file in the folder.
    `DomainLinkManagementToolForRSFileServer.cmd`

The Domain Link Management Tool for File Server starts.

17. Complete the settings for linking domain.

TIP

- If you start the Domain Link Management Tool as a local user who has authority to change IT security settings, the domain user authentication dialog box appears. The user name and password that you enter in the dialog box do not have to be those of the domain administrator.
- If the file server is shared with CENTUM VP, the domain linkage settings for CENTUM VP is required separately by using the Domain Link Management Tool for File Server in the software medium of CENTUM VP R6.08 or later.

Changing from standard model with standalone management on a file server

When changing from the standard model with standalone management to the standard model with linked domain management, use Domain Link Management Tool.

Follow these steps to change the user management type:

1. Join the file server to the domain.
2. Sign in to the file server as a local user or a domain user who has authority to change IT security settings.

TIP

If the file server is shared with CENTUM VP, the local user or domain user who has authority to change IT security settings must also belong to the CTM_MAINTENANCE group.

3. Use Explorer to display the following folder from the software medium of this product.
   `<Drive of software medium>:\ProSafe-RS\SECURITY\`
4. Double click the following program file in the folder.
   `DomainLinkManagementToolForRSFileServer.cmd`

   The Domain Link Management Tool for File Server starts.
5. Complete the settings for linking domain.

TIP

- If you start the Domain Link Management Tool as a local user who has authority to change IT security settings, the domain user authentication dialog box appears. The user name and password that you enter in the dialog box do not have to be those of the domain administrator.
- If the file server is shared with CENTUM VP, the domain linkage settings for CENTUM VP is required separately by using the Domain Link Management Tool for File Server in the software medium of CENTUM VP R6.08 or later.

Changing to standard model with standalone management on a file server

When changing from the standard model with linked domain management to the standard model with standalone management, use Domain Link Management Tool.

Follow these steps to change the user management type:

1. Keep the file server joined to the domain and sign in with a local user or a domain user who has authority to change IT security settings.

TIP

If the file server is shared with CENTUM VP, the local user or domain user who has authority to change IT security settings must also belong to the CTM_MAINTENANCE group.

2. Use Explorer to display the following folder from the software medium of this product.
   `<Drive of software medium>:\ProSafe-RS\SECURITY\`
3. Double click the following program file in the folder.
   `DomainLinkManagementToolForRSFileServer.cmd`

   The Domain Link Management Tool for File Server starts.

4. Complete the settings for unlinking the domain.

TIP

If the file server is shared with CENTUM VP, the domain unlinkage settings for CENTUM VP is required separately by using the Domain Link Management Tool for File Server in the software medium of CENTUM VP R6.08 or later.

5. Remove the file server from the domain.

Changing to another domain during linked domain management operation

This section describes the procedures assuming a case where a system is constructed using a temporary domain controller and the system is migrated to an official domain controller.

Follow these steps to change to another domain during linked domain management operation:

1. Keep the file server joined to the original domain and sign in with a local user or a domain user who has authority to change IT security settings.

TIP

If the file server is shared with CENTUM VP, the local user or domain user who has authority to change IT security settings must also belong to the CTM_MAINTENANCE group.

2. Use Explorer to display the following folder from the software medium of this product.
   `<Drive of software medium>:\ProSafe-RS\SECURITY\`
3. Double click the following program file in the folder.
   `DomainLinkManagementToolForRSFileServer.cmd`

   The Domain Link Management Tool for File Server starts.
4. Complete the settings for unlinking the domain.

TIP

If the file server is shared with CENTUM VP, the domain unlinkage settings for CENTUM VP is required separately by using the Domain Link Management Tool for File Server in the software medium of CENTUM VP R6.08 or later.

5. Remove the file server from the original domain.
6. Join the file server to the target domain.
7. Sign in to the file server as a local user or a domain user who has authority to change IT security settings.

TIP

If the file server is shared with CENTUM VP, the local user or domain user who has authority to change IT security settings must also belong to the CTM_MAINTENANCE group.

8. Use Explorer to display the following folder from the software medium of this product.
   `<Drive of software medium>:\ProSafe-RS\SECURITY\`
9. Double click the following program file in the folder.
   `DomainLinkManagementToolForRSFileServer.cmd`

   The Domain Link Management Tool for File Server starts.
10. Complete the settings for linking domain.

TIP

- If you start the Domain Link Management Tool as a local user who has authority to change IT security settings, the domain user authentication dialog box appears. The user name and password that you enter in the dialog box do not have to be those of the domain administrator.
- If the file server is shared with CENTUM VP, the domain linkage settings for CENTUM VP is required separately by using the Domain Link Management Tool for File Server in the software medium of CENTUM VP R6.08 or later.

6.4.3 Applying the IT Security Version 2.0 Settings to a File Server or Domain Controller

With ProSafe-RS R4.03 or later, when you apply the IT security version 2.0 settings on a file server or a domain controller by using the Setup function of the IT Security Tool, the procedure differs depending on whether IT security version 1.0 is already applied on the computer or a new computer is set up.

IMPORTANT

When you strengthen the security to IT security version 2.0, you must save the initial security settings of the file server or domain controller computer again.

When IT Security Version 1.0 is Applied Already

1. Restore the initial settings that was saved by using the saving function of the IT Security Tool before the computer went into operation.
2. From the installer menu, start the IT Security Tool.
3. Save the settings after restoration.
4. Using the Setup function of the IT Security Tool, apply the required security model.

TIP

If the file server or domain controller is shared with CENTUM VP, start the IT Security Tool for file server and domain controller from the installation menu of CENTUM VP software medium and set IT security for CENTUM VP as well. Use the software medium of the following revisions depending on the user management type.

- Linked domain management: R6.08 or later
- Other than Linked domain management: R6.04 or later

SEE ALSO

For more information about how to restore security settings by using the IT Security Tool, refer to:

6.6, “Restoring the IT Security Settings” on page 6-33

When Setting Up a New Computer

1. From the installer menu, start the IT Security Tool.
2. Save the initial settings by using the saving function.
3. Using the Setup function of the IT Security Tool, apply the required security model.

TIP

If the file server or domain controller is shared with CENTUM VP, start the IT Security Tool for file server and domain controller from the installation menu of CENTUM VP software medium and set IT security for CENTUM VP as well. Use the software medium of the following revisions depending on the user management type.

- Linked domain management: R6.08 or later
- Other than Linked domain management: R6.04 or later

6.5 Saving the IT Security Settings

You can save the IT security settings on the local computer using the Save function.

The Save/Restore function of the IT Security Tool is used in the procedure for setting/resetting IT security when building a file server or domain controller. It will not be used for any purpose other than the above, except when it is used according to instructions from YOKOGAWA in case of trouble.

Use the Export/Import function for back up/restore of each setting status that was configured by the IT Security Tool (IT security version, security model, user management type, and on/off of each setting item).

SEE ALSO For more information about the Export/Import function, refer to:

6.8, “Exporting/Importing the IT Security Setting File” on page 6-41

User Who Can Save IT Security Settings

To be able to save the IT security settings, you need to have the required rights depending on the applied security model and user management type.

Table 6.5-1 User Who Can Save Security Settings

Currently applied security model and user management type			
Legacy model	Standard model		
	Standalone management	Linked domain type	Domain/Combination management
User who belongs to the Administrators group of the local computer	User who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer	User who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer	User who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer
		User who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain	User who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain

Regarding the Files that Hold the Saved Security Settings

Saving the security settings creates two files with extensions of .hed and .csf.

When restoring the saved security settings, both files are required.

6.5.1 SENG PC, Computer Installed with Only AD Server, or Computer Dedicated to License Management

This section describes the procedure for saving the IT security settings on an SENG PC, a computer installed with only AD Server, or a computer dedicated to license management.

Saving Procedure

1. From the Start menu, start the IT Security Tool.
2. Click [Save].
   The Specify destination page appears.

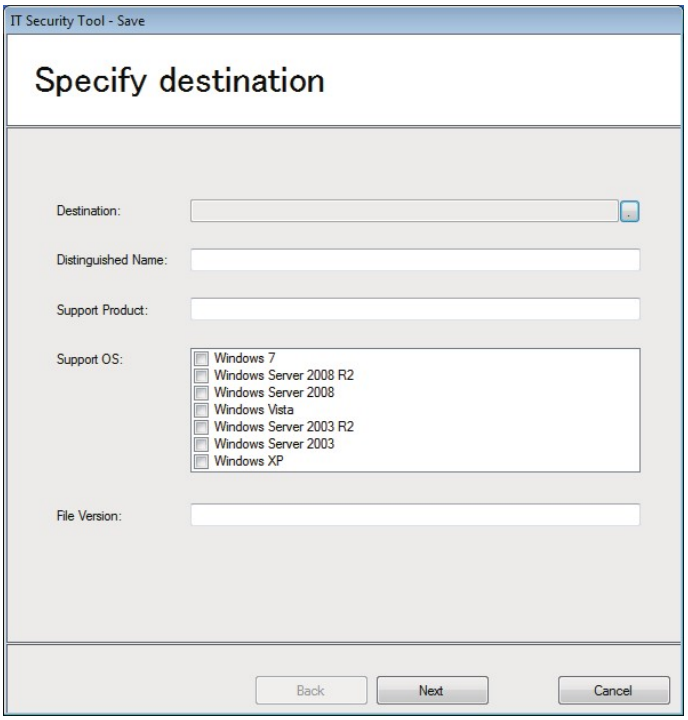


Figure 6.5.1-1 Specify Destination

3. Specify the destination folder and enter other required settings.
   The Distinguished Name and File Version are omissible.
4. Click [Next].
   The Type default account password page appears.

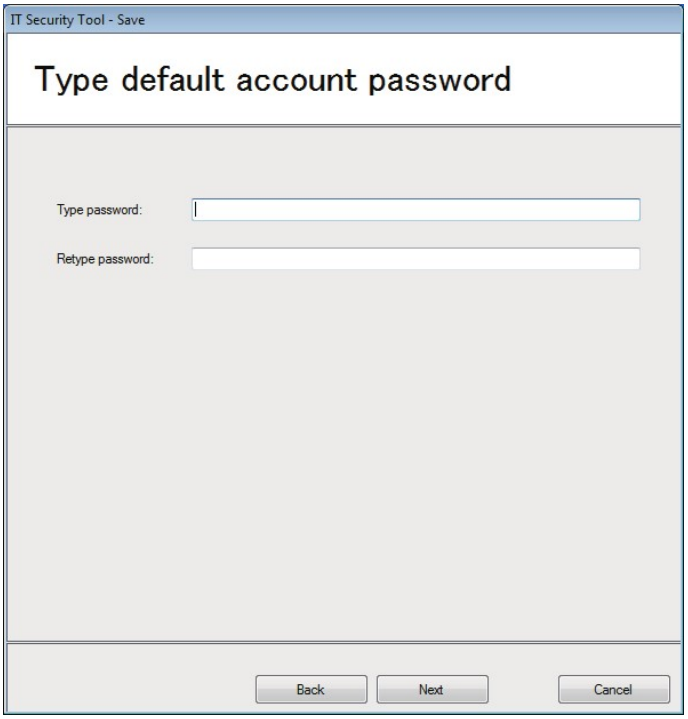


Figure 6.5.1-2 Type Default Account Password

5. Enter the password for use as the initial account password and click [Next].

TIP

This default password will be used when you recover the accounts that were saved with this tool. If the saved account does not exists at restoration, the account is created. This default password will be set as the initial password of the created account.

If multiple accounts have been created, the same password is set for all accounts.

If the set password does not meet the password policy for restoration, an error will occur when recovering an account.

Because this password is set for the account as the initial password, you will be prompted to change the password when you log on to the account for the first time.

The page for entering the password for use as the encryption key of the saved data appears.



Figure 6.5.1-3 Type Password (Encryption Key)

6. Enter the Encryption Key and then click [Next].
   Saving of the security settings starts.

IMPORTANT

- If this password (encryption key) is lost, the saved security settings cannot be restored. The password (encryption key) must be carefully kept by the customer.
- The password (encryption key) must be at least one character.
- The password can consist of upper-case and lower-case alphanumeric characters and the following symbols: ` ~ ! @ # $ % ^ & *( ) _ + - = { } | \ : “ ; ‘ < > ? , . /

  Double-byte characters cannot be used.

7. When the saving is completed, click [Finish].
   If the saving failed, the details of the failure are displayed.
8. On the IT Security Tool menu, click [Close].

IMPORTANT

If any save failures are displayed, contact YOKOGAWA Service.

SEE ALSO For more information about ProSafe-RS applications that can start from Start menu, refer to:

“ProSafe-RS and ProSafe-RS Lite applications that can start from Start menu” in Read Me First (IM 32P01A30-01EN)

6.5.2 Procedure for a File Server or Domain Controller

To save the IT security settings on a computer that serves only as a file server or a domain controller computer, start the installation menu from the ProSafe-RS software medium and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool. The rest of steps are the same as the procedure for an SENG PC.

IMPORTANT

You cannot save the group policy settings that were distributed from the domain controller. You can save only local group policy settings.

SEE ALSO For more information about how to start the installation menu, refer to:

B3.5, “Installing the ProSafe-RS Software” in Installation Guide (IM 32P01C50-01EN)

6.6 Restoring the IT Security Settings

You can restore the security settings of a local computer that were saved by using the Save function.

Preparation for Restoration

According to the user management type of the security settings to be restored, the computer may be required to join a domain or removed from a domain. To restore to the Legacy model, or the Standard model with Standalone or Linked domain management, the computer needs to be removed from a domain. To restore to the Standard model with Domain or Combination management, the computer needs to join a domain.

User Who Can Restore Security Settings

To be able to restore the IT security settings, you need to have the required rights depending on the applied security model and user management type.

Table 6.6-1 User Who Can Restore Security Settings

Security model and user management type to be restored to			
Legacy model	Standard model		
	Standalone type	Linked domain management type	Domain/Combination type
User who belongs to the Administrators group of the local computer	User who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer	User who belongs to both the Administrators and PSF_MAINTENANCE groups of the local computer	User who belongs to both the Administrators and PSF_MAINTENANCE_LCL groups of the local computer (*1)
		User who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain	User who belongs to both the Domain Admins and PSF_MAINTENANCE groups of the domain

*1: Sign in as a user who belongs to the groups shown in the cell below when the PSF_MAINTENANCE_LCL group does not exist on the local computer (that is, when the security model and user management type set before restoration is Legacy model or Standard model with Standalone management).

6.6.1 SENG PC, Computer Installed with Only AD Server, or Computer Dedicated to License Management

This section describes the procedure for restoring the IT security settings on an SENG PC, a computer installed with only AD Server, or a computer dedicated to license management.

IMPORTANT

If you saved the security settings by using the IT Security Tool, you must restore the same user management status as the saved status.

Restoring Procedure

1. From the Start menu, start the IT Security Tool.
2. Click [Restore].
   The Select Security Setting File page appears.

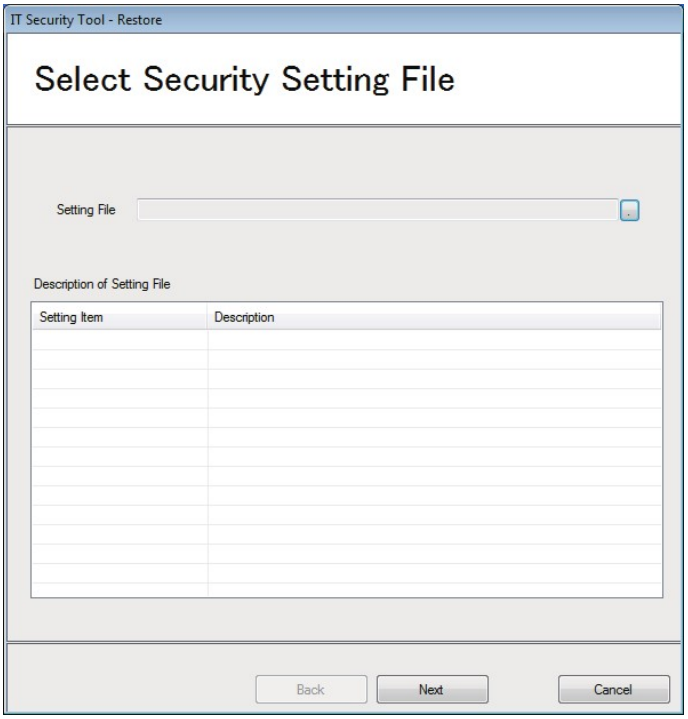


Figure 6.6.1-1 Select Security Setting File

3. Click [...] next to the Setting File box.
   The Open dialog box appears.
4. Select the file you want to use for restoration and then click [Open].

TIP Among the saved and created files, you need to select a file with .hed extension.

   A dialog box appears, prompting you to enter the password (encryption key) for reading the selected file.

5. Enter the password (encryption key) that was set when the file was saved and click [OK].
   If the selected file is restorable, the details are displayed in the Select Security Setting File page.
6. Click [Next].

The Confirm Setting Information page appears.

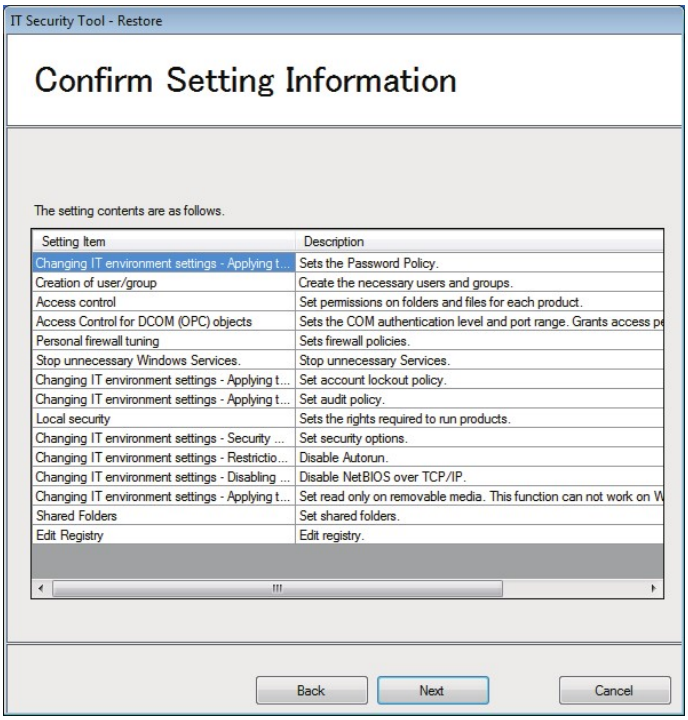


Figure 6.6.1-2 Confirm Setting Information

TIP

Items displayed in the Confirm Setting Information page represent the items accessed when restoring the saved security settings. Although the descriptions of these items are affirmative sentences, it doesn't mean that all of these settings will be applied. Note that the status of whether each item is set to be applied or not is not displayed on the screen.

7. Confirm the settings and click [Next].
   When the setup process is complete, the Setup Completed page appears.

TIP

If there are any items that failed to be set, a list of failed items is displayed.

8. Select the check box for [Restart Now] and click [Finish].
9. Click [Close] to end the IT Security Tool.

IMPORTANT

If any setup failures are displayed, contact YOKOGAWA Service.

SEE ALSO

For more information about ProSafe-RS applications that can start from Start menu, refer to:

"ProSafe-RS and ProSafe-RS Lite applications that can start from Start menu" in Read Me First (IM 32P01A30-01EN)

6.6.2 Procedure for a File Server or Domain Controller

To restore the IT security settings on a computer that serves only as a file server or a domain controller computer, start the installation menu from the ProSafe-RS software medium and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool. The rest of steps are the same as the procedure for an SENG PC.

SEE ALSO For more information about restoring IT security settings on a SENG PC, refer to:

"■ Restoring Procedure" on page 6-34

For more information about how to start the installation menu, refer to:

B3.5, "Installing the ProSafe-RS Software" in Installation Guide (IM 32P01C50-01EN)

6.7 Changing the Security Setting File Password

You can change the password (encryption key) for security setting files used by the IT Security Tool.

6.7.1 SENG PC, Computer Installed with Only AD Server, or Computer Dedicated to License Management

This section describes the procedure for changing the password for IT security setting files on an SENG PC, a computer installed with only AD Server, or a computer dedicated to license management.

When changing password, the two files with .hed version and .csf version having same file name are considered as a set. You can select either [One pair of] or [Multiple pair] for changing passwords. If you select [Multiple pair], the passwords of all the files within the specified folder are changed.

Changing Procedure

1. Log on as a member of the PSF_MAINTENANCE group.
2. From the Start menu, start the IT Security Tool.
3. Click [Change Password (Encryption Key)].
   The Specify backup file of security page appears.

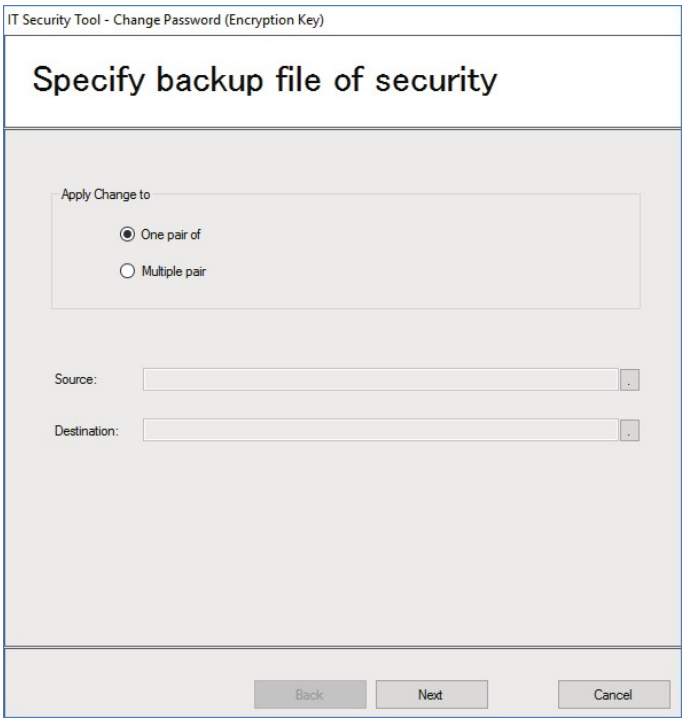


Figure 6.7.1-1 Specify backup file of security

4. Select either of the Apply change to options and set as follows:
   - For changing the encryption key of one pair
     In the [Apply change to] section, select [One pair of], and select the folder where the file set before change and the file set after change are to be saved. Select .hed file as the file set before change.
   - For changing the encryption key of multiple pair
     In the [Apply change to] section, select [Multiple pair], select the folder that contains the file set before change and the folder in which the file set after change is to be saved.
5. Click [Next].
   The Change Password (Encryption Key) page appears.



Figure 6.7.1-2 Change Password (Encryption Key)

6. Enter the old password and new password and click [Next].
   When the change of password (encryption key) is complete, the completion page appears.
7. Click [Finish].
8. On the IT Security Tool menu, click [Close].

SEE ALSO For more information about ProSafe-RS applications that can start from Start menu, refer to:

"ProSafe-RS and ProSafe-RS Lite applications that can start from Start menu" in Read Me First (IM 32P01A30-01EN)

6.7.2 Procedure for a File Server or Domain Controller

This section describes the procedure for changing the password (encryption key) for security setting files on a computer that serves only as a file server or a domain controller computer.

■ Changing Procedure

1. Log on as a member of the PSF_MAINTENANCE group.
2. From the software medium of ProSafe-RS, start the installation menu, click [IT Security Settings (for file server/domain controller)], and then start the IT Security Tool.
   The rest of steps are the same as the procedure for an SENG PC.

SEE ALSO

For more information about changing the password for the security setting files on a SENG PC, refer to:

"■ Changing Procedure" on page 6-38

For more information about how to start the installation menu, refer to:

B3.5, "Installing the ProSafe-RS Software" in Installation Guide (IM 32P01C50-01EN)

6.8 Exporting/Importing the IT Security Setting File

ProSafe-RS provides the function to export and import the selection state of the previously configured IT security settings.

The following IT security settings are the targets of export and import:

- IT security settings configured with R4.03 or later
  Use the export/import function of the IT Security Tool.
- IT security settings that were configured before R4.03
  To export the selection state of the settings configured before R4.03, use the ITSecurity-SettingItemExport tool that is included in the software medium.

  The exported files can be imported by using the IT Security Tool.

You can export and import the setting status configured in the page of "Select Setting Items" of the IT Security Tool.

IMPORTANT

- The Export/Import function reproduces the setting status configured by the IT Security Tool, but does not change the Domain link status displayed in the "Current status" dialog box. The domain link status can be changed by using the Domain Link Management Tool.

  For example, if you import the IT security setting file that was exported from a computer whose domain link status is Linked to a computer whose domain link status is Not linked, the domain link status of the destination computer remains Not linked.

  Conversely, if you import the IT security setting file that was exported from a computer whose domain link status is Not linked to a computer whose domain link status is Linked, the domain link status of the import destination computer remains Linked.
- If you export the IT security setting file from a computer that has domain management, combination management, or legacy model applied, and import the file to a computer whose domain link status is Linked, the import will succeed. If you try to continue the setting, a dialog box will appear prompting you to apply standalone management or close the IT Security Tool and change to another user management type. Take either action.
- After setting IT security by using the Import function, check the Current status dialog box to see if the domain link status is in the expected status. If required, change the user management type or the domain link status.
- You cannot use the ITSecuritySettingItemExport tool on file servers and domain controllers that were configured by using the IT Security Tool before R4.03. The IT security settings in these environments need to be restored manually.

6.8.1 Procedure to Export by Using the IT Security Tool

Follow these steps to export the IT security settings that were configured with R4.03 or later:

1. From the Start menu, start the IT Security Tool.

TIP

For a file server or a domain controller, start the installation menu from the software medium of the product, and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.

2. Click [Import or Export].
   The Export or Import the Selection State of Setting Items dialog box appears.
3. Select [Export].
   The default export destination file name appears automatically in the text box for file name entry.
   `C:\ProgramData\Yokogawa\IA\iPCS\Platform\Security\Config\DisplaySelectInfo.xml`
4. Leave the default file name as is, or change it if necessary.

TIP

Specify xml as the file extension. When any other extension is specified, ".xml" is added automatically to the end of the file name.

5. Click [Execute].
   The export processing starts. If you specified an existing file, the file will be overwritten.

   The following information is written to the specified file, and the Export or Import the Selection State of Setting Items dialog box closes.

   - Security model
   - User management type
   - IT security version
   - State of check box selections made in the Select Setting Items page of the tool

SEE ALSO

For more information about ProSafe-RS applications that can start from Start menu, refer to:

"ProSafe-RS and ProSafe-RS Lite applications that can start from Start menu" in Read Me First (IM 32P01A30-01EN)

6.8.2 Procedure to Export by Using the ITSecuritySettingItemExport Tool

Follow these steps to export the IT security settings that were configured before R4.03:

1. Run the following tool in the software medium as a user with administrative rights.
   `<Drive of ProSafe-RS software medium>:\ProSafe-RS\SECURITY\ITSecuritySettingItemExport.exe`
   The export processing starts. If you specified an existing file, the file will be overwritten.

   The following information is written to the specified file, and the Export or Import the Selection State of Setting Items dialog box closes.

   - Security model
   - User Management Types
   - IT security version
   - State of check box selections made in the Select Setting Items page of the tool

6.8.3 Procedure to Import by Using the IT Security Tool

Follow these steps to import the export IT security settings:

1. From the Start menu, start the IT Security Tool.

TIP

For a file server or a domain controller, start the installation menu from the software medium of the product, and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.

2. Click [Import or Export].
   The Export or Import the Selection State of Setting Items dialog box appears.
3. Select [Import].
   The text box is cleared.
4. Specify the file that you want to import.
5. Click [Execute].
   The Export or Import the Selection State of Setting Items dialog box closes.
6. In the IT Security Tool, click [Setup].
   The imported IT security settings are applied.

TIP

Alternatively, you can also import the selection state of IT security settings by clicking [Setup] in the IT Security Tool and then clicking [Import] in the IT Security Settings page.

SEE ALSO

For more information about ProSafe-RS applications that can start from Start menu, refer to:

"ProSafe-RS and ProSafe-RS Lite applications that can start from Start menu" in Read Me First (IM 32P01A30-01EN)

6.9 Viewing the Information Configured by the IT Security Tool

The information set by the IT Security Tool is displayed in the same dialog box as the Current status dialog box of the Domain Link Management Tool. In this dialog box, in addition to the information set by the IT Security Tool, the status related to linked domain management appears.

The items displayed as information set by the IT Security Tool are as follows:

- Computer information
  - IT security version
  - Security model
  - User management type
- Information for each product
  Security setting status

SEE ALSO For more information about the details of security setting status, refer to:

"■ Current status" on page 6-6

■ Procedure for Viewing

1. Sign in as a member of the PSF_MAINTENANCE group.
2. From the Start menu, start the IT Security Tool.

TIP For a file server or a domain controller, start the installation menu from the software medium of the product, and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.

3. Click the [Information] button.
   The Current status dialog box appears.

SEE ALSO For more information about ProSafe-RS applications that can start from Start menu, refer to:

"ProSafe-RS and ProSafe-RS Lite applications that can start from Start menu" in Read Me First (IM 32P01A30-01EN)

6.10 Active Directory-Based Consolidated Management of IT Security Settings

Windows Active Directory has a feature called Group Policy that is used to centrally manage the IT environment of computers and users. Using this Group Policy, you can manage the security policies for client computers within the domain in bulk by offering files for importing IT security settings. The following tasks are required:

- On the domain controller, create group policy objects for implementing security policies.
- By using Active Directory services, create Organizational Units on the domain controller and apply the group policy objects.

TIP

Active Directory-based consolidated management of IT security settings can be applied to computers on which R4.03 or later versions ProSafe-RS software installed.

6.10.1 Creating Group Policy Objects

Follow these steps to create group policy objects for implementing security policies on the domain controller:

1. Insert the software medium of the product into the drive of the domain controller computer.
2. Using Explorer, copy the following file to any folder on the domain controller. You must copy the file to a folder to which the administrator of the domain can access.
   `<Drive of ProSafe-RS software medium>:\ProSafe-RS\SECURITY\GPOFiles\xxx\PSF_Standard_xxx.zip`

   When xxx = 2.0 : The file corresponds to the Standard model of IT security version 2.0

   When xxx = 1.0 : The file corresponds to the Standard model of IT security version 1.0
3. Double click the file that you have copied.
   The file expands into files for import.
4. Open the Control Panel.
5. Select [Administrative Tools] > [Group Policy Management].
   The Group Policy Management dialog box appears.
6. In the left pane, right-click [Group Policy Objects] and select [New].
   The New GPO dialog box appears.
7. Set as follows:
   - Type any name for Name.
   - Select [(none)] for Source Starter GPO.
8. Click [OK].
   A new group policy object is created.
9. Right-click the new group policy object and select [Import Settings].
   The [Import Settings Wizard] appears.
10. Click [Next].
    A dialog box appears, prompting you to back up the existing settings.
11. Since it is a newly created group policy object, click [Next] without backing up.
    [Backup location] appears.
12. In the [Backup folder], select the parent folder of the folder to be imported, and click [Next].
    A list of importable group polices that are stored under the selected parent folder appears.

TIP If you want to view the setting information of the group policy object, click [View Settings...]. The information is displayed in Microsoft Internet Explorer.

13. Select the group policy and click [Next].
    A confirmation dialog box appears, showing whether the group policy to be imported contains any references to security principals or UNC paths.

TIP The following message is displayed in the confirmation dialog box.

"Scan Results:

The Backup do not contain any references to security principals or UNC paths. To continue, click [Next]."

14. Click [Next].
    The [Completing the Import Settings Wizard] dialog box appears.
15. Click [Finish].

Importing of the group policy object starts.

16. When the importing is completed, confirm the imported policy in [Group Policy Management].
17. Open the Control Panel and select [Administrative Tools] > [Group Policy Management] to open Group Policy Management. In the left pane, right-click the target group policy and select [View].

Creation of a group policy object is now completed. Subsequently, you need to create Organizational Units on the domain controller and apply group policy objects to them.

6.10.2 Applying Group Policy Objects to an Organizational Unit

Follow these steps to apply group policy objects to an Organizational Unit on the domain controller:

1. Log on to the domain controller as an administrative user.
2. Open the Control Panel.
3. Select [Administrative Tools] > [Active Directory Users and Computers].
   [Active Directory Users and Computers] appears.
4. In the left pane, right-click the domain controller where you want to create an Organizational Unit, and select [New] > [Organizational Unit].
   [New Object - Organizational Unit] appears.
5. Set as follows:
   - In the Name box, type any name for the Organizational Unit.
   - Select the [Protect container from accidental deletion] check box.
6. Click [OK].
   A new Organizational Unit is created.
7. As necessary, build a hierarchy of Organizational Units. You can build it by repeating steps 3 to 5.
8. In the left pane of [Active Directory Users and Computers], select [Computers]. From the computers list that is displayed, select the computers to be added to Organizational Units, and drag and drop them to the target Organizational Units as desired. A warning message regarding moving the objects appears, but click [Yes] to continue.

TIP

The computers that belong to an Organizational Unit must be limited to computers to which the same group policies are to be applied. Because you will apply group policies to the Organizational Units in the subsequent procedure, ensure that one Organizational Unit does not contain computers with different IT security levels.

Creation of Organizational Units is now completed. The next task is to apply group policy objects to the Organizational Units.

Deleting an Organizational Unit

If the Protect container from accidental deletion check box was selected in the [New Object - Organizational Unit] dialog box at the creation of an Organizational Unit, a message appears when you delete that Organizational Unit. Follow these steps to delete such an Organizational Unit:

1. Open the Control Panel.
2. Select [Administrative Tools] > [Active Directory Users and Computers].
   [Active Directory Users and Computers] appears.
3. Right-click the Organizational Unit that you want to delete and select [Properties], then click the [Object] tab. If the [Object] tab is not displayed, you can make it visible by selecting [View] > [Advanced Features] in [Active Directory Users and Computers].
4. Click the [Protect container from accidental deletion] check box, and click [OK].
   Now you can delete this Organizational Unit.
5. Delete the Organizational Unit.

Deletion of an Organizational Unit is now completed.

Applying Group Policy Objects to an Organizational Unit

Follow these steps:

1. Open the Control Panel.
2. Select [Administrative Tools] > [Group Policy Management].
   [Group Policy Management] appears.
3. In the left pane, select [Group Policy Objects]. From the object list that is displayed, select the group policy that you want to apply, and drag and drop them to the target Organizational Unit.
   A confirmation dialog box appears.
4. Click [OK].
   Group Policy Management Console appears. If you change the applied group policy object here, you are notified that the change will be shared with other Organizational Units.
5. Click [OK].
6. Restart the domain controller.

Application of group policy objects is now completed.

TIP

Even if you do not restart the domain controller, the group policy object will be updated when the group policy checking function of the OS runs.

Canceling Application of Group Policy Objects to an Organizational Unit

Even if you cancel application of a group policy object to an Organizational Unit, the group policy object itself is not deleted.

Follow these steps:

1. Open the Control Panel.
2. Select [Administrative Tools] > [Group Policy Management].
   [Group Policy Management] appears.
3. Select the Organizational Unit in the left pane, right-click the group policy object that you want to cancel application, and select [Delete].
   A confirmation message appears.
4. Click [OK].

Application of a group policy object for an Organizational Unit has been canceled.

6.11 Other Utility Programs

This section describes the utility programs other than the IT Security Tool.

6.11.1 CreateProSafeProcess

This utility program creates the PSF_PROCESS user. It is also used to change the password of the PSF_PROCESS user.

Detailed Explanation

CreateProSafeProcess is used on computers installed with ProSafe-RS or CENTUM VP and on file server computers. This tool creates the PSF_PROCESS user and automatically sets a password for it. If you want to manage the password, you can specify an option to set a desired password.

Start Method

Follow these steps to start CreateProSafeProcess.

1. Log on using an administrative user account.
2. Insert the ProSafe-RS software medium into the drive, start the command prompt window, and move to the following folder.
   `<Drive of software medium>:\ProSafe-RS\SECURITY`
3. Run the following command.
   `ProSafe.Security.CreateProSafeProcess.exe`

   If the PSF_PROCESS user does not exist, it is created and a password is set automatically. The passwords for Windows services registered for use by the PSF_PROCESS user are also set.

   If the PSF_PROCESS user already exists, its password is changed to the initial password.

TIP

If you want to set a desired password, run the following command.

```
ProSafe.Security.CreateProSafeProcess.exe -p(password to be set)
```

You can set a password within 127 characters. Setting a password is mandatory. If the PSF_PROCESS user does not exist, it is created and the specified password is set. At the same time, the passwords for Windows services registered for use by the PSF_PROCESS user are also changed to the specified password.

If the PSF_PROCESS user already exists, its password is changed to the specified password.

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on all computers on which the PSF_PROCESS user exists, such as the computers installed with ProSafe-RS or other software packages that collaborate with ProSafe-RS and file server computers.
- After you change the password of an existing PSF_PROCESS user, restart the computer.

6.11.2 CreateLicenseProcess

This utility program changes the password of the LIC_PROCESS user.

Detailed Explanation

CreateLicenseProcess is used on computers installed with ProSafe-RS or CENTUM VP and on file server computers. By running this tool, you can set a desired password for the LIC_PROCESS user.

Start Method

Follow these steps to start CreateLicenseProcess.

1. Log on using an administrative user account.
2. Insert the ProSafe-RS software medium into the drive and run the following command from the command prompt window.
   ```
   <Drive of software medium>:\ProSafe-RS\SECURITY\Yokogawa.IA.iPCS.Platform.License.CreateLicenseProcess.exe -p (password to be set)
   ```

TIP

You can set a password within 127 characters. Setting a password is mandatory. At the same time, the passwords for Windows services registered for use by the LIC_PROCESS user are also changed to the specified password.

If you run the command without specifying "-p (password to be set)," the currently set password is changed to the initial password.

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on all computers on which the LIC_PROCESS user exists, such as the computers installed with ProSafe-RS or other software packages that collaborate with ProSafe-RS and file server computers.
- After you change the password of an existing LIC_PROCESS user, restart the computer.

6.11.3 CreateAdsProcess

This utility creates the ADS_PROCESS user. It is also used to change the password of the ADS_PROCESS user.

Detailed Explanation

CreateAdsProcess is a tool that is used on the Automation Design Server computer. This tool creates the ADS_PROCESS user and automatically sets a password for it. If you want to manage the password, you can specify an option to set a desired password.

Start Method

Follow these steps to start CreateAdsProcess:

1. Log on using an administrative user account.
2. Insert the ProSafe-RS software medium into the drive and run the following command from the command prompt window.
   `<Drive of software medium>:\ProSafe-RS\SECURITY\Yokogawa.IA.iPCS.ChronusENG.Security.CreateAdsProcess.exe`

   If the ADS_PROCESS user does not exist, it is created and a password is set automatically. The passwords for Windows services registered for use by the ADS_PROCESS user are also set.

   If the ADS_PROCESS user exists, its password is changed to the default password.

TIP

If you want to set a desired password, run the following command:

`<Drive of software medium>:\ProSafe-RS\SECURITY\Yokogawa.IA.iPCS.ChronusENG.Security.CreateAdsProcess.exe -p (password to be set)`

You can specify a password within 127 characters. No password is not allowed. If the ADS_PROCESS user does not exist, it is created and the specified password is set. At the same time, the passwords for Windows services that are registered for use by the ADS_PROCESS user are also changed to the specified password.

If the ADS_PROCESS user exists, its password is changed to the specified password.

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on all computers on which the ADS_PROCESS user exists, such as the computers installed with ProSafe-RS or other software packages that collaborate with ProSafe-RS.
- After you change the password of an existing ADS_PROCESS user, restart the computer.

SEE ALSO

For more information about Automation Design Server, refer to:

A., “Overview of Automation Design Suite” in Engineer's Reference Manual (IM 32P04B10-01EN)

6.11.4 CreateAdsAgent

Using this utility, you can change the password of the ADS_AGENT user.

Detailed Explanation

CreateAdsAgent is used on computers where ProSafe-RS is installed. By running this tool, you can set a desired password for the ADS_AGENT user.

TIP

For more information about running this tool, contact YOKOGAWA Service.

Start Method

Follow these steps to start CreateAdsAgent.

1. Log on as a user with administrative rights.
2. Insert the ProSafe-RS software medium into the drive and run the following command from the command prompt window.

   ```
   <Drive of software medium>:\ProSafe-RS\SECURITY\Yokogawa.IA.iPCS.ChronusENG.Security.CIM.CreateAdsAgent.exe -p (password to be set)
   ```

   You can set a password within 127 characters. Setting a password is mandatory.

   When you run this command, the passwords for Windows services registered for use by the ADS_AGENT user are also changed to the same password.

TIP

If you run the command without specifying a password, the default password is set.

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on all the PCs where the ADS_AGENT user exists.
- After you change the password of an existing ADS_AGENT user, restart the PC.

6.11.5 YWVNETCreateVNTUser

YWVNETCreateVNTUser is a utility program that changes the password of the users for running Vnet/IP Interface Package. This utility changes the password of the following users:

- VNT_COMMON
- VNT_NVP_CORE
- VNT_BKNET

IMPORTANT

- When you change the password, you must prepare an ISO format file of the ProSafe-RS software medium in advance.
- To be able to change the password, Vnet/IP Interface Package must be installed. Before you change the password, make sure that Vnet/IP Interface Package is installed on the computer.
- After you change the password, restart the virtual machine.

Start Method

Follow these steps to start YWVNETCreateVNTUser:

1. Sign in to the host OS of the virtualization host computer as an administrative user.
2. Copy the ISO format file of the ProSafe-RS software to a folder in the host OS.
3. Select [Start] > [Server Manager].
   Server Manager starts.
4. Select [Tools] > [Hyper-V Manager].
   Hyper-V Manager starts.
5. On the left pane, select the virtualization host computer.
   The virtual machines on the selected virtualization host computer appear on the middle pane of Hyper-V Manager.
6. Right-click the virtual machine on which you want to run YWVNETCreateVNTUser, and select [Connect].
   The Connect Virtual Machine window appears.

TIP The Connect Virtual Machine window may be displayed full-screen. If it is displayed full-screen, click [Restore] to exit the full-screen mode.

7. Select [Media] > [DVD Drive] > [Insert Disk].
   The Open dialog box appears.
8. Select the ISO format file of the ProSafe-RS software medium that you have copied and click [Open].
   The selected ISO format file is mounted to the virtual machine.
9. Run the Command Prompt as Administrator.
10. Run the following command from the command prompt window:
    <Mounted drive>:`\ProSafe-RS\security\ywvnetcreatevntuser.exe -u user name -p password to be set`

    You can set a password within 127 characters. Setting a password is mandatory.
11. Restart the virtual machine.

IMPORTANT

- You must run this utility with Vnet/IP Interface Package installed. If you have changed the password by using this utility while Vnet/IP Interface Package is not installed, change the password again after installing Vnet/IP Interface Package.
- If you install Vnet/IP Interface Package after changing the password, the changed password will be reset. Therefore, change the password again.

6.11.6 CreateTISService

Using this utility, you can change the password of the TIS_SERVICE user.

Detailed Explanation

CreateTISService is a tool which is used on a computer where Dongle Gateway is installed. By running this tool, you can set a desired password for the TIS_SERVICE user.

Start Method

Follow these steps to start CreateTISService:

1. Sign in as a user with administrative rights.
2. Insert the ProSafe-RS software medium into the drive and run the following command from the command prompt window. In the case of a virtualization environment, mount the ISO format file of the ProSafe-RS software medium on the virtual machine and then run the command.
   ```
   <Drive of software medium>:\ProSafe-RS\SECURITY\Yokogawa.IA.iPCS.ProSafe.Security.CreateTISService.exe -p (password to be set)
   ```
   You can set a password within 127 characters. Setting a password is mandatory.

   When you run this command, the passwords for Windows services registered for use by the TIS_SERVICE user are also changed to the same password.

TIP

If you run the command without specifying a password, the default password is set.

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on all the computers where the TIS_SERVICE user exists.
- After you change the password of an existing TIS_SERVICE user, restart the computer.

SEE ALSO

For more information about how to mount the ISO format file on the virtual machine, refer to:

"● Mounting an ISO Format File on a Virtual Machine" in "■ Creating and Mounting ISO Format Files" in B1.3, "Precautions for Setting Up ProSafe-RS on a Virtual Machine on the Virtualization Platform" in Installation Guide (IM 32P01C50-01EN)

6.11.7 StorageDeviceCTL

This utility temporarily cancels the following disabling of storage devices.

- Disabling of write permissions set by applying the StorageDevicePolicies function
- Disabling set by applying "Disabling USB storage devices"

Detailed Explanation

When you cannot write to storage devices due to application of the StorageDevicePolicies function or disabling of USB storage devices, you can execute StorageDeviceCTL to cancel the effect of these security measures temporarily. Writing to storage devices is enabled while StorageDeviceCTL is running.

Start this tool, connect a USB storage device to the PC, and then perform writing tasks.

The PSF_MAINTENANCE right is required to execute the tool.

Use this tool only on PCs for which the StorageDevicePolicies function or disabling of USB storage devices is set.

IMPORTANT

Be sure to make the PC recognize the storage device after starting this tool.

Start Method

Follow these steps to start StorageDeviceCTL:

1. Use Windows Explorer to open the following folder.
   This example is when the system drive is drive C.

   `C:\Program Files (x86)\Yokogawa\IA\iPCS\Platform\SECURITY\PROGRAM\`

2. Double click the following program file in the folder.
   `Yokogawa.IA.iPCS.Platform.Security.StorageDeviceCTL.exe`

   The task is displayed only in the taskbar immediately after the start.

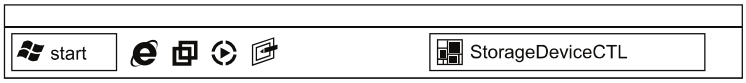


Figure 6.11.7-1 Taskbar

3. Connect the USB storage device to the computer.
4. Read/write necessary data from/to the USB storage device.
5. Remove the USB storage device from the computer.

TIP

To remove a USB storage device, right-click the [Safely Remove Hardware and Eject Media] icon from the task tray and select [Eject USB Flash Disk] to stop the device.

6. Click [StorageDeviceCTL] from the taskbar and then click [WriteStop].

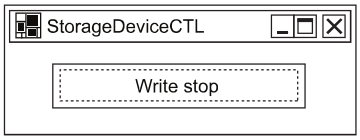


Figure 6.11.7-2 StorageDeviceCTL Dialog Box

StorageDeviceCTL ends and USB storage devices are disabled again.

SEE ALSO

For more information about the StorageDevicePolicies function, refer to:

3.5.4, “Applying the StorageDevicePolicies Function” on page 3-30

For more information about disabling USB storage devices, refer to:

3.5.5, “Disabling USB Storage Devices” on page 3-31

6.11.8 ITSecuritySettingItemExport

This utility exports the security model, user management type, changes made to settings, and IT security version number that were set by the IT Security Tool of R4.02 or earlier to a file.

Detailed Explanation

The exported information is the settings at the last IT security configuration of the environment where you run the utility.

By importing the exported file using the IT Security Tool, you can restore the security setting status that was configured by the IT Security Tool of the environment where the information was exported.

Start Method

Follow these steps to run the ITSecuritySettingItemExport utility:

1. Log on as a user with administrative rights.
2. Insert the software medium of the product into the drive, and run the following command from the command prompt:
   `<Drive of software medium>:\ProSafe-RS\SECURITY\ITSecuritySettingItemExport.exe`
3. After running the utility, a file is automatically created and a confirmation dialog box appears. Click [OK].
   The file is exported to the following fixed folder. This example is when the system drive is drive C.

   `C:\ProgramData\Yokogawa\IA\iPCS\Platform\Security\Config\DisplaySelectInfo.xml`

IMPORTANT

- This utility is available only on computers where a YOKOGAWA system product is installed. It is not available on a file server or domain controller, where security configuration is performed by using the IT Security Tool without installing product software.
- The account used to run this utility must belong to the maintenance group of the product.
- The folder and file that are exported by this utility have a fixed name. If they exist on the computer already, the file will be overwritten.
- When you cannot access the folder and file that are exported by this utility, an access violation error message appears.

Appendix 1. IT Security Setting Items

This section describes the security setting items that are configured with IT security version 2.0 and IT security version 1.0.

Appendix 1.1 IT Security Version 2.0

This section describes the security setting items that are configured with IT security version 2.0, their default values, and whether they can be modified.

Appendix 1.1.1 Setting Items for a Computer with ProSafe-RS Software Installed

This section describes the security setting items for a computer on which the product software is installed for each combination of security model and user management type.

Security Setting Items for Standard Model with Standalone Management/Linked Domain Management

The following table shows the security setting items for the combination of Standard model and Standalone management or Linked domain management.

Table Appendix 1.1.1-1 Standard Model - Standalone Management/Linked Domain Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Access control for product registry	Selected	Fixed
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Disable 'Personal Firewall-[Allow unicast response]'	Selected	Editable
Disabling NetBIOS over TCP/IP	When the domain is linked: Selected When the domain is not linked: Clear	Editable
Applying the StorageDevicePolicies function	Clear	Editable
Disabling USB storage devices	Clear	Editable
Applying the software restriction policies	Clear	Editable
User Rights Assignment-[Deny log on locally]	Selected	Fixed
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Selected	Editable
Security Options-[Devices: Prevent users from installing printer drivers]	Selected	Editable
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Selected	Editable
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Selected	Editable
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Selected	Editable
Security Options-[Interactive logon: Do not display last user name]	Selected	Fixed
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]'	Selected	Editable
Security Options-[Interactive logon: Prompt user to change password before expiration]	Selected	Editable
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Selected	Editable
Security Options-[Microsoft network server: Server SPN target name validation level]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-1 Standard Model - Standalone Management/Linked Domain Management (Table continued)

Setting item	Default check box state	Modification
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Selected	Editable
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Selected	Editable
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Selected	Editable
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Selected	Editable
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Selected	Editable
Disable 'Security Options-[Network security: Allow Local System NULL session fallback]'	Selected	Editable
Security Options-[Network security: LAN Manager authentication level]	Selected	Fixed
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Selected	Editable
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Selected	Editable
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Selected	Editable
Security Options-[User Account Control: Admin Approval Mode for the Built-in Administrator account]	Selected	Editable
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Credential Validation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security Group Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit User Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Process Creation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Account Lockout]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logoff]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Logon/Logoff Events]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-1 Standard Model - Standalone Management/Linked Domain Management (Table continued)

Setting item	Default check box state	Modification
Advanced Audit Policy Configuration-[Audit Special Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Removable Storage]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other System Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security State Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security System Extension]	Selected	Editable
Advanced Audit Policy Configuration-[Audit System Integrity]	Selected	Editable
Personalization-[Prevent enabling lock screen camera]	Selected	Editable
Personalization-[Prevent enabling lock screen slide show]	Selected	Editable
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services]	Selected	Editable
Group Policy-[Configure registry policy processing]	Selected	Editable
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Selected	Editable
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Selected	Editable
Internet Communication settings-[Turn off printing over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Search Companion content file updates]	Selected	Editable
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Selected	Editable
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Clear	Fixed
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Clear	Fixed
Logon-[Do not display network selection UI]	Selected	Editable
Logon-[Do not enumerate connected users on domain-joined computers]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-1 Standard Model - Standalone Management/Linked Domain Management (Table continued)

Setting item	Default check box state	Modification
Disable 'Logon-[Enumerate local users on domain-joined computers]'	Selected	Editable
Logon-[Turn off app notifications on the lock screen]	Selected	Editable
Mitigation Options-[Untrusted Font Blocking]	Selected	Editable
User Profiles-[Turn off the advertising ID]	Selected	Editable
App Privacy-[Let Windows apps access account information]	Selected	Editable
App Privacy-[Let Windows apps access call history]	Selected	Editable
App Privacy-[Let Windows apps access contacts]	Selected	Editable
App Privacy-[Let Windows apps access email]	Selected	Editable
App Privacy-[Let Windows apps access location]	Selected	Editable
App Privacy-[Let Windows apps access messaging]	Selected	Editable
App Privacy-[Let Windows apps access motion]	Selected	Editable
App Privacy-[Let Windows apps access the calendar]	Selected	Editable
App Privacy-[Let Windows apps access the camera]	Selected	Editable
App Privacy-[Let Windows apps access the microphone]	Selected	Editable
App Privacy-[Let Windows apps access trusted devices]	Selected	Editable
App Privacy-[Let Windows apps control radios]	Selected	Editable
App Privacy-[Let Windows apps sync with devices]	Selected	Editable
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Selected	Editable
AutoPlay Policies-[Turn off Autoplay]	Selected	Editable
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Selected	Editable
Cloud Content-[Do not show Windows Tips]	Selected	Editable
Cloud Content-[Turn off Microsoft consumer experiences]	Selected	Editable
Data Collection and Preview Builds-[Allow Telemetry]	Selected	Editable
Data Collection and Preview Builds-[Disable pre-release features or settings]	Selected	Editable
Data Collection and Preview Builds-[Do not show feedback notifications]	Selected	Editable
Data Collection and Preview Builds-[Toggle user control over Insider builds]	Selected	Editable
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(System)-[Specify the maximum log file size (KB)]	Selected	Editable
File Explorer-[Turn off heap termination on corruption]	Selected	Editable
HomeGroup-[Prevent the computer from joining a homegroup]	Selected	Editable
OneDrive-[Prevent the usage of OneDrive for file storage]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-1 Standard Model - Standalone Management/Linked Domain Management (Table continued)

Setting item	Default check box state	Modification
OneDrive-[Save documents to OneDrive by default] (Save documents to the local PC by default)	Selected	Editable
Remote Desktop Connection Client-[Do not allow passwords to be saved]	Selected	Editable
Device and Resource Redirection-[Do not allow drive redirection]	Selected	Editable
Security-[Require secure RPC communication]	Selected	Editable
Security-[Require user authentication for remote connections by using Network Level Authentication]	Selected	Editable
Disable 'Search-[Allow Cortana]'	Selected	Editable
Software Protection Platform-[Turn off KMS Client Online AVS Validation]	Selected	Editable
Sync your settings-[Do not sync Apps]	Selected	Editable
Sync your settings-[Do not sync start settings]	Selected	Editable
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Selected	Fixed
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Selected	Editable
Notifications-[Turn off toast notifications on the lock screen]	Selected	Editable

SEE ALSO For more information about creation of users/groups, refer to:

"■ Combination of User Management and Security Model for Windows" on page 2-17

■ Security Setting Items for Standard Model with Domain or Combination Management

The following table shows the security setting items for the combination of Standard model and Domain or Combination management.

Table Appendix 1.1.1-2 Standard Model - Domain/Combination Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Access control for product registry	Selected	Fixed
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Disable 'Personal Firewall-[Allow unicast response]'	Selected	Editable
Disabling NetBIOS over TCP/IP	Selected	Editable
Applying the StorageDevicePolicies function	Clear	Editable
Disabling USB storage devices	Clear	Editable
Applying the software restriction policies	Clear	Editable

Continues on the next page

Table Appendix 1.1.1-2 Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Selected	Editable
Security Options-[Devices: Prevent users from installing printer drivers]	Selected	Editable
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Selected	Editable
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Selected	Editable
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Selected	Editable
Security Options-[Interactive logon: Do not display last user name]	Selected	Fixed
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]'	Selected	Editable
Security Options-[Interactive logon: Prompt user to change password before expiration]	Selected	Editable
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Selected	Editable
Security Options-[Microsoft network server: Server SPN target name validation level]	Selected	Editable
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Selected	Editable
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Selected	Editable
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Selected	Editable
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Selected	Editable
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Selected	Editable
Disable 'Security Options-[Network security: Allow LocalSystem NULL session fallback]'	Selected	Editable
Security Options-[Network security: LAN Manager authentication level]	Selected	Fixed
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Selected	Editable
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Selected	Editable
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Selected	Editable
Security Options-[User Account Control: Admin Approval Mode for the Built-in Administrator account]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-2 Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Credential Validation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security Group Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit User Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Process Creation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Account Lockout]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logoff]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Logon/Logoff Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Special Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Removable Storage]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other System Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security State Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security System Extension]	Selected	Editable
Advanced Audit Policy Configuration-[Audit System Integrity]	Selected	Editable
Personalization-[Prevent enabling lock screen camera]	Selected	Editable
Personalization-[Prevent enabling lock screen slide show]	Selected	Editable
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-2 Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Group Policy-[Configure registry policy processing]	Selected	Editable
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Selected	Editable
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Selected	Editable
Internet Communication settings-[Turn off printing over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Search Companion content file updates]	Selected	Editable
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Selected	Editable
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Selected	Fixed
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Selected	Fixed
Logon-[Do not display network selection UI]	Selected	Editable
Logon-[Do not enumerate connected users on domain-joined computers]	Selected	Editable
Disable 'Logon-[Enumerate local users on domain-joined computers]'	Selected	Editable
Logon-[Turn off app notifications on the lock screen]	Selected	Editable
Mitigation Options-[Untrusted Font Blocking]	Selected	Editable
User Profiles-[Turn off the advertising ID]	Selected	Editable
App Privacy-[Let Windows apps access account information]	Selected	Editable
App Privacy-[Let Windows apps access call history]	Selected	Editable
App Privacy-[Let Windows apps access contacts]	Selected	Editable
App Privacy-[Let Windows apps access email]	Selected	Editable
App Privacy-[Let Windows apps access location]	Selected	Editable
App Privacy-[Let Windows apps access messaging]	Selected	Editable
App Privacy-[Let Windows apps access motion]	Selected	Editable
App Privacy-[Let Windows apps access the calendar]	Selected	Editable
App Privacy-[Let Windows apps access the camera]	Selected	Editable
App Privacy-[Let Windows apps access the microphone]	Selected	Editable
App Privacy-[Let Windows apps access trusted devices]	Selected	Editable
App Privacy-[Let Windows apps control radios]	Selected	Editable
App Privacy-[Let Windows apps sync with devices]	Selected	Editable
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Selected	Editable
AutoPlay Policies-[Turn off Autoplay]	Selected	Editable
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Selected	Editable
Cloud Content-[Do not show Windows Tips]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-2 Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Cloud Content-[Turn off Microsoft consumer experiences]	Selected	Editable
Data Collection and Preview Builds-[Allow Telemetry]	Selected	Editable
Data Collection and Preview Builds-[Disable pre-release features or settings]	Selected	Editable
Data Collection and Preview Builds-[Do not show feedback notifications]	Selected	Editable
Data Collection and Preview Builds-[Toggle user control over Insider builds]	Selected	Editable
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(System)-[Specify the maximum log file size (KB)]	Selected	Editable
File Explorer-[Turn off heap termination on corruption]	Selected	Editable
HomeGroup-[Prevent the computer from joining a home-group]	Selected	Editable
OneDrive-[Prevent the usage of OneDrive for file storage]	Selected	Editable
OneDrive-[Save documents to OneDrive by default] (Save documents to the local PC by default)	Selected	Editable
Remote Desktop Connection Client-[Do not allow pass-words to be saved]	Selected	Editable
Device and Resource Redirection-[Do not allow drive redi-rection]	Selected	Editable
Security-[Require secure RPC communication]	Selected	Editable
Security-[Require user authentication for remote connec-tions by using Network Level Authentication]	Selected	Editable
Disable ‘Search-[Allow Cortana]’	Selected	Editable
Software Protection Platform-[Turn off KMS Client Online AVS Validation]	Selected	Editable
Sync your settings-[Do not sync Apps]	Selected	Editable
Sync your settings-[Do not sync start settings]	Selected	Editable
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Selected	Fixed
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Selected	Editable
Notifications-[Turn off toast notifications on the lock screen]	Selected	Editable

SEE ALSO For more information about creation of users/groups, refer to:

“■ Combination of User Management and Security Model for Windows” on page 2-17

Appendix 1.1.2 Setting Items for a File Server or Domain Controller

This section provides lists of the security setting items for a file server or a domain controller for each combination of security model and user management type.

Security Setting Items for File Server: Standard Model with Standalone Management/Linked Domain Management

The following table shows the security setting items for the combination of Standard model and Standalone management or Linked domain management on a file server.

Table Appendix 1.1.2-1 File Server: Standard Model - Standalone Management/Linked Domain Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Disable 'Personal Firewall-[Allow unicast response]'	Selected	Editable
Disabling NetBIOS over TCP/IP	When the domain is linked: Selected When the domain is not linked: Clear	Editable
Applying the StorageDevicePolicies function	Clear	Editable
Disabling USB storage devices	Clear	Editable
User Rights Assignment-[Deny log on locally]	Selected	Fixed
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Selected	Editable
Security Options-[Devices: Prevent users from installing printer drivers]	Selected	Editable
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Selected	Editable
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Selected	Editable
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Selected	Editable
Security Options-[Interactive logon: Do not display last user name]	Selected	Editable
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]'	Selected	Editable
Security Options-[Interactive logon: Prompt user to change password before expiration]	Selected	Editable
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Selected	Editable
Security Options-[Microsoft network server: Server SPN target name validation level]	Selected	Editable
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-1 File Server: Standard Model - Standalone Management/Linked Domain Management (Table continued)

Setting item	Default check box state	Modification
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Selected	Editable
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Selected	Editable
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Selected	Editable
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Selected	Editable
Disable 'Security Options-[Network security: Allow Local System NULL session fallback]'	Selected	Editable
Security Options-[Network security: LAN Manager authentication level]	Selected	Fixed
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Selected	Editable
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Selected	Editable
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Selected	Editable
Security Options-[User Account Control: Admin Approval Mode for the Built-in Administrator account]	Selected	Editable
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Credential Validation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security Group Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit User Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Process Creation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit RPC Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Account Lockout]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logoff]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Logon/Logoff Events]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-1 File Server: Standard Model - Standalone Management/Linked Domain Management (Table continued)

Setting item	Default check box state	Modification
Advanced Audit Policy Configuration-[Audit Special Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Application Generated]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Removable Storage]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other System Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security State Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security System Extension]	Selected	Editable
Advanced Audit Policy Configuration-[Audit System Integrity]	Selected	Editable
Personalization-[Prevent enabling lock screen camera]	Selected	Editable
Personalization-[Prevent enabling lock screen slide show]	Selected	Editable
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services]	Selected	Editable
Group Policy-[Configure registry policy processing]	Selected	Editable
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Selected	Editable
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Selected	Editable
Internet Communication settings-[Turn off printing over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Search Companion content file updates]	Selected	Editable
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Selected	Editable
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Selected	Fixed
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Selected	Fixed
Logon-[Do not display network selection UI]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-1 File Server: Standard Model - Standalone Management/Linked Domain Management (Table continued)

Setting item	Default check box state	Modification
Logon-[Do not enumerate connected users on domain-joined computers]	Selected	Editable
Disable 'Logon-[Enumerate local users on domain-joined computers]'	Selected	Editable
Logon-[Turn off app notifications on the lock screen]	Selected	Editable
Mitigation Options-[Untrusted Font Blocking]	Selected	Editable
User Profiles-[Turn off the advertising ID]	Selected	Editable
App Privacy-[Let Windows apps access account information]	Selected	Editable
App Privacy-[Let Windows apps access call history]	Selected	Editable
App Privacy-[Let Windows apps access contacts]	Selected	Editable
App Privacy-[Let Windows apps access email]	Selected	Editable
App Privacy-[Let Windows apps access location]	Selected	Editable
App Privacy-[Let Windows apps access messaging]	Selected	Editable
App Privacy-[Let Windows apps access motion]	Selected	Editable
App Privacy-[Let Windows apps access the calendar]	Selected	Editable
App Privacy-[Let Windows apps access the camera]	Selected	Editable
App Privacy-[Let Windows apps access the microphone]	Selected	Editable
App Privacy-[Let Windows apps access trusted devices]	Selected	Editable
App Privacy-[Let Windows apps control radios]	Selected	Editable
App Privacy-[Let Windows apps sync with devices]	Selected	Editable
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Selected	Editable
AutoPlay Policies-[Turn off Autoplay]	Selected	Editable
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Selected	Editable
Cloud Content-[Do not show Windows Tips]	Selected	Editable
Cloud Content-[Turn off Microsoft consumer experiences]	Selected	Editable
Data Collection and Preview Builds-[Allow Telemetry]	Selected	Editable
Data Collection and Preview Builds-[Disable pre-release features or settings]	Selected	Editable
Data Collection and Preview Builds-[Do not show feedback notifications]	Selected	Editable
Data Collection and Preview Builds-[Toggle user control over Insider builds]	Selected	Editable
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(System)-[Specify the maximum log file size (KB)]	Selected	Editable
File Explorer-[Turn off heap termination on corruption]	Selected	Editable
HomeGroup-[Prevent the computer from joining a homegroup]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-1 File Server: Standard Model - Standalone Management/Linked Domain Management (Table continued)

Setting item	Default check box state	Modification
OneDrive-[Prevent the usage of OneDrive for file storage]	Selected	Editable
OneDrive-[Save documents to OneDrive by default] (Save documents to the local PC by default)	Selected	Editable
Remote Desktop Connection Client-[Do not allow passwords to be saved]	Selected	Editable
Device and Resource Redirection-[Do not allow drive redirection]	Selected	Editable
Security-[Require secure RPC communication]	Selected	Editable
Security-[Require user authentication for remote connections by using Network Level Authentication]	Selected	Editable
Disable 'Search-[Allow Cortana]'	Selected	Editable
Software Protection Platform-[Turn off KMS Client Online AVS Validation]	Selected	Editable
Sync your settings-[Do not sync Apps]	Selected	Editable
Sync your settings-[Do not sync start settings]	Selected	Editable
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Selected	Fixed
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Selected	Editable
Notifications-[Turn off toast notifications on the lock screen]	Selected	Editable

SEE ALSO For more information about creation of users/groups, refer to:

"■ Combination of User Management and Security Model for Windows" on page 2-17

■ Security Setting Items for File Server: Standard Model with Domain or Combination Management

The following table shows the security setting items for the combination of Standard model and Domain or Combination management on a file server.

Table Appendix 1.1.2-2 File Server: Standard Model - Domain/Combination Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Disable 'Personal Firewall-[Allow unicast response]'	Selected	Editable
Disabling NetBIOS over TCP/IP	Selected	Editable
Applying the StorageDevicePolicies function	Clear	Editable
Disabling USB storage devices	Clear	Editable
User Rights Assignment-[Deny log on locally]	Selected	Fixed

Continues on the next page

Table Appendix 1.1.2-2 File Server: Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Selected	Editable
Security Options-[Devices: Prevent users from installing printer drivers]	Selected	Editable
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Selected	Editable
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Selected	Editable
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Selected	Editable
Security Options-[Interactive logon: Do not display last user name]	Selected	Editable
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]'	Selected	Editable
Security Options-[Interactive logon: Prompt user to change password before expiration]	Selected	Editable
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Selected	Editable
Security Options-[Microsoft network server: Server SPN target name validation level]	Selected	Editable
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Selected	Editable
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Selected	Editable
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Selected	Editable
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Selected	Editable
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Selected	Editable
Disable 'Security Options-[Network security: Allow LocalSystem NULL session fallback]'	Selected	Editable
Security Options-[Network security: LAN Manager authentication level]	Selected	Fixed
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Selected	Editable
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Selected	Editable
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-2 File Server: Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Security Options-[User Account Control: Admin Approval Mode for the Built-in Administrator account]	Selected	Editable
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Credential Validation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security Group Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit User Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Process Creation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit RPC Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Account Lockout]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logoff]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Logon/Logoff Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Special Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Application Generated]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Removable Storage]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other System Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security State Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security System Extension]	Selected	Editable
Advanced Audit Policy Configuration-[Audit System Integrity]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-2 File Server: Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Personalization-[Prevent enabling lock screen camera]	Selected	Editable
Personalization-[Prevent enabling lock screen slide show]	Selected	Editable
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services]	Selected	Editable
Group Policy-[Configure registry policy processing]	Selected	Editable
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Selected	Editable
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Selected	Editable
Internet Communication settings-[Turn off printing over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Search Companion content file updates]	Selected	Editable
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Selected	Editable
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Selected	Fixed
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Selected	Fixed
Logon-[Do not display network selection UI]	Selected	Editable
Logon-[Do not enumerate connected users on domain-joined computers]	Selected	Editable
Disable 'Logon-[Enumerate local users on domain-joined computers]'	Selected	Editable
Logon-[Turn off app notifications on the lock screen]	Selected	Editable
Mitigation Options-[Untrusted Font Blocking]	Selected	Editable
User Profiles-[Turn off the advertising ID]	Selected	Editable
App Privacy-[Let Windows apps access account information]	Selected	Editable
App Privacy-[Let Windows apps access call history]	Selected	Editable
App Privacy-[Let Windows apps access contacts]	Selected	Editable
App Privacy-[Let Windows apps access email]	Selected	Editable
App Privacy-[Let Windows apps access location]	Selected	Editable
App Privacy-[Let Windows apps access messaging]	Selected	Editable
App Privacy-[Let Windows apps access motion]	Selected	Editable
App Privacy-[Let Windows apps access the calendar]	Selected	Editable
App Privacy-[Let Windows apps access the camera]	Selected	Editable
App Privacy-[Let Windows apps access the microphone]	Selected	Editable
App Privacy-[Let Windows apps access trusted devices]	Selected	Editable
App Privacy-[Let Windows apps control radios]	Selected	Editable
App Privacy-[Let Windows apps sync with devices]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-2 File Server: Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Selected	Editable
AutoPlay Policies-[Turn off Autoplay]	Selected	Editable
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Selected	Editable
Cloud Content-[Do not show Windows Tips]	Selected	Editable
Cloud Content-[Turn off Microsoft consumer experiences]	Selected	Editable
Data Collection and Preview Builds-[Allow Telemetry]	Selected	Editable
Data Collection and Preview Builds-[Disable pre-release features or settings]	Selected	Editable
Data Collection and Preview Builds-[Do not show feedback notifications]	Selected	Editable
Data Collection and Preview Builds-[Toggle user control over Insider builds]	Selected	Editable
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(System)-[Specify the maximum log file size (KB)]	Selected	Editable
File Explorer-[Turn off heap termination on corruption]	Selected	Editable
HomeGroup-[Prevent the computer from joining a homegroup]	Selected	Editable
OneDrive-[Prevent the usage of OneDrive for file storage]	Selected	Editable
OneDrive-[Save documents to OneDrive by default] (Save documents to the local PC by default)	Selected	Editable
Remote Desktop Connection Client-[Do not allow passwords to be saved]	Selected	Editable
Device and Resource Redirection-[Do not allow drive redirection]	Selected	Editable
Security-[Require secure RPC communication]	Selected	Editable
Security-[Require user authentication for remote connections by using Network Level Authentication]	Selected	Editable
Disable ‘Search-[Allow Cortana]’	Selected	Editable
Software Protection Platform-[Turn off KMS Client Online AVS Validation]	Selected	Editable
Sync your settings-[Do not sync Apps]	Selected	Editable
Sync your settings-[Do not sync start settings]	Selected	Editable
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Selected	Fixed
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Selected	Editable
Notifications-[Turn off toast notifications on the lock screen]	Selected	Editable

SEE ALSO For more information about creation of users/groups, refer to:

“■ Combination of User Management and Security Model for Windows” on page 2-17

Security Setting Items for Domain Controller: Standard Model with Standalone Management

The following table shows the security setting items for the Standard model on a domain controller.

Table Appendix 1.1.2-3 Domain Controller: Standard Model

Setting item	Default check box state	Modification
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Editable
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Disable 'Personal Firewall-[Allow unicast response]'	Selected	Editable
Disabling NetBIOS over TCP/IP	Selected	Editable
Applying the StorageDevicePolicies function	Clear	Editable
Disabling USB storage devices	Clear	Editable
User Rights Assignment-[Access this computer from the network]	Selected	Editable
User Rights Assignment-[Add workstations to domain]	Selected	Editable
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Selected	Editable
Security Options-[Devices: Prevent users from installing printer drivers]	Selected	Editable
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Selected	Editable
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Selected	Editable
Disable 'Security Options-[Domain controller: Allow server operators to schedule tasks]'	Selected	Editable
Disable 'Security Options-[Domain controller: Refuse machine account password changes]'	Selected	Editable
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Selected	Editable
Security Options-[Interactive logon: Do not display last user name]	Selected	Editable
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]'	Selected	Editable
Security Options-[Interactive logon: Prompt user to change password before expiration]	Selected	Editable
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Selected	Editable
Security Options-[Microsoft network server: Server SPN target name validation level]	Selected	Editable
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Selected	Editable
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-3 Domain Controller: Standard Model (Table continued)

Setting item	Default check box state	Modification
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Selected	Editable
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Selected	Editable
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Selected	Editable
Disable 'Security Options-[Network security: Allow Local System NULL session fallback]'	Selected	Editable
Security Options-[Network security: Force logoff when logon hours expire]	Selected	Editable
Security Options-[Network security: LAN Manager authentication level]	Selected	Fixed
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Selected	Editable
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Selected	Editable
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Selected	Editable
Security Options-[User Account Control: Admin Approval Mode for the Built-in Administrator account]	Selected	Editable
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Credential Validation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security Group Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit User Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Process Creation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit RPC Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Directory Service Access]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Directory Service Changes]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Account Lockout]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logoff]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logon]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-3 Domain Controller: Standard Model (Table continued)

Setting item	Default check box state	Modification
Advanced Audit Policy Configuration-[Audit Other Logon/ Logoff Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Special Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Application Generated]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Removable Storage]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Selected	Editable
Advanced Audit Policy Configuration-[Audit IPsec Driver]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other System Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security State Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security System Extension]	Selected	Editable
Advanced Audit Policy Configuration-[Audit System Integrity]	Selected	Editable
Personalization-[Prevent enabling lock screen camera]	Selected	Editable
Personalization-[Prevent enabling lock screen slide show]	Selected	Editable
Logon-[Do not display network selection UI]	Selected	Editable
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Selected	Editable
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(System)-[Specify the maximum log file size (KB)]	Selected	Editable
File Explorer-[Turn off heap termination on corruption]	Selected	Editable
Security-[Require secure RPC communication]	Selected	Editable
Store-[Turn off Automatic Download and Install of updates]	Selected	Editable
Store-[Turn off Automatic Download of updates on Win8 machines]	Selected	Editable
Store-[Turn off the offer to update to the latest version of Windows]	Selected	Editable
Store-[Turn off the Store application]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-3 Domain Controller: Standard Model (Table continued)

Setting item	Default check box state	Modification
Sync your settings-[Do not sync Apps]	Selected	Editable
Sync your settings-[Do not sync start settings]	Selected	Editable
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Selected	Editable
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Selected	Editable

SEE ALSO For more information about creation of users/groups, refer to:

"■ Combination of User Management and Security Model for Windows" on page 2-17

Appendix 1.2 IT Security Version 1.0

This section describes the security setting items that are configured with IT security version 1.0, their default values, and whether they can be modified.

Appendix 1.2.1 Setting Items for a Computer with ProSafe-RS Software Installed

This section describes the security setting items for a computer with ProSafe-RS software installed for each combination of security model and user management type. However, some security setting items may not appear depending on the OS version.

Security Setting Items for Legacy Model

The following table shows the security setting items for the Legacy model.

Table Appendix 1.2.1-1 Legacy Model

Setting item	Default check box state	Modification	Remarks
Access control for files and folders	Selected	Fixed	Adds full control access permissions to the Everyone group. For some tools' folders under the Windows folder, reverts to the access permissions of parent folders.
Access control for product registry	Selected	Fixed	Adds full control access permissions to the Everyone group.
Access control for DCOM (OPC) objects	Selected	Fixed	Adds full control access permissions to the Everyone group.
Personal firewall tuning	Selected	Fixed	Disables the personal firewall. In Windows 10 Enterprise LTSC 2019 and Windows 10 Enterprise LTSC 2021, Windows Defender Firewall is disabled by Local Group Policy.
Local security	Selected	Fixed	Grants access permissions to the Everyone group.
Changing IT environment settings - Hiding the last logon user name	Selected	Editable	None
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable	None

SEE ALSO For more information about creation of users/groups, refer to:

"■ Combination of User Management and Security Model for Windows" on page 2-17

Security Setting Items for Standard Model with Standalone Management/Linked Domain Management

The following table shows the security setting items for the combination of Standard model and Standalone management or Linked domain management.

Table Appendix 1.2.1-2 Standard Model - Standalone Management/Linked Domain Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Access control for product registry	Selected	Fixed
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed

Continues on the next page

Table Appendix 1.2.1-2 Standard Model - Standalone Management/Linked Domain Management (Table continued)

Setting item	Default check box state	Modification
Local security	Selected	Fixed
Changing IT environment settings - Changing the LAN Manager authentication level	Selected	Editable
Changing IT environment settings - Hiding the last logon user name	Selected	Editable
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable
Changing IT environment settings - Disabling NetBIOS over TCP/IP	When the domain is linked: Selected When the domain is not linked: Clear	Editable
Changing IT environment settings - Applying the StorageDevicePolicies function	Clear	Editable
Changing IT environment settings - Disabling USB storage devices	Clear	Editable
Changing IT environment settings - Applying software restriction policies	Clear	Editable

Security Setting Items for Standard Model with Domain or Combination Management

The following table shows the security setting items for the combination of Standard model and Domain or Combination management.

Table Appendix 1.2.1-3 Standard Model - Domain/Combination Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Access control for product registry	Selected	Fixed
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Local security	Selected	Fixed
Changing IT environment settings - Changing the LAN Manager authentication level	Selected	Editable
Changing IT environment settings - Hiding the last logon user name	Selected	Editable
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable
Changing IT environment settings - Disabling NetBIOS over TCP/IP	Selected	Editable
Changing IT environment settings - Applying the StorageDevicePolicies function	Clear	Editable
Changing IT environment settings - Disabling USB storage devices	Clear	Editable
Changing IT environment settings - Applying software restriction policies	Clear	Editable

Appendix 1.2.2 Setting Items for a File Server or Domain Controller

This section provides lists of the security setting items for a file server or a domain controller for each combination of security model and user management type.

Security Setting Items for File Server: Legacy Model

The following table shows the security setting items for the Legacy model on a file server.

Table Appendix 1.2.2-1 File Server: Legacy Model

Setting item	Default check box state	Modification	Remarks
Creating local users and groups	Selected	Fixed	Creates the CTM_PROCESS user.
Access control for files and folders	Selected	Fixed	For the Windows folder, reverts to the access permissions of parent folders. For the Project folder, adds full control access permissions to the Everyone group.
Personal firewall tuning	Selected	Fixed	Disables the personal firewall.
Local security	Selected	Fixed	Grants access permissions to the Everyone group.

Security Setting Items for File Server: Standard Model with Standalone Management/Linked Domain Management

The following table shows the security setting items for the combination of Standard model and Standalone management or Linked domain management on a file server.

Table Appendix 1.2.2-2 File Server: Standard Model - Standalone Management/Linked Domain Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Local security	Selected	Fixed
Changing IT environment settings - Applying the audit policy	Selected	Editable
Changing IT environment settings - Changing the LAN Manager authentication level	Selected	Editable
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable
Changing IT environment settings - Disabling NetBIOS over TCP/IP	When the domain is linked: Selected When the domain is not linked: Clear	Editable
Changing IT environment settings - Applying the StorageDevicePolicies function	Clear	Editable
Changing IT environment settings - Disabling USB storage devices	Clear	Editable

Security Setting Items for File Server: Standard Model with Domain or Combination Management

The following table shows the security setting items for the combination of Standard model and Domain or Combination management on a file server.

Table Appendix 1.2.2-3 File Server: Standard Model - Domain/Combination Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Local security	Selected	Fixed
Changing IT environment settings - Applying the audit policy	Selected	Editable
Changing IT environment settings - Changing the LAN Manager authentication level	Selected	Editable
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable
Changing IT environment settings - Disabling NetBIOS over TCP/IP	Selected	Editable
Changing IT environment settings - Applying the StorageDevicePolicies function	Clear	Editable
Changing IT environment settings - Disabling USB storage devices	Clear	Editable

Security Setting Items for Domain Controller: Standard Model with Domain or Combination Management

The following table shows the security setting items for the combination of Standard model and Domain or Combination management on a domain controller.

Table Appendix 1.2.2-4 Domain Controller: Standard Model - Domain or Combination Management

Setting item	Default check box state	Modification
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Editable
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Changing IT environment settings - Applying the audit policy	Selected	Editable
Changing IT environment settings - Changing the LAN Manager authentication level	Selected	Editable
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable
Changing IT environment settings - Disabling NetBIOS over TCP/IP	Selected	Editable

Continues on the next page

Table Appendix 1.2.2-4 Domain Controller: Standard Model - Domain or Combination Management (Table continued)

Setting item	Default check box state	Modification
Changing IT environment settings - Applying the StorageDevicePolicies function	Clear	Editable
Changing IT environment settings - Disabling USB storage devices	Clear	Editable

TIP

The IT Security Tool creates only the users and groups that are to be created on the domain.

Revision information

Title : ProSafe-RS Security Guide

Manual No. : IM 32P01C70-01EN

Dec. 2023/10th Edition/R4.10 or later

2.1	Added or updated descriptions in Security Models and Security Measures.
3.3	Added descriptions of supported OS, and deleted descriptions of unsupported OS.
3.5.7, 3.5.8, 3.5.9, 3.6.3, Appendix 1.2.1	Added descriptions of supported OS.
3.6.5	Updated descriptions in App Privacy (Windows Component) and Data Collection and Preview Builds (Windows Component).
Appendix 1.1.1, Appendix 1.1.2	Deleted footnote.

Nov. 2022/9th Edition/R4.08

3.3, 3.5.7	Added descriptions about Windows Server IoT 2019.

Jan. 2022/8th Edition/R4.07

1.2	Added descriptions to Security Measures and Handled Security Threats.
2.1	Added or updated descriptions in Security Models and Security Measures.
2.2.3	Added descriptions in “Combination of User Management and Security Model for Windows” and “The users for using iDefine in a virtualization environment.”
3.3, 3.5.1, 3.5.7	Added descriptions about Windows Server 2019.
3.5.5	Added descriptions in cautions and added descriptions about steps for restoring access to the required devices.
3.5.10	Added descriptions about enabling SMB signing.
3.5.11	Added descriptions about preventing illegal dll from loading.
3.6.3	Added description to cautionary notes.
3.6.5	Added cautionary notes in “Data Collection and Preview Builds (Windows Component).”
5.3	Added descriptions about the procedure of product disposal and descriptions about ports used by SCS Vnet/IP.
6.4.1, 6.4.2	Added descriptions about migrating the standard model (combination/domain management) computer to other domain.
6.10	Added a TIP.
Appendix 1.1.1, Appendix 1.1.2	Added footnotes.

Feb. 2021/7th Edition/R4.06

1	Added a new section “Overview of ProSafe-RS.”
1.2	Added descriptions to Security Measures and Handled Security Threats.
2.1	Added descriptions to Security Models and Security Measures.
2.2, 4.1, 6.1, 6.3 to 6.6, 6.8, Appendix 1, 2	Added descriptions of linked domain management.

3.1, 3.3, 3.5, 3.6.3, 6.10, 6.11.7	Deleted the descriptions of OS that is not supported.
3.1.1, 6, 6.2, 6.9	Added descriptions of Domain Link Management Tool.
3.3	Added descriptions of Windows 10 Enterprise 2019 LTSC
3.5.7	Added descriptions of Windows Update Delivery Optimization
3.5.8	Added descriptions of Disabling Windows Defender.
3.5.9	Added description of Disabling Shared experiences.

Dec. 2019/6th Edition/R4.05

Introduction	Updated descriptions of registered trademarks and trademarks.
3.1.1, 3.1.2	Added description of the Forced I/O Viewer function.
5.3	Updated descriptions for when behavior suspected to be resulting from vulnerability is found.

Aug. 2018/5th Edition/R4.04

Introduction	Updated descriptions of Yokogawa Electric registered trademark.
2.1	Updated the table of security models and security measures.
2.2.3, 3.1.1, 3.1.2, 3.1.5, 3.2	Added descriptions of Vnet/IP interface package.
2.2.3, 3.1.5, 3.2	Added descriptions of TIS_SERVICE and Dongle Gateway.
3.1.1, 3.3, 3.5.1, 3.5.2	Added descriptions of Windows Server 2016 to OS.
3.6.4	Added descriptions for the case of a Domain Controller or File Server.
4.1	Updated descriptions of .NET Framework.
6.1	Added descriptions when different IT security settings are applied.
6.5.1, 6.6.1	Updated descriptions of update procedure.
6.9.5	Added descriptions of CreateVNTUser.
6.9.6	Added descriptions of CreateTISService.
Appendix 1	Updated the table of security setting items.

Oct. 2017/4th Edition/R4.03.10

2.2.3	Added an automatically created user.
3.1	Added some target folders.
	Added some access permission information.
3.2	Added a Personal Firewall exception setting.
6.9	Added a new section “■ CreateAdsAgent.”

May 2017/3rd Edition/R4.03

Introduction	Deleted Windows Vista from the description of trademarks.
1.2, chapter 3	Updated to introduce IT security versions for stronger system security.
2.1	Reorganized and updated to introduce IT security versions for stronger system security.
6.2 to 6.4	Added descriptions of operation to configure IT security settings.
Appendix	Newly added.

Oct. 2016/2nd Edition/R4.02

Entire manual	Changed symbols.
Introduction	Updated descriptions in "■ Safety, Protection, and Modification of the Product," "■ Symbols," and "■ Trademark Acknowledgments." Added descriptions in "■ Full Names and Simplified Terms."
3.2	Deleted ETCP.exe and Scs-Simulator. Added iDefine related descriptions.
6.1	Added iDefine related descriptions.

Dec. 2015/Newly published/R4.01

Newly published

■ For Questions and More Information Online Query: A query form is available on the following URL for online query. http://www.yokogawa.com/iss
■ Written by Yokogawa Electric Corporation
■ Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Attachment 9.7 Safety Manual

IM32P01S10-01EN

User's Manual

ProSafe-RS
ProSafe-RS Lite

Safety Manual

IM 32P01S10-01EN

YOKOGAWA
Yokogawa Electric Corporation

IM 32P01S10-01EN
9th Edition

Introduction

This document presents the safety requirements for building a safety system with ProSafe-RS and ProSafe-RS Lite.

IMPORTANT

The information in this manual applies to both ProSafe-RS and ProSafe-RS Lite. Unless otherwise noted, the descriptions for ProSafe-RS include descriptions of both ProSafe-RS and ProSafe-RS Lite. The differences between ProSafe-RS and ProSafe-RS Lite are described separately for each product.

By following the requirements described in this manual, safety applications that meet the requirements up to SIL 3 of the IEC 61508 standard can be realized by ProSafe-RS, and by ProSafe-RS Lite, those of up to SIL 2 can be realized.

The ProSafe-RS and ProSafe-RS Lite have been certified by TÜV Rheinland Industrial Services GmbH, Business Sector ASI (http://tuvasi.com/), TÜV Rheinland Group to fulfill the requirements of IEC 61508. The contents of this safety manual have also been approved by TÜV.

For the proper use of ProSafe-RS, also refer to the user's manuals available on our Website (http://www.yokogawa.com)

This document consists of the following chapters.

- 1. Safety Lifecycle
  This chapter explains an overview of the safety conditions for building a safety instrumented system.
- 2. System Considerations
  This chapter explains details of the safety considerations for building a safety instrumented system with the ProSafe-RS.

9th Edition : Jun. 2023 (YK)
All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Safety Precautions for Use

Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Be sure to confirm the specifications and required settings of the devices that are used in combination with the Product by referring to the instruction manual or other documents of the devices.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:



Indicates that caution is required. This symbol for the Product indicates the possibility of dangers such as electric shock on personnel and equipment, and also indicates that the user must refer to the User's Manuals for necessary actions. In the User's Manuals, this symbol is used together with a word "CAUTION" or "WARNING" at the locations where precautions for avoiding dangers are described.

<French> Signale qu'il faut faire preuve de prudence. Ce symbole pour le produit signale la possibilité d'un danger pour le personnel et l'équipement comme un choc électrique, et signale également que l'utilisateur doit se référer au Manuel de l'utilisateur afin de prendre les mesures nécessaires. Dans le Manuel de l'utilisateur, ce symbole est utilisé conjointement avec la mention «CAUTION» ou «WARNING» aux endroits où sont décrites les précautions pour éviter les dangers.



Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.

<French> Signale qu'il faut faire preuve de prudence avec la surface brûlante. Les appareils sur lesquels est apposé ce symbole risquent de devenir brûlants. Tout contact physique ou matériel avec ces appareils risque de provoquer des brûlures ou des dommages.



Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.



Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.

Indicates an AC supply.

Indicates a DC supply.

| Indicates that a component such as a power supply switch is turned ON.

○ Indicates that a component such as a power supply switch is turned OFF.

Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

Warning and Disclaimer

- In realization of the Safety Instrumented System (SIS), an appropriate competence management system is required to conform to the Functional Safety Management (FSM) defined in IEC 61508 and IEC 61511. Hence, YOKOGAWA cannot assure conformance of ProSafe-RS and other related YOKOGAWA products (“Products”) unless YOKOGAWA or YOKOGAWA’s authorized partners are fully involved in or control engineering, configuration, adaptation, maintenance, repair and other work in SIS lifecycle.
- In no event shall YOKOGAWA be liable for any result, claim, loss or damage whatsoever arising out of or in connection with use or inability to use of Products, if any part of engineering, configuration, adaptation, maintenance, repair, improvement, addition of functions, adjustment or other modification work for the Products is made or controlled by a person other than YOKOGAWA or YOKOGAWA’s authorized partners.
- Except for the limited warranties agreed upon in writing, YOKOGAWA disclaims all other warranties, express or implied, in fact or in law, including without limitation, warranties of merchantability, fitness for a particular purpose and non-infringement. If warranty is provided, repair or replacement of the Products is the exclusive remedy for breach of warranty.
- In no event shall YOKOGAWA be liable for any indirect or consequential loss or damage incurred arising out of or in relation to use or inability to use the Products regardless of whether foreseeable or not, whether arising in or for breach of contract, tort (including negligence), breach of statutory duty or otherwise or whether YOKOGAWA has been advised of the possibility thereof.

Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the Software Product's merchantability or suitability for any particular purpose, except as specified in the warranty terms.
- Purchase the appropriate number of licenses of the Software Product according to the number of computers to be used.
- No copy of the Software Product may be made for any purpose other than backup; otherwise, it is deemed as an infringement of YOKOGAWA's Intellectual Property rights.
- Keep the software medium of the Software Product in a safe place.

- No reverse engineering, reverse compiling, reverse assembling, or converting the Software Product to human-readable format may be performed for the Software Product.
- No part of the Software Product may be transferred, converted, or sublet for use by any third-party, without prior written consent from YOKOGAWA.

Documentation Conventions

Symbols

The following symbols are used in the User's Manuals.

 WARNING	Indicates precautions to avoid a danger that may lead to death or severe injury.
 CAUTION	Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.
IMPORTANT	Indicates important information required to understand operations or functions.
TIP	Indicates additional information.
SEE ALSO	Indicates referenced content. In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

Typographical Conventions

The following typographical conventions are used throughout the User's Manuals.

Commonly Used Conventions throughout the User's Manuals

- Δ Mark
  Indicates that a space must be entered between character strings.
  Example:

  ```
  .ALΔPIC010Δ-SC
  ```

- Character string enclosed by braces { }
  Indicates character strings that may be omitted.

  Example:

  ```
  .PRΔTAG{Δ.sheet name}
  ```

Conventions Used to Show Key or Button Operations

- Characters enclosed by brackets [ ]
  When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a button name in a window, or an item in a list box displayed in a window.

  Example:

  To alter the function, press the [ESC] key.

Conventions of a User-defined Folder

- User-defined folder name enclosed by parenthesis ( )
  User definable path is written in a pair of parentheses.

  Example:

  ```
  (RS Project Folder)\SCS0101
  ```

If the RS Project Folder is `C:\MYRSPJT`, the above path becomes `C:\MYRSPJTSCS0101`.

Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.
If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

Definitions of Node and Module Terms

In the User's Manuals, nodes and modules are referred to by using collective terms, another terms, or abbreviations based on the following definitions:

- Definitions of nodes
  - Node: A node is a collective term for an FIO node and an N-IO node.
  - FIO node: This is a collective term for a safety control unit, a safety node unit, and a unit for optical ESB bus repeater module.
  - CPU node: This is another term for a safety control unit. The abbreviation of safety control unit is SCU.
  - I/O node: This is another term for a safety node unit. The abbreviation of safety node unit is SNU.
  - N-IO node: This is a collective term for a node interface unit and an N-IO I/O unit. The abbreviation of node interface unit is NIU.
- Definitions of modules
  - I/O module: This is a collective term for an FIO I/O module and an N-IO I/O module.
  - FIO I/O module: This is a collective term for an analog I/O module and a digital I/O module for FIO, and a communication module.
  - N-IO I/O module: This is a collective term for the modules that can be mounted on an N-IO I/O unit.
  - AIO/DIO module: This is a collective term for an analog I/O module, a digital I/O module, and a universal type I/O module.
  - Analog I/O module: This is a collective term for an analog input module and an analog output module.
  - Digital I/O module: This is a collective term for a digital input module and a digital output module.
  - Universal type I/O module: This is a collective term for the I/O modules for which the channel signal category can be changed by software.

- Input module: This is a collective term for an analog input module, digital input module, and a universal type I/O module with defined input channels.
- Output module: This is a collective term for an analog output module, digital output module, and a universal type I/O module with defined output channels.
- Communication module: This is a collective term for a serial communication module, an Ethernet communication module, and a fire and gas communication module.

Full Names and Simplified Terms

In the User's Manuals, simplified terms listed in the following table are used.

Table Info-1 Full Names and Simplified Terms

Full Name	Simplified Term
Automation Design Suite	AD Suite
Automation Design Organizer	AD Organizer
Automation Design Server	AD Server
Automation Design project	AD project
Automation Design Master Database	ADMDB
Automation Design Suite Administration Tool	ADS Administration Tool
iDefine for ProSafe-RS	iDefine
Modification Package	ModPack
SCSV1-S (SCS supporting the SSC10S/SSC10D safety control units)	SCSV1
SCSP1-S (SCS supporting the SSC50S/SSC50D safety control units)	SCSP1
SCSP2-S (SCS supporting the SSC60S/SSC60D safety control units)	SCSP2
SCSP3-S (SCS supporting the S2SC70S/S2SC70D safety control units)	SCSP3
SCSL2-S (SCS supporting the L1SC70S/L1SC70D safety control units)	SCSL2
SCSU1-S (SCS supporting the SSC57S/SSC57D safety control units)	SCSU1

Copyright and Trademark Notices

All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, PRM, Exaopc, FieldMate Validator, and STARDOM are registered trademarks or trademarks of Yokogawa Electric Corporation.
- The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

Safety Manual

IM 32P01S10-01EN 9th Edition

CONTENTS

1. Safety lifecycle....1-1
2. System considerations....2-1
2.1 Overview of ProSafe-RS....2-2
2.2 Hardware configuration....2-3
2.3 Application development....2-8
2.4 Security....2-12
2.5 Online change....2-13
2.6 Forcing....2-14
2.7 Maintenance override....2-15
2.8 Replacement of modules in SCS....2-16

Safety Manual

IM 32P01S10-01EN 9th Edition

CONTENTS

Appendix

Appendix 1. Product support..... App.1-1

1. Safety lifecycle

The IEC 61508 requires the use of its safety lifecycle for configuring and maintaining safety systems properly. This chapter explains the overview of the safety lifecycle.

The following table lists the abbreviations used in this safety manual.

Table 1-1 Abbreviations

Abbreviation/ generic term	Definition	Remarks
AI	Analog Input	
AO	Analog Output	
CENTUM	CENTUM VP, the Integrated Production Control System of Yokogawa.	
CPU	Central Processing Unit	
DI	Digital Input	
DO	Digital Output	
ENG	Engineering Personal Computer	Device of CENTUM
FB	Function Block	Element used in FBD/LD/ST
FBD	Function Block Diagram	IEC 61131-3 language
FCS	Field Control Station	Device of CENTUM
FU	Function	Element used in FBD/LD/ST
HIS	Human Interface Station	Device of CENTUM
I/O	Input/Output	
LD	Ladder Diagram	IEC 61131-3 language
PFD	Probability of Failure on Demand	Defined by IEC 61508
SC	Systematic Capability	Defined by IEC 61508
SCS	Safety Control Station	Device of ProSafe-RS system
SENG	Safety Engineering Personal Computer	Device of ProSafe-RS system
SIL	Safety Integrity Level	Defined by IEC 61508
ST	Structured Text	IEC 61131-3 language

Overview of the safety lifecycle

The safety lifecycle, which consists of sixteen phases that start at the concept phase of a system and end at the systems usage expiration, defines necessary activities for these phases. As the safety lifecycle is considered as a framework to minimize the systematic failure caused by human errors, persons involved in the implementation of the safety functions need to understand the requirements of the safety lifecycle well and follow them.

As part of the safety lifecycle, the three planning phases for operation and maintenance, safety validation, and installation and commissioning are required prior to actual implementation phases. This is because adequate preparations that include the procedures and measures derived from the impact analysis are important to ensure functional safety and/or to prevent an unsafe state during the implementation.

The standard also requires that the functional safety management runs in parallel with the safety lifecycle phases with emphasis on the importance of the documentation. The information about all activities and the results of each phase need to be documented in such way that the descriptions are accurate and easy to understand for users. The document of one phase is used as an input of the subsequent phase of the safety lifecycle in principle. This makes it possible to maintain the consistency of the lifecycle and trace the activities afterward.

Another requirement of the functional safety management is to manage competence. The organizations and/or persons involved in the safety lifecycle must be competent for their activities that they have responsibilities for. Adequate experience and training are necessary for this purpose.

This safety manual provides information for all planning phases of the safety lifecycle to ensure the correct use of ProSafe-RS to reach the aimed safety integrity by the end user.

2. System considerations

This chapter provides details of the safety considerations for building the safety system with the ProSafe-RS.

2.1 Overview of ProSafe-RS

This section explains the overview of ProSafe-RS.

Overview of ProSafe-RS

ProSafe-RS is a safety system consisting of a safety controller, SCS, and an engineering and maintenance PC, SENG. The minimum configuration includes one SCS and one SENG.

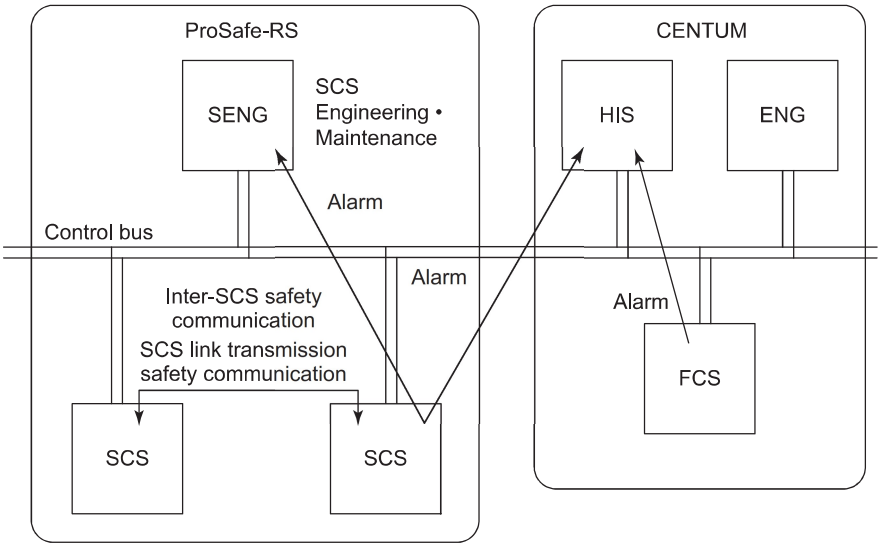


Figure 2.1-1 Example of system configuration

An SCS of ProSafe-RS in which both CPU and I/O modules are in single configuration can be used for applications that meet the IEC 61508 SIL 3 requirements. An SCS of ProSafe-RS Lite can be applied to applications that meet the IEC 61508 SIL 2 requirements in a single configuration. To increase the system availability, CPU modules and/or I/O modules can be duplexed (dual-redundant).

By using inter-SCS safety communication or SCS link transmission safety communication, ProSafe-RS can build the SIL 3 safety loop between different SCSs connected via the control bus, and ProSafe-RS Lite can build the SIL 2 safety loop between them.

You can also use ProSafe-RS SCS and ProSafe-RS Lite SCS to build the SIL 2 safety loop between different SCSs.

ProSafe-RS and ProSafe-RS Lite comply with the requirements of IEC 61508 SC3 (Systematic Capability 3).

The ProSafe-RS can be integrated seamlessly into a CENTUM VP system connected on the same control bus. This allows operators to monitor the SCSs through the HIS.

For details on how to use ProSafe-RS and ProSafe-RS Lite, refer to the ProSafe-RS User's Guide (IM 32P01B10-01EN).

Safety applications

ProSafe-RS is primarily intended to be used for the following safety applications. The use of ProSafe-RS conforming to the standards for each application is also certified by TÜV.

For the details of the requirements, refer to each standard.

- ESD (Emergency Shutdown System) / PSD (Process Shutdown System)
- F&G (Fire and Gas detection System: EN 54, NFPA 72)
- BMS (Burner Management System: EN 298, NFPA 85, NFPA 86, EN 50156)

2.2 Hardware configuration

This section explains the hardware structure.

Safety requirements and system availability

An SCS of ProSafe-RS in which both CPU and I/O modules are in single configuration can be used for applications that meet the SIL 3 requirements. An SCS of ProSafe-RS Lite can be applied to applications that meet the SIL 2 requirements in a single configuration. For the models and revisions of each module, refer to our Website (http://www.yokogawa.com/).

To increase the availability, CPU modules and/or I/O modules can be duplexed (dual-redundant). When a fault is detected in one module in a dual-redundant configuration, the other module takes over control to continue operation.

SCS hardware

SCS basic components

The basic components of the SCS hardware include the following.

- Safety control unit
  - CPU module
  - Power supply module (dual-redundant)
  - ESB BUS coupler module (dual-redundant)
  - N-ESB bus coupler module (dual-redundant)
  - Optical ESB bus repeater module (dual-redundant)
- Safety node unit
  - Power supply module (dual-redundant)
  - ESB bus interface module (dual-redundant)
  - Optical ESB bus repeater module (dual-redundant)
- Node interface unit
  - Power supply unit (dual-redundant)
  - N-ESB bus module (dual-redundant)
- N-IO I/O unit

I/O modules

The following table lists the I/O modules used for the ProSafe-RS system.

Use safety I/O modules for safety loops.

Table 2.2-1 Safety I/O module list (for safety control unit and safety node unit)

Safety I/O module
Digital Input Module (24 V DC)
Digital Output Module (24 V DC)
Digital Output Module (48 V DC)
Digital Output Module (100-120 V AC)
Analog Input Module (4-20 mA)

Continues on the next page

Table 2.2-1 Safety I/O module list (for safety control unit and safety node unit) (Table continued)

Safety I/O module
Analog Input Module (1-5 V/1-10 V)
Analog Input Module (TC/mV)
Analog Input Module (RTD)
Analog Output Module (4-20 mA)
Fire and Gas Communication Module

Table 2.2-2 Safety I/O module list (for N-IO I/O unit)

Safety I/O module
Analog Digital I/O Module (DI/DO: 24 V DC, AI/AO: 4-20 mA)
Digital I/O Module (DI/DO: 24 V DC)

Table 2.2-3 Interference-free I/O module list (for safety control unit, safety node unit)

Interference-free I/O module
Serial Communication Module (RS-232C)
Serial Communication Module (RS-422/RS-485)
Ethernet Communication Module

Environmental requirements

For details of the permissible environmental conditions for ProSafe-RS and ProSafe-RS Lite, and their connection with external devices such as I/O module, refer to the following documents:

- For ProSafe-RS: ProSafe-RS Installation Guidance (TI 32P01J10-01EN)
- For ProSafe-RS Lite: ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

Fault detection and reaction

Basic behavior

CPU modules and I/O modules are diagnosed by the hardware and software periodically. Errors in communications between the CPU module and I/O modules, communications between the CPU module and fire and gas communication modules (hereafter, referred to as fire and gas communication), and inter-SCS safety communications are detected by various measures.

When an error is detected, the failsafe value is used for the output value and a diagnostic information message is issued. The diagnostic information message, which is sent to the SENG and HIS (when integrated with CENTUM) via the control bus, is useful for identifying the details and the cause of the error.

In a dual-redundant configuration, the other module that is working normally takes over control to continue the operation.The diagnostic information message that is issued at the same time helps identify the failed module.

The user can define the fail-safe behavior of the system when faults are detected in I/O modules. The following section describes the details.

Diagnosis and reaction

This section explains the fault detection and reaction of the system in the single configuration.

In a dual-redundant configuration, the other module that is working normally takes over control to continue the operation.

- CPU module
  The major components in the CPU module are duplexed, and their operation results are always compared between the two. This enables to detect a fault in a very short time. The detection of a fault causes a shutdown of the CPU module. Accordingly, the output modules detect a communication halt of the CPU module and outputs the failsafe value predefined for each channel.
- Input module
  Diagnostic tests of input modules are performed by the firmware periodically. When one of the following faults is detected, the status of input channel changes to “bad” and a predefined value (input value for a fault) is transferred to the application logic. This means, faults in input modules, as well as demands (changes in input values), can be handled by application logic.
  - Fault in the common part of an input module
  - Fault in an input channel
  - Failure in communication between an input module and a CPU module
- Output module
  Diagnostic tests of output modules are performed by the firmware periodically. When one of the following faults is detected, the Output Shutoff Switch is activated to force all the output channels to OFF (0).
  - Fault in the common part of an output module
  - A channel is stuck-at-ON, that is, the output cannot be turned to OFF (digital output module (24 V DC, 48 V DC))
    (In the case of digital output module (100-120 V AC), only the fault-detected channel is turned to OFF(0).)
  - Output current read back error (analog output module)

  In case of a communication fault between an output module and a CPU module, the failsafe value for each channel is output.
- Analog digital I/O module (for N-IO I/O unit)
  Diagnostic tests of analog digital I/O modules are performed by the firmware periodically. The following table describes the types of faults and operations in the event of a fault.

Table 2.2-4 Analog digital I/O module operations in the event of a fault

Type of fault	Operation in the event of a fault	
	Input channel	Output channel
Fault in the common part of analog digital I/O modules	The I/O Shutoff Switch is activated to force all the analog input channels (two-wire type) and digital input channels to the input value for a fault.	The I/O Shutoff Switch is activated to force all the analog output channels to 0 mA. The DO Shutoff Switch is activated to force all the digital output channels to OFF (0).
Output current read back error in an analog output channel		
Communication fault between an analog digital I/O module and a CPU module	The status of input channel changes to “bad” and a predefined value (input value for a fault) is transferred to the application logic. This means, faults in input modules, as well as demands (changes in input values), can be handled by application logic.	The failsafe value specified for each output channel is output.
Fault in an input channel		-
Stuck-at-ON fault rendering it no longer feasible to turn the digital output channels OFF	-	The DO Shutoff Switch is activated to force all the digital output channels to OFF (0).

- Digital I/O module (for N-IO I/O unit)
  Diagnostic tests of digital I/O modules are performed by the firmware periodically. The following table describes the types of faults and operations in the event of a fault.

Table 2.2-5 Digital I/O module operations in the event of a fault

Type of fault	Operation in the event of a fault	
	Input channel	Output channel
Fault in the common part of digital I/O modules	All digital input channels are forced to the input value for a fault.	The DO Shutoff Switch is activated to force all the digital output channels to OFF (0).
Communication fault between a digital I/O module and a CPU module	The status of input channel changes to “bad” and a predefined value (input value for a fault) is transferred to the application logic. This means, faults in input modules, as well as demands (changes in input values), can be handled by application logic.	The failsafe value specified for each output channel is output.
Fault in an input channel		-
Stuck-at-ON fault rendering it no longer feasible to turn the digital output channels OFF	-	The DO Shutoff Switch is activated to force all the digital output channels to OFF (0).

- Diagnosis of Field Wiring
  A diagnostic function is provided to detect open and short circuits in wiring between field devices and I/O modules.

  The behavior after detection of such a fault is the same as the case of a fault in the channel of the I/O modules.

  To perform this diagnosis on a DI channel of a digital input module or universal type I/O module, connect a dedicated wiring check adapter with the wiring close to the field device. The wiring check adapters are available for “Normally Energized” and for “Normally De-energized” respectively.
- Fire and gas communication
  SCS is capable of PROFIsafe-compliant safety communication with fire and gas devices. When an error is detected in safety communication, the predefined value is transferred to the application logic in the SCS.
- Inter-SCS Safety Communication and SCS Link Transmission Safety Communication
  The receiver side of SCS can detect failures caused by faults in the SCSs and the relay devices on the communication path.

  When a failure in inter-SCS safety communication and/or SCS link transmission safety communication is detected, the predefined value is transferred to the application logic in the receiver side of SCS. This is implemented by the dedicated FBs for inter-SCS safety communication and SCS link transmission safety communication respectively.

System timing

System reaction time of the SCS

The system reaction time of SCS includes the reaction time for the external demand and the reaction time when a fault is detected in the SCS. For details on the system reaction time of the SCS, refer to Engineering Guide Vol. 1 (IM 32P01C10-01EN).

Process safety time

The process safety time is the period from the time of fault occurrence in the process until the time process enters a dangerous state, which is determined for each process. The safety system needs to transfer the process to a safe state within the process safety time after the demand (process error).

The reaction time of the safety system, which is the total of the reaction time of the sensor, actuator, and safety controller, needs to be shorter than the process safety time. Consider the above system reaction time of the SCS as the reaction time of the safety controller.

PFD calculation

The ProSafe-RS has been designed to meet the requirements for PFD of SIL 3 that are defined as a fraction of 10^{-4} to 10^{-3} in the IEC 61508, with the condition that the interval between proof tests is ten years. As for the ProSafe-RS Lite, it is designed to meet the requirements for PFD of SIL 2 that are defined as a fraction of 10^{-3} to 10^{-2} under the same condition. For details, refer to Engineering Guide Vol. 1 (IM 32P01C10-01EN).

Check list for hardware engineering

Table 2.2-6 Check list for hardware engineering

No.	Description	Check
1	Have the products that meet the requirements for target SIL been used?	
2	Have the modules for safety and the ones for non-safety been used appropriately?	
3	Have the devices and wiring been installed according to the Installation Guidance?	
4	Has the mechanism of the fault detection and reaction been understood?	
5	To perform field wiring diagnosis on a DI channel of a digital input module or universal type I/O module, has a dedicated wiring check adapter been connected?	
6	Has the system reaction time of the SCS and the process safety time been understood?	

SEE ALSO

For more information about each No. of the check list, refer to:

"■ SCS hardware" on page 2-3

For more information about the installation and wiring, refer to:

"● Environmental requirements" on page 2-4

2.3 Application development

This section explains about the application development.

Parameter settings

To ensure normal operation of the system, you must set parameters to the appropriate values by using the engineering function.

Scan Period

A safety application runs at intervals of a defined scan period.

Determine a scan period to meet the requirements for the process safety time.

Automatic scan period extension

This function automatically extends the scan period of the application logic. This function is a temporary containment of negative effects on communication with SENG and the CENTUM integration function when the processing time for the application logic exceeds the specified scan period. Note that the extended scan period may not meet the requirements for the process safety time. This function can be used only when permanent measures are available for example the amount of application logic can be reduced when the scan period is extended. For details, refer to Engineering Guide Vol. 1 (IM 32P01C10-01EN).

Input value for a fault and failsafe value

Define the value (input value for a fault) which will be passed to the application logic when a fault is detected in an input module or universal type I/O module. Define the value (failsafe value) which will be output from a module when a CPU fault is detected or a communication fault occurs between a CPU and an output module or universal type I/O module. These can be individually defined on each channel.

These values, that determine the safety state, should be cautiously defined depending on the application. In general, for digital I/O channels, 0 is used in a De-energize to trip system and 1 in an Energize to trip system. If different values are used, the immediate repair after a failure occurs should be considered.

Activation of Output Shutoff Switch, DO Shutoff Switch, and I/O Shutoff Switch

Output modules have a shutoff switch for shutting off the outputs when a dangerous failure which disables correct output operation occurs.

Analog output modules and digital output modules have an Output Shutoff Switch. There are two types of shutoff switches for analog digital I/O modules: DO Shutoff Switch and I/O Shutoff Switch. There is only one type of shutoff switches for digital I/O modules: DO Shutoff Switch.

The Output Shutoff Switch is common to all output channels in the module and normally closed (ON). The Output Shutoff Switch can be activated to shut off all channels of the output module when a stuck-at-ON fault, which makes the channel unable to turn the output OFF (0), for a digital output module (24 V DC or 48 V DC) or an output current read back error for an analog output module is detected by self-diagnosis.

The behavior of the shutoff switch is definable per channel. Select the default value to all channels for a safety application, which activates the switch when the previously mentioned fault is detected in a channel.

The DO Shutoff Switch is common to all digital output channels in the module and normally closed (ON). The DO Shutoff Switch can be activated to shut off the digital output when a stuck-at-ON fault (which renders it no longer feasible to turn the output OFF) of a digital output channel is detected by self-diagnosis. The behavior of the shutoff switch is definable per

channel. Select the default value to all channels for a safety application, which activates the switch when the previously mentioned fault is detected in a channel.

On the other hand, the I/O Shutoff Switch is common to all analog output channels in the module and normally closed (ON). The I/O Shutoff Switch can be activated to shut off the analog output when a current read back error for an analog output channel is detected by self-diagnosis. AI and DI channels are forced to the input value for a fault. The behavior of the shutoff switch is definable per channel. Select the default value to all channels for a safety application, which activates the switch when the previously mentioned fault is detected in a channel.

When the I/O Shutoff Switch is activated, the I/O of all AI (two-wire type), AO, DI, and DO channels of the module are shutoff.

Diagnostics of field wiring

For each channel of I/O modules, specify whether to perform diagnosis of field wiring.

Timeout settings for inter-SCS safety communication and SCS link transmission safety communication

Set the proper timeout values for the inter-SCS safety communication dedicated FB and SCS link transmission safety communication parameter.

For calculation of the timeout values, refer to Engineering Guide Vol. 2 (IM 32P01C20-01EN).

Input value for a fault and timeout settings for fire and gas communication

Define the value (input value for a fault) which will be passed to the application logic when a fault is detected in the safety communication in fire and gas communication. This value can be specified for each signal in communication definitions and should be determined depending on the application.

Set the proper timeout value for safety communication (F_WD_Time) for each safety communication data that is defined.

For the policy for timeout value setting, refer to Engineering Guide Vol. 1 (IM 32P01C10-01EN).

However, in using fire and gas communication, it is necessary to establish the application logic based on the specifications for in-use fire and gas communication devices. For the details including the above-mentioned items, refer to Engineering Guide Vol. 2 (IM 32P01C20-01EN).

Behavior at abnormal calculation

SCS stops if abnormal calculation occurs during application logic execution. If “Continue operations” is specified for the behavior at abnormal calculation, SCS continues the operation without stopping at abnormal calculation. However, in this case, intended control can no longer be performed. “Continue operations” can be specified only when the application logic can be modified promptly. For details, refer to Engineering Guide Vol. 1 (IM 32P01C10-01EN).

Programming

The engineering function of the ProSafe-RS provides the programming languages conforming to the IEC 61131-3 standard. The following languages are used to program safety application.

- FBD (Function Block Diagram)
- LD (Ladder Diagram)
- ST (Structured Text)

Use proper FU/FB, LD elements, and ST statements of these languages. Some of them can be used for safety applications, but the others cannot.

For details, refer to the POU Reference Manual (IM 32P03B20-01EN).

Application test

After programming an application, you need to verify if it operates according to the specifications.

- After programming the application, save it, print it out using the Self-Documentation Function, and check that the inputs of programming and the contents of the printout match.
- Use the Integrity Analyzer to check whether the FU/FB, etc. used for programming the safety application are applicable to safety use. Confirm that the result is as intended.
- The simulator on SENG can test the application for debugging, without the need of the actual SCS.
- Testing the safety application logic can be done with the Target Test Function on the target SCS even when no I/O modules are installed in the SCS or when no field devices are connected.
- You should perform the final test on the target system with the necessary devices installed.
- When loading the application into SCS, make sure that the correct application has been loaded with the version information shown on the SENG.
- When starting the operation after completion of the test at the security level 0, perform the off-line download and change the security level to Level 2.

When a part of the application is modified, the impact of the modification needs to be analyzed before a test. Unintended result of the modification can be detected with the Cross Reference Analyzer before the test. This helps identify the part to be tested, so that only the modified part needs to be tested. The procedure is as follows:

1. After modifying the application using the engineering tool, print it out and make sure that the inputs of programming and the contents of the printout match.
2. Make sure that the check results by the Cross Reference Analyzer are as intended.
3. If necessary, check the operation of the application with the SCS simulator.
4. Validate it on the target SCS.

To modify the application correctly, the modification history of the current application needs to be managed. For this purpose, the version control function is provided.

Check list for application development

Check list for parameter settings and programming

Table 2.3-1 Check list for parameter settings and programming

No.	Description	Check
1	Has the scan period been determined to meet the requirements for the process safety time?	
2	Have the settings of the automatic scan period extension been carefully considered to be appropriate with proper awareness on the impacts of extended scan period?	
3	Have the DO Shutoff Switch, I/O Shutoff Switch, and Output Shutoff Switch been selected to be activated?	
4	Have the input values for faults and failsafe values been determined?	
5	For inter-SCS safety communication, SCS link transmission safety communication, and fire and gas communication, has the application logic been written with the dedicated FB?	

Continues on the next page

Table 2.3-1 Check list for parameter settings and programming (Table continued)

No.	Description	Check
6	For inter-SCS safety communication, SCS link transmission safety communication, and fire and gas communication, have the proper timeout values been set?	
7	Have the behavior settings at abnormal calculation been carefully considered to be appropriate with proper awareness on the impacts of abnormal calculation?	
8	Has the application logic been written with the proper language or language element?	

Check list for procedure for application test

The following check list shows the procedure after application input. When an error is found at a step, go back to a proper step, the application input step in principle.

Table 2.3-2 Check list for procedure for application test

No.	Description	Check
1	Save the application on SENG, print it out with the Self-Documentation Function, and compare the inputs with the printout.	
2	Use the Integrity Analyzer and check the results.	
3	Use the Cross Reference Analyzer and check the results.	
4	Use simulator on the SENG for debugging.	
5	Download the application into SCS.	
6	Test the application on target.	

2.4 Security

To prevent accesses from unauthorized users or devices during the operation and unintended changes due to user's operation errors, consider the security mentioned in this section.

SCS security level

The SCS controls the security levels for the safe operation of the system.

Set the security level to Level 2 during the normal operation of SCS to protect the SCS against illegal access. It needs to be set to Level 1 for maintenance, and to Level 0 for off-line operation. To prevent erroneous changes of the security level, password authorization is required.

Assign different passwords for authorization to individual security levels and SCSs. Check that the security level on the display of SENG is correct when changing the security level.

Access to SCS

Changing the security level enables SCS to be accessed. To prevent erroneous access to SCS, correct operation on SENG is needed. For this purpose, SENG is provided with the display of the system alarms and SCS status to indicate which part of SCS is to be accessed. When accessing SCS, use these functions to ensure the correct access for its safe operation.

Access control on SENG

The safety application is protected with a password, so that only authorized users are allowed to operate and modify it. The passwords for operating the safety application need to be different for each SCS.

N-ESB bus module maintenance port

Disable the maintenance port of the N-ESB bus module during the normal operation of SCS to protect the SCS against illegal access.

Check list for security

Table 2.4-1 Check list for security

No.	Description	Check
1	Is the usage of the SCS Security Levels understood?	
2	Have different passwords for changing SCS Security Levels been assigned to individual security levels and individual SCSs?	
3	Has the Security Level of the SCS in operation been set to Level 2?	
4	Performing operations on SCS, have you confirmed that the settings and the state of SCS are the same as you intended?	
5	Have different passwords for operating safety application on the SENG been assigned to individual SCSs?	
6	Has the maintenance port of the N-ESB bus module of the SCS currently operating been disabled?	

2.5 Online change

ProSafe-RS allows the application to be modified, I/O modules to be added or removed, and the I/O module settings to be changed online.

Before Online Change, analyze its impact on the system, provide external measures when necessary or appropriate, and then execute it with much caution.

Online change consideration

After modifying the application and completing the check, you need to perform Online Change Download and test the modified part. Before Online Change Download, change the SCS Security Level to Level 1, and return it to Level 2 after completion of the test.
To prevent a system error, Online Change Download must not be performed while maintenance override operation by HIS is going on.

If the modified application contains any unintended changes, Online Change can lead to unexpected system behavior. To prevent adverse influence on the parts outside of SCS caused by the unexpected behavior, use the Forcing Function, and also provide appropriate measures outside of SCS to deal with emergency situations in advance.

For the detailed procedure for Online Change, refer to Engineering Guide Vol. 1 (IM 32P01C10-01EN).

In addition, there are some considerations for using fire and gas communication, which are different from the considerations for using AIO/DIO modules. For the procedure for Online Change, refer to Engineering Guide Vol. 1 (IM 32P01C10-01EN) and Engineering Guide Vol. 2 (IM 32P01C20-01EN).

Check list for online change

Table 2.5-1 Check list for online change

No.	Description	Check
1	Has the plan of modification been reviewed and approved?	
2	Does the modification need to be done online?	
3	Has the impact of the online change on the system been analyzed and the results fully understood?	
4	Are the Integrity Analyzer and Cross Reference Analyzer used for change verification?	
5	Has the Forcing Function or Fixing All Output Function been taken into account?	
6	Have adequate measures for emergency situations been prepared outside SCS?	
7	Has the procedure for the online change been clearly established?	

2.6 Forcing

This section explains the consideration at the time of performing the Forcing Function.

Forcing function

The forcing function of the SENG is for locking and forcing the values on I/O channels, the variables used in the application logic, and the data values for inter-SCS safety communication, SCS link transmission safety communication, and fire and gas safety communication. To start the forcing function, change the SCS Security Level to Level 1.

When operating from the SENG, make sure that the correct variables are locked.

To return to the normal operation, unlock all the I/O channels, variables, and safety communication data to bring them back to the normal state, and change the SCS Security Level to Level 2.

Using the dedicated FB helps management of the forcing condition, such as the number of locked variables and forced unlocking of locked variables.

Before performing the forcing function, which is used for maintenance of devices and for Online Change, analyze the impact on the system and take adequate measures beforehand.

Check list for forcing

Table 2.6-1 Check list for forcing

No.	Description	Check
1	Has the impact of the forcing on the system been analyzed and the results fully understood?	
2	Has the use of the dedicated FB for managing the forcing condition been taken into account?	
3	Has the procedure for forcing been clearly established?	
4	Does the procedure include the instruction that, after forcing is finished, all the variables must be set back to the normal values and then unlocked?	
5	Have adequate measures for emergency situations been prepared outside SCS?	

2.7 Maintenance override

This section explains the consideration at the time of performing the maintenance override.

Maintenance override

The maintenance override, which is used for device maintenance, assigns a predefined value or state to an I/O variable.

For a maintenance override from the HIS in a CENTUM-integrated system, build the safety application logic beforehand, using the dedicated FB for maintenance overrides.

The maintenance override operation has two steps: the authorization command and the execution command of the override. After completion of maintenance, clear the maintenance override.

Perform a series of operations from the HIS by operator's confirming the contents and the message on the display.

Check list for maintenance override

Table 2.7-1 Check list for maintenance override

No.	Description	Check
1	Has the effect of the maintenance override been analyzed and the results fully understood?	
2	Has the application logic been written with the dedicated FB for the maintenance override?	
3	Has the operation manual been prepared and confirmed by the operators?	
4	Does the operation manual include the instruction that all overrides must be removed at the completion of the maintenance?	
5	Has an alternative method for removing overrides been prepared?	
6	Have adequate measures for emergency situations been prepared outside SCS?	

2.8 Replacement of modules in SCS

This section explains the consideration at the time of replacement of modules.

Replacement of modules

When a module failure occurs, identify the failed location in SCS using the LED display of modules or the diagnostic information of the SENG to replace the relevant module.

After replacing the CPU module in a single configuration, perform Master Database Offline Download and ensure the correct application has been downloaded.

In case a module failure does not lead to a shutdown in a single configuration, the replacement of the module should take place within Mean Time To Repair (MTTR).

Even in case of a failure in one module of a duplex configuration, the safety level of the applicable SIL is guaranteed. The failed module can be replaced while the SCS is in operation.

Check list for replacement of modules

Table 2.8-1 Check list for replacement of modules

No.	Description	Check
1	Has the diagnostic information of the SENG been confirmed?	
2	Is the LED display of the relevant module showing the failure?	
3	Has the module replacement procedure been understood correctly?	
4	After replacing a CPU module, has the application been confirmed correct (in the single configuration)?	
5	Has Master Database Offline Download been performed to load the correct application if necessary?	

Appendix 1. Product support

Please contact our offices listed below for the technical support of the ProSafe-RS system.

Table Appendix 1-1 Product support list

Yokogawa Electric Corporation 2-9-32 Nakacho, Musashino-Shi, Tokyo 180-8750 Japan Phone:(81)-422-52-5634 Fax: (81)-422-52-9802 E-mail: 200502prosafe_com@yg.jp.yokogawa.com
Yokogawa Europe Solutions B.V. Euroweg 2, 3825 HD Amersfoort P.O. Box 163, 3800 AD Amersfoort The Netherlands Phone: (31)-281-340-3800 Fax: (31)-281-340-3838 E-mail: Info@nl.yokogawa.com
Yokogawa Corporation of America 12530 West Airport Blvd, Sugar Land, Texas 77478 U.S.A. Phone: (1)-88-4641000 Fax: (1)-88-4641111 E-mail:prosafe@us.yokogawa.com
Yokogawa Middle East B.S.C. P.O. Box 10070, Manama Building 577, Road 2516, Busaiteen 225, Muharraq, Bahrain Phone: (973)-17-358100 Fax: (973)-17-336100 E-mail: YME-SIS-ENG@bh.yokogawa.com
Yokogawa China Co., Ltd. 3F TowerD Cartelo Crocodile Building, No.568 West Tianshan Road, Shanghai 200335, China Phone: (86)-21-62396262 Fax: (86)-21-62387866 E-mail: YCN_RS_TEAM@gr.cn.yokogawa.com
Yokogawa Engineering Asia Pte Ltd Safety Excellence Center 5 Bedok South Road Singapore 469270 Phone: (65)-6241-9933 Fax: (65)-6241-2606 E-mail: prosafe@sg.yokogawa.com

Revision Information

Title : Safety Manual

Manual No. : IM 32P01S10-01EN

Jun. 2023/9th Edition/R4.09 or later

1, 2.1	Added descriptions of Systematic Capability.

Jan. 2022/8th Edition/R4.07

2.3	Added descriptions of automatic scan period extension and behavior at abnormal calculation.

Feb. 2021/7th Edition/R4.06

Introduction, 2.1, 2.2	Added descriptions of the ProSafe-RS Lite.
2.2, 2.8	Added and updated the descriptions about SIL.

Dec. 2019/6th Edition/R4.05

Introduction	Updated description of registered trademarks and trademarks.

Aug. 2018/5th Edition/R4.04

Introduction	Updated description of registered trademarks of YOKOGAWA.

Oct. 2017/4th Edition/R4.03.10

2.2	Added descriptions of the fire and gas communication module.
2.3	Added descriptions of the fire and gas communication.
2.6	Added descriptions of the fire and gas communication.
2.8	Updated a check list item.

May 2017/3rd Edition/R4.03

Introduction	Deleted Windows Vista in Trademark Acknowledgments.
2.2	Added an explanation about Digital I/O module.

Oct. 2016/2nd Edition/R4.02

Introduction	Updated descriptions in "■ Safety, Protection, and Modification of the Product," "■ Symbols," and "■ Trademark Acknowledgments." Added a new term in "■ Full Names and Simplified Terms."

Dec. 2015/1st Edition/R4.01

Newly published

■ For Questions and More Information Online Query: A query form is available on the following URL for online query. http://www.yokogawa.com/iss
■ Written by Yokogawa Electric Corporation
■ Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Attachment 9.8 Message Reference Manual
IM32P02B10-01EN

User's Manual

ProSafe-RS
ProSafe-RS Lite

Messages Reference Manual

IM 32P02B10-01EN

YOKOGAWA
Yokogawa Electric Corporation

IM 32P02B10-01EN
9th Edition

Introduction

This manual describes the details of Diagnostic Information messages displayed in the Diagnostic Information Window of SCS Maintenance Support Tool or System Alarm View of HIS.

The table of the contents of this manual can be used as message number index.

If you are using YFGW520, replace the term “YFGW510” with “YFGW520” in the User’s Manual.

This manual consists of the following chapters:

Chapter 1 : This chapter explains how to refer to the Diagnosis Information in SENG.

Chapter 2 : This chapter explains the details about SCS Messages.

Chapter 3 : This chapter explains the details about common messages of CENTUM VP or CS 3000 and SENG.

Appendix : A list of the alarm class for the corresponding message number is provided.

9th Edition : Dec. 2023 (YK)
All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Safety Precautions for Use

Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Be sure to confirm the specifications and required settings of the devices that are used in combination with the Product by referring to the instruction manual or other documents of the devices.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:



Indicates that caution is required when handling the equipment. This symbol is labeled on the Product to indicate the possibility of dangers such as electric shock on personnel and equipment, and also indicate that the user must refer to the User's Manuals for necessary actions. In the User's Manuals, this symbol is used together with a signal word "WARNING" or "CAUTION" at the locations where precautions for avoiding dangers are described.

<French> Signale qu'il faut faire preuve de prudence pendant la manutention de l'équipement. Ce symbole, apposé sur le produit, signale les risques potentiels tels qu'une électrocution du personnel ou de l'équipement, et demande à l'opérateur de se reporter aux manuels de l'utilisateur pour savoir les actions nécessaires. Dans les manuels de l'utilisateur, ce symbole est utilisé conjointement avec le mot « WARNING » ou « CAUTION » aux emplacements où des précautions doivent être observées pour éviter les dangers décrits.



Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.

<French> Signale qu'il faut faire preuve de prudence avec la surface brûlante. Les appareils sur lesquels est apposé ce symbole risquent de devenir brûlants. Tout contact physique ou matériel avec ces appareils risque de provoquer des brûlures ou des dommages.



Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.



Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.

Indicates an AC supply.

Indicates a DC supply.

| | Indicates the ON position of a power on/off switch.

◯ Indicates the OFF position of a power on/off switch.

Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

Warning and Disclaimer

- Except as specified in the warranty terms, YOKOGAWA shall not provide any warranty for the Product.
- YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Product.

Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the Software Product's merchantability or suitability for any particular purpose, except as specified in the warranty terms.
- Purchase the appropriate number of licenses of the Software Product according to the number of computers to be used.
- No copy of the Software Product may be made for any purpose other than backup; otherwise, it is deemed as an infringement of YOKOGAWA's Intellectual Property rights.
- Keep the software medium of the Software Product in a safe place.
- No reverse engineering, reverse compiling, reverse assembling, or converting the Software Product to human-readable format may be performed for the Software Product.
- No part of the Software Product may be transferred, converted, or sublet for use by any third-party, without prior written consent from YOKOGAWA.

Documentation Conventions

Symbols

The following symbols are used in the User's Manuals.

 WARNING	Indicates precautions to avoid a danger that may lead to death or severe injury.
 CAUTION	Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.
IMPORTANT	Indicates important information required to understand operations or functions.
TIP	Indicates additional information.
	Indicates referenced content. In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

Typographical Conventions

The following typographical conventions are used throughout the User's Manuals.

Commonly Used Conventions throughout the User's Manuals

- Δ Mark
  Indicates that a space must be entered between character strings.
  Example:

  ```
  .ALΔPIC010Δ-SC
  ```

- Character string enclosed by braces { }
  Indicates character strings that may be omitted.

  Example:

  ```
  .PRΔTAG{Δ.sheet name}
  ```

Conventions Used to Show Key or Button Operations

- Characters enclosed by brackets [ ]
  When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a button name in a window, or an item in a list box displayed in a window.

  Example:

  To alter the function, press the [ESC] key.

Conventions of a User-defined Folder

- User-defined folder name enclosed by parenthesis ( )
  User definable path is written in a pair of parentheses.

  Example:

  ```
  (RS Project Folder)\SCS0101
  ```

If the RS Project Folder is `C:\MYRSPJT`, the above path becomes `C:\MYRSPJTSCS0101`.

Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.
If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

Definitions of Node and Module Terms

In the User's Manuals, nodes and modules are referred to by using collective terms, another terms, or abbreviations based on the following definitions:

- Definitions of nodes
  - Node: A node is a collective term for an FIO node and an N-IO node.
  - FIO node: This is a collective term for a safety control unit, a safety node unit, and a unit for optical ESB bus repeater module.
  - CPU node: This is another term for a safety control unit. The abbreviation of safety control unit is SCU.
  - I/O node: This is another term for a safety node unit. The abbreviation of safety node unit is SNU.
  - N-IO node: This is a collective term for a node interface unit and an N-IO I/O unit. The abbreviation of node interface unit is NIU.
- Definitions of modules
  - I/O module: This is a collective term for an FIO I/O module and an N-IO I/O module.
  - FIO I/O module: This is a collective term for an analog I/O module and a digital I/O module for FIO, and a communication module.
  - N-IO I/O module: This is a collective term for the modules that can be mounted on an N-IO I/O unit.
  - AIO/DIO module: This is a collective term for an analog I/O module, a digital I/O module, and a universal type I/O module.
  - Analog I/O module: This is a collective term for an analog input module and an analog output module.
  - Digital I/O module: This is a collective term for a digital input module and a digital output module.
  - Universal type I/O module: This is a collective term for the I/O modules for which the channel signal category can be changed by software.

- Input module: This is a collective term for an analog input module, digital input module, and a universal type I/O module with defined input channels.
- Output module: This is a collective term for an analog output module, digital output module, and a universal type I/O module with defined output channels.
- Communication module: This is a collective term for a serial communication module, an Ethernet communication module, and a fire and gas communication module.

Full Names and Simplified Terms

In the User's Manuals, simplified terms listed in the following table are used.

Table Info-1 Full Names and Simplified Terms

Full Name	Simplified Term
Automation Design Suite	AD Suite
Automation Design Organizer	AD Organizer
Automation Design Server	AD Server
Automation Design project	AD project
Automation Design Master Database	ADMDB
Automation Design Suite Administration Tool	ADS Administration Tool
iDefine for ProSafe-RS	iDefine
Modification Package	ModPack
SCSV1-S (SCS supporting the SSC10S/SSC10D safety control units)	SCSV1
SCSP1-S (SCS supporting the SSC50S/SSC50D safety control units)	SCSP1
SCSP2-S (SCS supporting the SSC60S/SSC60D safety control units)	SCSP2
SCSP3-S (SCS supporting the S2SC70S/S2SC70D safety control units)	SCSP3
SCSL2-S (SCS supporting the L1SC70S/L1SC70D safety control units)	SCSL2
SCSU1-S (SCS supporting the SSC57S/SSC57D safety control units)	SCSU1

Copyright and Trademark Notices

All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, PRM, Exaopc, FieldMate Validator, and STARDOM are registered trademarks or trademarks of Yokogawa Electric Corporation.
- The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

Messages Reference Manual

IM 32P02B10-01EN 9th Edition

CONTENTS

1. Referencing Diagnostic Information Messages on the SENG..... 1-1
   - 1.1 How to Display the Diagnostic Information Window.....1-2
   - 1.2 Diagnostic Information Window.....1-3
   - 1.3 Printout of Diagnostic Information Message.....1-4
2. Details of Output Messages Specific to the SCS..... 2-1
   - 2.1 System Alarms (Message Numbers 4101 through 4222).....2-2
     - No. 4101 Inter-SCS safety communication error information 2-2
     - No. 4102 Inter-SCS safety communication error recovery information 2-3
     - No. 4103 Variable lock 2-3
     - No. 4104 Cancellation of variable lock 2-4
     - No. 4105 I/O module lock 2-5
     - No. 4106 Cancellation of I/O module lock 2-5
     - No. 4107 All input module locks 2-5
     - No. 4108 Cancellation of all input module locks 2-6
     - No. 4109 All output module locks 2-6
     - No. 4110 Cancellation of all output module locks 2-6
     - No. 4111 All module locks 2-6
     - No. 4112 Cancellation of all module locks 2-6
     - No. 4113 Number of locks exceeded 2-7
     - No. 4114 Recovery from exceeded number of locks 2-7
     - No. 4115 Override setting 2-7
     - No. 4116 Cancellation of override 2-7
     - No. 4117 Information of change to override enabled state 2-8
     - No. 4118 Information of change to override disabled state 2-8
     - No. 4119 Number of overrides exceeded 2-8
     - No. 4120 Recovery from exceeded number of overrides 2-8
     - No. 4121 Number of enabled overrides exceeded 2-8
     - No. 4122 Recovery from exceeded number of enabled overrides 2-9
     - No. 4123 Number of active PASSWD FBs exceeded 2-9
     - No. 4124 Recovery from exceeded number of active PASSWD FBs 2-9
     - No. 4125 I/O module channel error occurred 2-9
     - No. 4126 Recovery from I/O module channel error 2-10
     - No. 4127 Setting PASSWD FB to ON 2-11

No. 4128 Setting PASSWD FB to OFF 2-11
No. 4129 GPS interface unit error 2-11
No. 4130 Recovery of GPS interface unit 2-12
No. 4131 Communication module lock 2-12
No. 4132 Cancellation of Communication module lock 2-12
No. 4133 Information of a diagnosis error in the received data of SCS Link Transmission. 2-12
No. 4134 Information of a diagnosis error recovery in the received data of SCS Link Transmission. 2-14
No. 4135 SCS Link Transmission data lock 2-14
No. 4136 Cancellation of SCS Link Transmission data lock 2-14
No. 4137 Number of Locked Stations in SCS Link Transmission Exceeded 2-15
No. 4138 Recovery from exceeded number of locked stations in SCS Link Transmission 2-15
No. 4139 Inter-SCS Safety Communication data lock 2-15
No. 4140 Cancellation of Inter-SCS Safety Communication data lock 2-15
No. 4141 Number of locked stations in Inter-SCS Safety Communication exceeded 2-16
No. 4142 Recovery from exceeded number of locked stations in Inter-SCS Safety Communication 2-16
No. 4143 Start of automatic scan period extension 2-16
No. 4144 Cancellation of automatic scan period extension 2-16
No. 4145 Abnormal calculation occurred 2-17
No. 4146 Recovery from abnormal calculation 2-17
No. 4151 Information of retainable data initialization 2-17
No. 4152 Online change of scan period 2-18
No. 4153 Information of Inter-SCS Safety Communication data lock time-up 2-18
No. 4154 Information of forced cancellation of Inter-SCS Safety Communication data locks 2-18
No. 4155 Information of SCS Link Transmission status change. 2-18
No. 4156 Information of SCS Link Transmission definition change 2-19
No. 4157 Information of SCS Link Transmission wiring change 2-19
No. 4158 Information of SCS Link Transmission lock time-up 2-19
No. 4159 Information of forced cancellation of SCS Link Transmission locks 2-19
No. 4160 Invalid password for Manual Operation FB 2-19
No. 4161 Information of Output IOM Shutdown 2-20
No. 4162 Information of communication I/O definition change 2-20
No. 4163 Information of communication I/O wiring change 2-20
No. 4164 Information of disabling security level change 2-20
No. 4165 Information of enabling security level change 2-21
No. 4166 Information of communication module lock time-up 2-21

No. 4167 Information of forced cancellation of communication module locks ... 2-21
No. 4168 Information of tag name change by online change download 2-21
No. 4169 NVRAM diagnosis error 2-21
No. 4170 Flash memory diagnosis error 2-22
No. 4172 Information of resource change by online change download 2-22
No. 4173 Completion of writing to flash memory 2-22
No. 4174 Failed to write to flash memory 2-23
No. 4175 Failed to update external communication data 2-23
No. 4177 Information of SCS security level change 2-23
No. 4178 Information of security level time-up 2-24
No. 4179 Information of communication I/O module output enable operation ... 2-24
No. 4180 Information of password change 2-24
No. 4181 Information of output enable operation 2-24
No. 4182 Information of FIO output module start operation 2-25
No. 4183 Request to upload SOE to SENG 2-25
No. 4184 Notification on saving SOE trip signal file in SCS 2-25
No. 4185 Information of variable value change 2-25
No. 4186 Information of lock time-up 2-26
No. 4187 Information of forced cancellation of locks 2-26
No. 4188 Start of online change download 2-26
No. 4189 Completion of online change download 2-26
No. 4190 Online change download error 2-26
No. 4191 Completion of I/O definition rewriting 2-27
No. 4192 Information of override state time-up 2-27
No. 4193 Information of forced release of all overrides 2-28
No. 4194 Information of override enabled state time-up 2-28
No. 4195 Information of communication I/O data status change 2-28
No. 4196 Invalid password for PASSWD FB 2-28
No. 4197 Information on active PASSWD FB time-up 2-29
No. 4198 Information on forced reset of PASSWD FB 2-29
No. 4199 Override communication error 2-29
No. 4201 Information of node maintenance port enable operation 2-29
No. 4202 Information of node maintenance port disable operation 2-29
No. 4203 Information of node maintenance port disable operation for all N-IO nodes 2-30
No. 4205 Information of node maintenance port enabled state 2-30
No. 4206 Information of node maintenance port disabled state 2-30
No. 4207 Information of HSDTR FB or GASDTR FB reset operation 2-30
No. 4208 Communication error in HSDTR FB or GASDTR FB reset operation 2-30
No. 4209 Safety subsystem communication error 2-31

No. 4210 Recovery from safety subsystem communication error 2-32
No. 4211 Safety subsystem communication path error..... 2-32
No. 4212 Recovery from safety subsystem communication path error 2-34
No. 4213 Safety subsystem communication I/O lock 2-34
No. 4214 Cancellation of safety subsystem communication I/O lock 2-35
No. 4215 Number of safety subsystem communication I/O locks exceeded 2-35
No. 4216 Recovery from exceeded number of safety subsystem communication I/O locks 2-35
No. 4217 Safety subsystem communication I/O data status change 2-35
No. 4219 Safety subsystem communication I/O lock time-up 2-36
No. 4220 Forcible cancellation of all safety subsystem communication I/O locks 2-36
No. 4221 Alarm for the operation data reset switch of CPU module 2-36
No. 4222 Recovery from alarm for the operation data reset switch of CPU module.....2-36

3. Details of Output Messages in Common with CENTUM..... 3-1

3.1 Safety Control Station Error Occurrence and Recovery Messages (Message Numbers 0001 through 0094).....3-2

No. 0001 Reset start of safety control station 3-2
No. 0003 Safety control station automatic reset start 3-2
No. 0005 Power ON initial cold start of safety control station 3-2
No. 0009 Transfer of control right of safety control station 3-2
No. 0011 Fail information of safety control station.....3-3
No. 0013 AC power supply failure of safety control station 3-4
No. 0015 Self-diagnosis error of clock inside CPU module 3-4
No. 0017 ROM checksum error of CPU module 3-5
No. 0021 Internal task error of safety control station 3-5
No. 0023 Mapping block fatal error 3-5
No. 0025 Function control word error 3-5
No. 0027 Mapping block record information error 3-5
No. 0033 Online downloading abnormal end 3-6
No. 0041 Safety control station fan alarm 3-6
No. 0042 Recovery from safety control station fan alarm 3-6
No. 0043 Safety control station temperature alarm 3-7
No. 0044 Recovery from safety control station temperature alarm 3-7
No. 0045 Power supply module alarm of safety control station 3-7
No. 0046 Recovery from power supply module alarm of safety control station 3-7
No. 0047 Battery alarm of CPU module 3-7
No. 0048 Recovery from battery alarm of CPU module 3-8
No. 0053 Safety control station cabinet temperature alarm 3-8
No. 0054 Recovery from safety control station cabinet temperature alarm 3-8

No. 0055 Information of same frame reception in online change download communication 3-8
No. 0057 Information of online change download error 3-9
No. 0059 Information of recovery from node power failure 3-9
No. 0063 ESB bus error 3-9
No. 0064 Normal recovery of ESB bus 3-10
No. 0065 Failure of N-ESB bus module or ESB Bus Interface module..... 3-10
No. 0066 Normal recovery of N-ESB bus module or ESB Bus Interface module of node..... 3-11
No. 0067 Failure of power supply of node 3-11
No. 0068 Normal recovery of power supply of a node 3-12
No. 0069 Error before database download to I/O module 3-12
No. 0073 Error in the F-SB bus connecting the N-IO I/O unit and node interface unit 3-13
No. 0074 Normal recovery of the F-SB bus connecting the N-IO I/O unit and node interface 3-13
No. 0081 Failure of I/O module..... 3-13
No. 0082 Normal recovery of I/O module 3-15
No. 0083 I/O module database error occurred 3-15
No. 0085 I/O module communication error occurred 3-16
No. 0086 Recovery from I/O module communication error 3-16
No. 0087 Node error occurred 3-17
No. 0088 Normal recovery of node 3-17
No. 0089 Subsystem communication error 3-17
No. 0090 Subsystem communication recovered 3-19
No. 0093 CPU node's housekeeping unit error 3-19
No. 0094 Normal recovery of CPU node's housekeeping unit 3-19

3.2 Safety Control Station Status Change Related Messages (Message Numbers 0425 through 0480)..... 3-20

No. 0425 Start of online upgrade..... 3-20
No. 0426 Normal completion of online upgrade..... 3-20
No. 0427 Online upgrade error..... 3-20
No. 0447 Node maintenance port enabled notification 3-20
No. 0448 Node maintenance port disabled notification 3-20
No. 0450 Copy program and database on control side of safety control station to standby side 3-21
No. 0451 Information of switching of control side of safety control station 3-21
No. 0452 Information of switching of standby side of safety control station 3-21
No. 0455 Node maintenance notification 3-21
No. 0456 Node maintenance cancellation notification 3-21
No. 0459 Information of I/O module service side 3-22
No. 0460 Information of I/O module out service 3-22
No. 0471 Normal completion of online change download 3-22

No. 0474 Information of tag list duplicate error 3-22
No. 0475 Start of database download to I/O module 3-22
No. 0476 Normal completion of database download to I/O module 3-23
No. 0477 Database download error to I/O module 3-23
No. 0480 Heavy load on periodical processing 3-24

3.3 Safety Control Station Related Messages (Message Numbers 0727 through 0787)..... 3-25

No. 0727 Block mode recovery error information 3-25
No. 0743 Self-diagnostic SEN-BUS Failure 3-25
No. 0744 Self-diagnostic SEN-BUS Recovery 3-25
No. 0749 Self-diagnosis detected an I/O Error 3-25
No. 0750 I/O Recovery from the error detected by self-diagnosis 3-26
No. 0751 Time self-diagnostic testing error 3-26
No. 0753 Communication Overload 3-26
No. 0767 ESB bus error on either bus 3-27
No. 0768 Recovery from ESB bus error on either bus 3-27
No. 0769 Error in the diagnosis of the safety control station cabinet by external equipment 3-27
No. 0770 Recovery from error in the diagnosis of the safety control station cabinet by external equipment 3-28
No. 0787 Self-diagnosis detected I/O error in CPU module 3-28

3.4 Fieldbus Messages (Message Numbers 3401 through 3408)..... 3-29

No. 3401 HART device event notification 3-29
No. 3403 IOM detected a HART device status change 3-29
No. 3405 Communication error when acquiring HART device status (No response) 3-29
No. 3407 Communication error when acquiring HART device status 3-30
No. 3408 Normal recovery of HART device status acquisition communication 3-31

Messages Reference Manual

IM 32P02B10-01EN 9th Edition

CONTENTS

Appendix

Appendix 1. Alarm Class..... App.1-1

1. Referencing Diagnostic Information Messages on the SENG

You can view diagnostic information messages on the Diagnostic Information window, which is called up from SCS Status Overview window.

1.1 How to Display the Diagnostic Information Window

You can display the Diagnostic Information window from the SCS Status Overview window.

1. In the SCS Status Overview window, select an SCS.
   The following figure shows an example of the SCS Status Overview window.

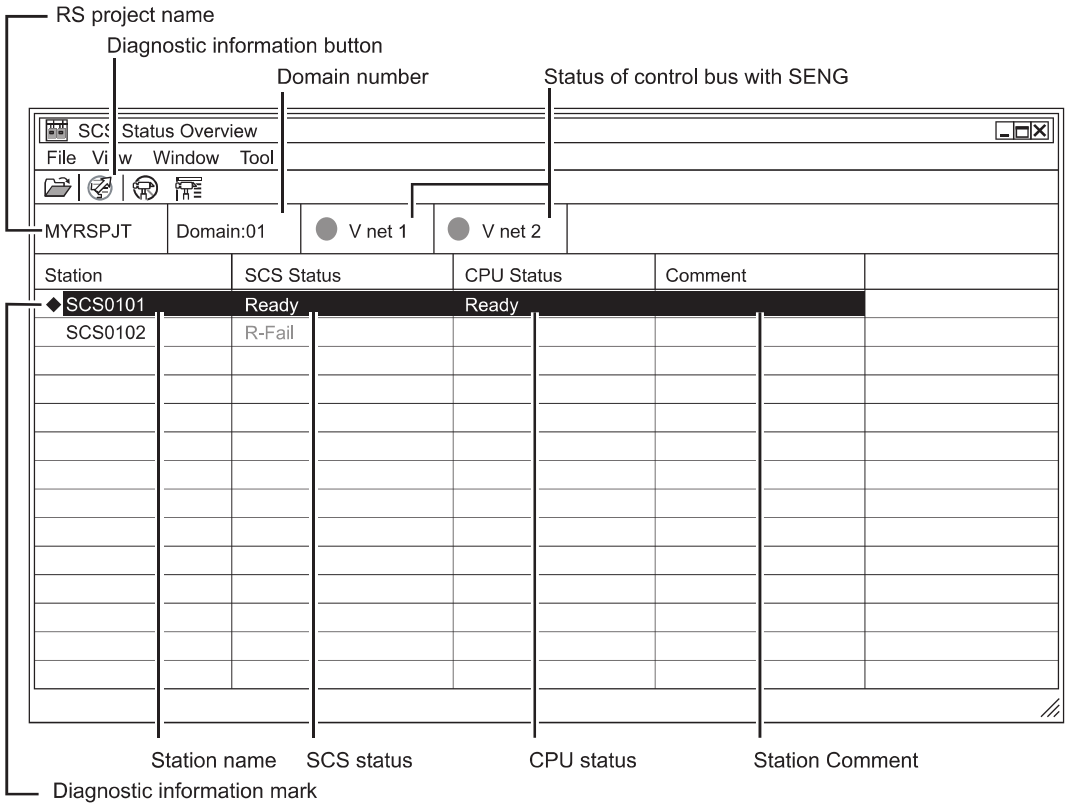


Figure 1.1-1 SCS Status Overview Window and Diagnostic Information button

2. Click the [Diagnostic Information] button on the tool bar.
   The Diagnostic Information window is displayed, showing the diagnostic information messages of the station you have selected.

1.2 Diagnostic Information Window

The Diagnostic Information window is shown in the figure below.

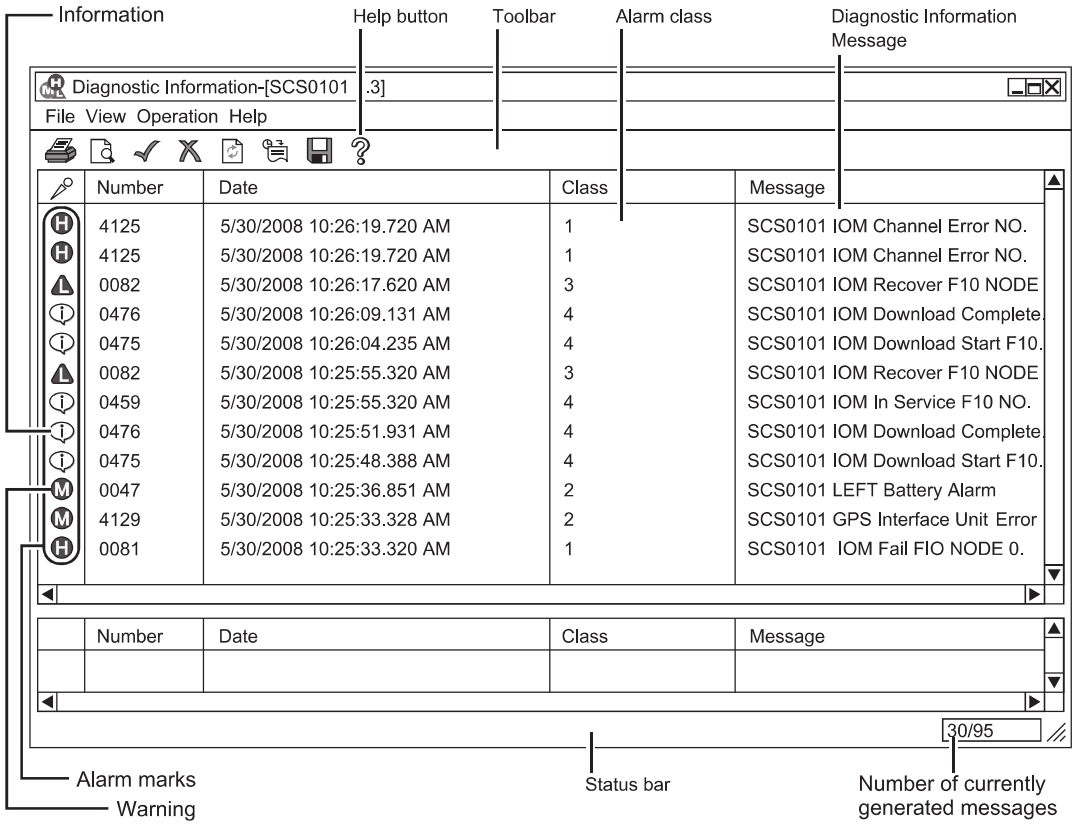


Figure 1.2-1 Diagnostic Information Window

SEE ALSO For more information about the Diagnostic Information window, refer to:

H5., “Displaying SCS diagnostic information” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

How to Display the Help Dialog Box

The details of Diagnostic Information window is displayed in the Help dialog box.

1. In the Diagnostic Information window, select a diagnostic information message.
2. Click the [Help] button on the tool bar.
   The Help dialog box is displayed.

SEE ALSO For more information about the Help dialog box, refer to:

H6.3, “Diagnostic information message help function” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

1.3 Printout of Diagnostic Information Message

The printout of diagnostic information messages is shown in the figure below.

5/30/2008 2:02:44 PM	page 1/1
Search condition	SCS0101 1.3
Format	Alarm mark, Message number, Date, Class, Message
Selection mark	New Alarm:No mark, Acknowledged:A, Deleted:D

0081 5/30/2008 9:00:15.980 AM 1 SCS0101 IOM Fail FIO NODE 01 SLOT 05 Code = 5103
0083 5/30/2008 9:00:15.980 AM 2 SCS0101 IOM Configuration Error FIO NODE 01 SLOT 05
0081 5/30/2008 9:00:15.980 AM 1 SCS0101 IOM Fail FIO NODE 01 SLOT 03 Code = 5103
0083 5/30/2008 9:00:15.980 AM 2 SCS0101 IOM Configuration Error FIO NODE 01 SLOT 03
0081 5/30/2008 9:00:15.980 AM 1 SCS0101 IOM Fail FIO NODE 01 SLOT 01 Code = 5103
0083 5/30/2008 9:00:15.980 AM 2 SCS0101 IOM Configuration Error FIO NODE 01 SLOT 01
0451 5/30/2008 9:00:00.465 AM 2 SCS0101 LEFT Control
0005 5/30/2008 9:00:00.465 AM 2 SCS0101 Power ON (Cold Start)
0013 5/30/2008 9:00:00.465 AM 2 SCS0101 AC Fail (Time 1/1/1970 9:00:00 AM)

Figure 1.3-1 Printout of Diagnostic Information Message

2. Details of Output Messages Specific to the SCS

This section describes the details of output messages specific to the SCS. The format for each message follows the example shown below, Cause, Action, Remark, Note and Error code may be omitted, depending on the message.

No.xxxx

Message name Name of the message.

Example: Information of security level time-up

Printing example Indicates an example of print or display.

Example: SCS0101 Security Level = 1 Elapsed the Specified Period = 08 : 00 : 00

In this document, space in messages and the leading “00” of various numbers may be different from actual printing examples to the extent they do not impair the understanding of messages.

Meaning Meaning of a message.

Example: The security level is set to “1” for the duration exceeding the time limit (8 hours in the above example) specified in SYS_SECURE Function Block (hereinafter referred to as “FB”).

Cause Describes the cause of occurrence. The description may be omitted depending on the message.

Example: The security level has not been reverted.

Action Describes the action to take. The description may be omitted depending on the message.

Example: Revert the security level to “2.”

Remark Describes an item(s) related to the message. The description may be omitted depending on the message.

Note Describes cautions. The description may be omitted depending on the message.

Error code Describes details of the error code included in the message, if any. The description may be omitted depending on the message.

2.1 System Alarms (Message Numbers 4101 through 4222)

This section describes system alarm messages issued from the SCS.

No.4101

Message name Inter-SCS safety communication error information

Printing example SCS0101 Inter-SCS Safety Communication Receive Error Variable = C0102001 Code = 5041-8000

Meaning An error is detected during inter-SCS safety communication. The erroneous binding variable (C0102001 in the above example) is included in the message.

Cause The following causes may be considered. Check the error codes for more detail.

- Stop/restart on the producing side SCS
- Problem in the communication path
- Change in the application of inter-SCS safety communication

Remark Inter-SCS safety communication

Error code The first four digits are an error code, and the next four digits are a cause code. The error detail can be found from the descriptions of both the codes.

The error code represents the type of error. The table explains each error code and the action you can take to fix the error.

Table 2.1-1 Message No. 4101 - Error Code List

Code (hexadecimal)	Description	Action
5040	An error that occurs when an application is created incorrectly.	Check the application logic.
5041	No data received within the reception interval timeout value.	Check the producing side SCS and the communication path.
5042	Time diagnosis found an error.	
5043	Communication protocol error (internal error)	Record the message content and report to Yokogawa's service department.

The cause code represents the event that caused the problem and is logical OR of the following codes.

Table 2.1-2 Message No. 4101 - Cause Code List

Code (hexadecimal)	Errors	Description	Presumed cause
8000	No response	Communication stopped and data no longer arrived.	Communication was cut off, or the producing side stopped.
4000	Reset detection	The restart on the producing side was detected.	Restart on the producing side

Continues on the next page

Table 2.1-2 Message No. 4101 - Cause Code List (Table continued)

Code (hexa-decimal)	Errors	Description	Presumed cause
2000	CRC error in delay-related diagnosis information	The CRC code of delay-related diagnosis information is not correct.	Temporary communication error
1000	CRC mismatch	The communication content and CRC do not match.	Temporary communication error
0400	Equalization error of delay-related diagnosis information	Communication for acquiring delay-related diagnosis information stopped.	Communication was interrupted or the producer SCS is stopped.
0200	Variable name error	The variable name is not “Cddssxxx.”	An application was created incorrectly.
0100	Address error	The domain and station numbers are different from the binding variable.	An application was created incorrectly.
0040	Transmission delay occurred	Communication was updated later than the transmission delay timeout time.	Communication delay
0020	Date/time error on the producing side	An error occurred in time management on the producing side, so the date/time is not reliable.	Date/time management error on the producing side
0010	Date/time error on the consuming side	An error occurred in time management on the consuming side, so the date/time is not reliable.	Date/time management error on the producing side
0004	Different FB ID information	The FB ID information is different from the initial value.	Internal error
0001	Data type error	The data type does not match.	Internal error

No.4102

Message name Inter-SCS safety communication error recovery information

Printing example SCS0101 Inter-SCS Safety Communication Receive Recover Variable = C0102001

Meaning An inter-SCS safety communication error for the variable (C0102001 in the above example) recovered. (This is a recovery message of No. 4101.)

Cause The following causes may be considered.

- Recovery of the producing side SCS
- Recovery of the communication path
- Recovery of the application of inter-SCS safety communication

Remark Inter-SCS safety communication

No.4103

Message name Variable lock

Printing example 1 In the case of I/O (N-IO) variables:

SCS0101 Variable Locked Variable=VAR001 N-IO NODE 01 UNIT 01 SLOT 02 CH 03

Printing example 2 In the case of I/O (FIO) variables:

SCS0101 Variable Locked Variable=VAR001 NODE 1 SLOT 2 CH 3

Printing example 3 In the case of internal variables:

SCS0101 Variable Locked Variable=VAR001

Meaning The variable (VAR001 in the above example) was locked by operation from the SENG. For an I/O variable, the channel location corresponding to the variable (N-IO node 1, unit 1, slot 2, channel 3 in printing example 1, and FIO node 1, slot 2, channel 3 in printing example 2) is also included in the message.

Remark Forcing function

Note Be sure to unlock the variables that were locked.

If an IO_BOOL type or IO_REAL type variable is locked, the member variable v or status will be indicated in the format of [Variable=VAR001.v] at the position of the variable name in the system alarms. If the variable is not wired to the channel, the member variable v will be always displayed. Nevertheless, in any of the above cases, the whole IO_BOOL type or IO_REAL type variable will be locked.

When locking an array element, the whole array will be locked. Under this circumstance, the variable name displayed in the system alarm will be attached with the array element subscript as [Variable=VAR001[1]].

No.4104

Message name Cancellation of variable lock

Printing example 1 In the case of I/O (N-IO) variables:

SCS0101 Variable Unlocked Variable=VAR001 N-IO NODE 01 UNIT 01 SLOT 02 CH 03

Printing example 2 In the case of I/O (FIO) variables:

SCS0101 Variable Unlocked Variable=VAR001 NODE 1 SLOT 2 CH 3

Printing example 3 In the case of internal variables:

SCS0101 Variable Unlocked Variable=VAR001

Meaning The lock of the variable (VAR001 in the above example) was cancelled by operation from the SENG. For an I/O variable, the channel location corresponding to the variable (N-IO node 1, unit 1, slot 2, channel 3 in printing example 1, and FIO node 1, slot 2, channel 3 in printing example 2) is also included in the message.

Remark Forcing function

Note If an IO_BOOL type or IO_REAL type variable is unlocked, the member variable v or status will be indicated in the format of [Variable=VAR001.v] at the position of the variable name in the system alarms. If the variable is not wired to the channel, the member variable v will be always displayed. Nevertheless, in any of the above cases, the whole IO_BOOL type or IO_REAL type variable will be unlocked.

Moreover, when unlocking an array element, the whole array will be unlocked. Under this circumstance, the variable name displayed in the system alarm will be attached with the array element subscript as [Variable=VAR001[1]].

No.4105

Message name I/O module lock

Printing example 1 SCS0101 IOM Locked N-IO NODE 01 UNIT 01 SLOT 02

Meaning 1 An N-IO I/O module was locked by operation from the SENG. The location of the N-IO I/O module (N-IO node 1, unit 1, slot 2 in the the above example) is included in the message.

Printing example 2 SCS0101 IOM Locked N-IO NODE 01 UNIT 01 SLOT 02 All Input Channel

Meaning 2 All input channels of the N-IO I/O module were locked by operation from the SENG. The location of the N-IO I/O module (N-IO node 1, unit 1, slot 2 in the the above example) is included in the message.

Printing example 3 SCS0101 IOM Locked N-IO NODE 01 UNIT 01 SLOT 02 All Output Channel

Meaning 3 All output channels of the N-IO I/O module were locked by operation from the SENG. The location of the N-IO I/O module (N-IO node 1, unit 1, slot 2 in the the above example) is included in the message.

Printing example 4 SCS0101 IOM Locked NODE 01 SLOT 02

Meaning 4 An FIO I/O module was locked by operation from the SENG. The location of the FIO I/O module (FIO node 1, slot 2 in the above example) is included in the message.

Remark Forcing function

Note Be sure to cancel the lock of the I/O module that was locked.

No.4106

Message name Cancellation of I/O module lock

Printing example 1 SCS0101 IOM Unlocked N-IO NODE 01 UNIT 01 SLOT 02

Meaning 1 The N-IO I/O module was unlocked by operation from the SENG. The location of the N-IO I/O module (N-IO node 1, unit 1, slot 2 in the the above example) is included in the message.

Printing example 2 SCS0101 IOM Unlocked N-IO NODE 01 UNIT 01 SLOT 02 All Input Channel

Meaning 2 All input channels of the N-IO I/O module were unlocked by operation from the SENG. The location of the N-IO I/O module (N-IO node 1, unit 1, slot 2 in the the above example) is included in the message.

Printing example 3 SCS0101 IOM Unlocked N-IO NODE 01 UNIT 01 SLOT 02 All Output Channel

Meaning 3 All output channels of the N-IO I/O module were unlocked by operation from the SENG. The location of the N-IO I/O module (N-IO node 1, unit 1, slot 2 in the the above example) is included in the message.

Printing example 4 SCS0101 IOM Unlocked NODE 01 SLOT 02

Meaning 4 The FIO I/O module was unlocked by operation from the SENG. The location of the FIO I/O module (FIO node 1, slot 2 in the above example) is included in the message.

Remark Forcing function

No.4107

Message name All input module locks

Printing example SCS0101 All Input IOM Locked

Meaning All input channels of universal-type I/O modules, and FIO input modules, were locked by operation from the SENG.

Remark Forcing function

Note Be sure to unlock the input channels of universal-type I/O modules, and the FIO input modules, which were locked.

No.4108

Message name Cancellation of all input module locks

Printing example SCS0101 All Input IOM Unlocked

Meaning All input channels of universal-type I/O modules, and FIO input modules, were unlocked by operation from the SENG.

Remark Forcing function

No.4109

Message name All output module locks

Printing example SCS0101 All Output IOM Locked

Meaning All output channels of universal-type I/O modules, and FIO output modules, were locked by operation from the SENG.

Remark Forcing function

Note Be sure to unlock the output channels of universal-type I/O modules, and the FIO output modules, which were locked.

No.4110

Message name Cancellation of all output module locks

Printing example SCS0101 All Output IOM Unlocked

Meaning All output channels of universal-type I/O modules, and FIO output modules, were unlocked by operation from the SENG.

Remark Forcing function

No.4111

Message name All module locks

Printing example SCS0101 All IOM Locked

Meaning All I/O modules were locked by operation from the SENG.

Remark Forcing function

Note Be sure to cancel the locks of the I/O modules that were locked.

No.4112

Message name Cancellation of all module locks

Printing example SCS0101 All IOM Unlocked

Meaning The locks of all I/O modules were cancelled by operation from the SENG.

Remark Forcing function

No.4113

Message name Number of locks exceeded

Printing example SCS0101 Number of Locks Exceeds the Limit = 3

Meaning The total number of locked variables exceeded the limit count (3 in the above example) specified in SYS_FORCE FB.

Cause This is an operation from the SENG. The number of locks is too many.

Action Cancel the variable locks.

Remark Forcing function, SYS_FORCE FB

Note Lock variables within the limit count.

No.4114

Message name Recovery from exceeded number of locks

Printing example SCS0101 Number of Locks Within the Limit = 3

Meaning The total number of locked variables is reduced to within the limit count (3 in the above example) specified in SYS_FORCE FB. (This is a recovery message of No. 4113.)

Cause This is an operation from the SENG.

Remark Forcing function, SYS_FORCE FB

No.4115

Message name Override setting

Printing example SCS0101 TAG001 Overridden (Instance = OVR0001)

Meaning Override operation was performed for the override FB (OVR0001 in the above example) that corresponds to the tag name (TAG001 in the above example) from the HIS.

Remark OVR_B, OVR_I, OVR_R, OVR_IB, OVR_IR, GOV_B, GOV_IB FB

No.4116

Message name Cancellation of override

Printing example SCS0101 TAG001 Override Released (Instance = OVR0001)

Meaning An override was cancelled for the override FB (OVR0001 in the above example) that corresponds to the tag name (TAG001 in the above example) from the HIS.

Remark OVR_B, OVR_I, OVR_R, OVR_IB, OVR_IR, GOV_B, GOV_IB FB

No.4117

Message name Information of change to override enabled state

Printing example SCS0101 Override Enabled

Meaning An override was enabled.

Cause The SW input parameter of the override FB was set to “TRUE.”

Remark OVR_B, OVR_I, OVR_R, OVR_IB, OVR_IR, GOV_B, GOV_IB FB

Note If the SW input parameter of any override FB is set to “TRUE,” this message is generated.

No.4118

Message name Information of change to override disabled state

Printing example SCS0101 Override Disabled

Meaning An override was disabled.

Cause The SW input parameter of all override FBs were set to “FALSE.”

Remark OVR_B, OVR_I, OVR_R, OVR_IB, OVR_IR, GOV_B, GOV_IB FB

Note If the SW input parameters of all override FBs are set to “FALSE,” this message is generated.

No.4119

Message name Number of overrides exceeded

Printing example SCS0101 Number of Overrides Exceeds the Limit = 3

Meaning The total number of overridden override FBs exceeded the limit count (3 in the above example) specified in SYS_OVR FB.

Cause This is an operation from the HIS. There are too many overrides.

Action Cancel overrides.

Remark SYS_OVR FB

Note Override within the limit count.

No.4120

Message name Recovery from exceeded number of overrides

Printing example SCS0101 Number of Overrides Within the Limit = 3

Meaning The total number of overridden override FBs is within the limit count (3 in the above example) specified in SYS_OVR FB. (This is a recovery message of No. 4119.)

Cause This is an operation from the HIS.

Remark SYS_OVR FB

No.4121

Message name Number of enabled overrides exceeded

Printing example SCS0101 Number of Enabled OVR FBs Exceeds the Limit = 3

Meaning The total number of override FBs in the override enabled state exceeded the limit count (3 in the above example) specified in SYS_OVR FB.

Action Disable override FBs.

Remark SYS_OVR FB

Note Enable overrides within the limit count.

No.4122

Message name Recovery from exceeded number of enabled overrides

Printing example SCS0101 Number of Enabled OVR FBs Within the Limit = 3

Meaning The total number of override FBs in the override enabled state is within the limit count (3 in the above example) specified in SYS_OVR FB. (This is a recovery message of No. 4121.)

Remark SYS_OVR FB

No.4123

Message name Number of active PASSWD FBs exceeded

Printing example SCS0101 Number of Activated PASSWD FBs Exceeds the Limit = 3

Meaning The total number of active PASSWD FBs exceeded the limit count (3 in the above example) specified in SYS_PSWD FB.

Cause This is an operation from the HIS. There are too many active PASSWD FBs.

Action Inactivate (reset to OFF) the PASSWD FBs that have exceeded the limit count.

Remark SYS_PSWD FB

Note Make PASSWD FBs active within the limit count.

No.4124

Message name Recovery from exceeded number of active PASSWD FBs

Printing example SCS0101 Number of Activated PASSWD FBs Within the Limit = 3

Meaning The total number of active PASSWD FBs is within the limit count (3 in the above example) specified in SYS_PSWD FB. (This is a recovery message of No. 4123.)

Cause Active PASSWD FBs were inactivated (reset to OFF) by operation from the HIS.

Remark SYS_PSWD FB

No.4125

Message name I/O module channel error occurred

Printing example 1 SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLOT 02 CH 03 XXXXXXXX (YYYY)

Printing example 2 SCS0101 IOM Channel Error NODE 01 SLOT 02 CH 03 XXXXXXXX (YYYY)

Meaning An error occurred in a channel of an I/O module (N-IO node 1, unit 1, slot 2, channel 3 in printing example 1, and FIO node 1, slot 2, channel 3 in printing example 2). XXXXXXXX indicates an error cause. YYYY indicates an error code.

Cause The table shows the causes of errors and error codes.

Table 2.1-3 Message No. 4125 - Error Causes

Error cause	Code	Description	Remark
TRNS+	5121	Upper limit error of the transmitter occurred.	
TRNS-	5122	Lower limit error of the transmitter occurred.	
IOP+	5123	Upper limit error of the IOP occurred.	When an intrinsic safety barrier is pulled out and inserted online, IOP + may be detected temporarily.
IOP-	5124	Lower limit error of the IOP occurred.	When an intrinsic safety barrier is pulled out and inserted online, or when the barrier power supply for the base plate for barrier is turned on, IOP- may be detected temporarily.
OvrRange	5125 5126	Input value is outside of the range of input values (-25 % to 125 %). This indicates a failure of the I/O module.	
Ch Fail	5127	A channel error was detected.	Open circuits of AO/DI/DO of FIO AIO/DIO modules are included in this error code.
ISDiscon	5128	Intrinsic safety barriers are not installed.	
ISCfgErr	5129	Intrinsic safety barriers are installed incorrectly.	
Open	512a	An open circuit of input/output was detected.	• When intrinsic safety barriers are used, this error code may be displayed due to an error caused by a short circuit. • When an intrinsic safety barrier is pulled out and inserted online, an open circuit may be detected temporarily.
Short	512b	A short circuit of input/output was detected.	
FieldErr	512c	A field external failure, barrier LFD error, and so on occurred. Check the details in the IOM report.	• When intrinsic safety barriers are used, this error code may be displayed due to an error caused by a short circuit. • When an intrinsic safety barrier is pulled out and inserted online, a line fault may be detected temporarily.

Action Check to see if the connected devices and connecting cables are normal.

No.4126

Message name Recovery from I/O module channel error

Printing example 1 SCS0101 IOM Channel Recover N-IO NODE 01 UNIT 01 SLOT 02 CH 03

Meaning 1 A channel of an N-IO I/O module (N-IO node 1, unit 1, slot 2, channel 3 in the above example) recovered from an error. (This is a recovery message of No. 4125.)

Printing example 2 SCS0101 IOM Channel Recover NODE 01 SLOT 02 CH 03

Meaning 2 A channel of an FIO I/O module (FIO node 1, slot 2, channel 3 in the above example) recovered from an error. (This is a recovery message of No. 4125.)

Printing example 3 SCS0101 IOM Channel Recover N-IO NODE 01 UNIT 01 SLOT 02 CH 03 (Chattering suppression is over.)

Meaning 3 A channel of an N-IO I/O module (N-IO node 1, unit 1, slot 2, channel 3 in the above example) recovered from an error, and the chattering alarm suppression expired because the time to chattering recovery notice has elapsed. (This is a recovery message of No. 4125.)

Printing example 4 SCS0101 IOM Channel Recover NODE 01 SLOT 02 CH 03 (Chattering suppression is over.)

Meaning 4 A channel of an FIO I/O module (FIO node 1, unit 1, slot 2, channel 3 in the above example) recovered from an error, and the chattering alarm suppression expired because the time to chattering recovery notice has elapsed. (This is a recovery message of No. 4125.)

No.4127

Message name Setting PASSWD FB to ON

Printing example SCS0101 TAG001 PASSWD FB Set to ON (Instance = PASSWD001)

Meaning PASSWD FB (PASSWD001 in the above example) that corresponds to the tag name (TAG001 in the above example) was set to ON (active) by operation from the HIS.

No.4128

Message name Setting PASSWD FB to OFF

Printing example SCS0101 TAG001 PASSWD FB Set to OFF (Instance = PASSWD001)

Meaning PASSWD FB (PASSWD001 in the above example) that corresponds to the tag name (TAG001 in the above example) was inactivated (reset to OFF) by operation from the HIS.

No.4129

Message name GPS interface unit error

Printing example SCS0101 GPS Interface Unit Error (RIGHT CPU)

Meaning A CPU module (right side in the above example) detected a GPS unit error or time synchronization error.

Cause The following causes may be considered.

- Problem in the cable connecting the GPS unit and the GPS interface unit.
- Failure of the GPS interface unit

Action Check to see if a cable connecting the GPS unit and the GPS interface unit is disconnected or cut. Also, check to see if a terminator is connected to the ends of the cable. If everything is in place, replace the GPS interface unit.

Note If this message is displayed while the time synchronization method is V net time synchronization, the CPU module may be faulty.

No.4130

Message name Recovery of GPS interface unit

Printing example SCS0101 GPS Interface Unit Recover (RIGHT CPU)

Meaning Time synchronization of the GPS unit detected by CPU module (right side in the above example) is recovered. (This is a recovery message of No. 4129.)

No.4131

Message name Communication module lock

Printing example 1 SCS0101 Communication Module All Inputs/Outputs Locked NODE 01 SLOT 02

Printing example 2 SCS0101 Communication Module All Inputs Locked NODE 01 SLOT 02

Printing example 3 SCS0101 Communication Module All Outputs Locked NODE 01 SLOT 02

Printing example 4 SCS0101 Safety Subsystem Communication Module All Inputs Locked NODE 01 SLOT 02

Meaning The communication module was locked by operation from the SENG. The message varies depending on the locked range (inputs and outputs, inputs only or outputs only). The location of the communication module (FIO node 1, slot 2 in the above example) is also included in the message.

Remark Forcing function, subsystem communication, safety subsystem communication

Note Be sure to cancel the lock of the communication module that was locked.

No.4132

Message name Cancellation of Communication module lock

Printing example 1 SCS0101 Communication Module All Inputs/Outputs Unlocked NODE 01 SLOT 02

Printing example 2 SCS0101 Communication Module All Inputs Unlocked NODE 01 SLOT 02

Printing example 3 SCS0101 Communication Module All Outputs Unlocked NODE 01 SLOT 02

Printing example 4 SCS0101 Safety Subsystem Communication Module All Inputs Unlocked NODE 01 SLOT 02

Meaning The lock of the communication module was cancelled by operation from the SENG. The message varies depending on the locked range (inputs and outputs, inputs only or outputs only). The location of the communication module (FIO node 1, slot 2 in the the above example) is also included in the message.

Remark Forcing function, subsystem communication, safety subsystem communication

No.4133

Message name Information of a diagnosis error in the received data of SCS Link Transmission.

Printing example SCS0101 SCS Link Transmission Receive Error Stn(SCS)=05 Code = 5041-8000

Meaning A diagnosis error has been found in the received data of SCS Link Transmission. The source station number (such as 05) and the station type (SCS in the above example) that sent the Link Transmission are indicated in the message text. The station type indicated in the message is the station type defined on the SCS Link Transmission builder.

Cause The following causes may be considered. Check the error codes for more detail.

- Stop or restart the sender station
- Problem in the communication path
- The definition of the SCS Link Transmission builder may contain errors.

Remark SCS Link Transmission

Error code The first four digits are an error code, and the next four digits are a cause code. The error detail can be found from the descriptions of both the codes.

The error code represents the type of error. The table explains each error code and the action you can take to fix the error.

Table 2.1-4 Message No. 4133 - Error Code List

Code (hexadecimal)	Description	Action
5041	No data received within the reception interval timeout value.	Check the sender SCS and its communication path.
5042	Time diagnosis found an error.	
5043	Communication protocol error (internal error)	Record the message content and report to Yokogawa's service department.

The cause code represents the event that caused the problem and is logical OR of the following codes.

Table 2.1-5 Message No. 4133 - Cause Code List

Code (hexadecimal)	Errors	Description	Presumed Cause
8000	No response	Communication stopped and data no longer arrived.	Communication error, or the sender station stopped or unable to send outputs.
2000	CRC error in delay-related diagnosis information	The CRC code of delay-related diagnosis information is not correct.	Temporary communication error
1000	CRC error in communication data	The CRC code of SCS Link Transmission data is not correct.	Temporary communication error, or SCS Link Transmission builder definition may contain [Type] error.
0400	Equalization error of delay-related diagnosis information	Communication for acquiring delay-related diagnosis information stopped.	Communication was interrupted or the sender station is stopped.
0100	Address error	Illegal station number	The application may contain errors, or the setting in the database is inconsistent with the setting of dipswitches.
0040	Transmission delay occurred	Communication was updated later than the transmission delay timeout time.	Communication delay

Continues on the next page

Table 2.1-5 Message No. 4133 - Cause Code List (Table continued)

Code (hexa-decimal)	Errors	Description	Presumed Cause
0020	Time diagnosis error of the sender	Time diagnosis error occurred in the sender, so that this date/time may not be correct.	Time diagnosis error of the sender
0010	Time diagnosis error of the receiver	Time diagnosis error occurred in the receiver, so that this date/time may not be correct.	Time diagnosis error of the receiver
0008	Illegal scan cycle	The detected scan cycle is an illegal value 0.	Internal error

No.4134

Message name Information of a diagnosis error recovery in the received data of SCS Link Transmission.

Printing example SCS0101 SCS Link Transmission Receive Recover Stn(SCS)=05

Meaning The diagnosed reception error of SCS link transmission has been recovered. The source station number (such as 05) and the station type (SCS in the above example) are indicated in the message text. The station type indicated in the message is the same station type defined on the SCS Link Transmission builder.

(This is a recovery message of No. 4133.)

Cause The following causes may be considered.

- Recovery of the sender station
- Recovery of the communication path
- The errors in the SCS Link Transmission definition have been removed.

Remark SCS Link Transmission

No.4135

Message name SCS Link Transmission data lock

Printing example SCS0101 SCS Link Transmission Data Locked Stn(SCS)=02

Meaning The reception/transmission data for SCS Link Transmission (in the above example, data received from station 2) were locked. The (SCS) in the message text indicates the station type defined on the SCS Link Transmission builder.

Remark Forcing function, SCS Link Transmission

Note Be sure to cancel the lock of the station that was locked.

No.4136

Message name Cancellation of SCS Link Transmission data lock

Printing example SCS0101 SCS Link Transmission Data Unlocked Stn(SCS)=02

Meaning The lock of reception/transmission data for SCS Link Transmission (in the above example, data received from station 2) was cancelled. The (SCS) in the message text indicates the station type defined on the SCS Link Transmission builder.

Remark Forcing function, SCS Link Transmission

No.4137

Message name Number of Locked Stations in SCS Link Transmission Exceeded

Printing example SCS0101 Number of Locks about SCS Link Transmission Exceeds the Limit = 3

Meaning The number of locked stations exceeded the limit (3 in the above example), which is defined in SYS_FORCE_ LT FB as the number of stations allowed for forcing.

Cause Operation from the SENG to lock too many stations.

Action Cancel SCS Link Transmission locks for some SCS.

Remark Forcing function, SCS Link Transmission, SYS_FORCE_LT FB

Note You should not lock stations beyond the limit.

No.4138

Message name Recovery from exceeded number of locked stations in SCS Link Transmission

Printing example SCS0101 Number of Locks about SCS Link Transmission Within the Limit = 3

Meaning The number of locked stations fell within the limit (3 in the above example), which is defined in SYS_FORCE_ LT FB as the number of stations allowed for forcing. (This is the recovery message of No.4137.)

Cause Operation from the SENG.

Remark Forcing function, SCS Link Transmission, SYS_FORCE_LT FB

No.4139

Message name Inter-SCS Safety Communication data lock

Printing example SCS0101 Inter-SCS Safety Communication Data Locked Dom=01 Stn=02

Meaning The Inter-SCS Safety Communication data received from a producer SCS (in the above example, station 2 in domain 1) were locked.

The message for a lock of the local station (data produced by the station are locked) is also output in the same format, showing its own domain number and station number.

Remark Forcing function, Inter-SCS Safety Communication

Note Be sure to cancel the lock of the station that was locked.

No.4140

Message name Cancellation of Inter-SCS Safety Communication data lock

Printing example SCS0101 Inter-SCS Safety Communication Data Unlocked Dom=01 Stn=02

Meaning The lock of Inter-SCS Safety Communication data received from a producer SCS (in the above example, station 2 in domain 1) was cancelled.

The message of cancellation for the lock of local station (data produced by the station are locked) is also output in the same format, showing its own domain number and station number.

Remark Forcing function, Inter-SCS Safety Communication

No.4141

Message name Number of locked stations in Inter-SCS Safety Communication exceeded

Printing example SCS0101 Number of Locks about Inter-SCS Safety Communication Exceeds the Limit = 3

Meaning The number of locked stations exceeded the limit (3 in the above example), which is defined in SYS_FORCE_ BD FB as the number of stations allowed for forcing.

Cause Operation from the SENG to lock too many stations

Action Cancel Inter-SCS Safety Communication locks for some SCS.

Remark Forcing function, Inter-SCS Safety Communication, SYS_FORCE_BD FB

Note You should not lock stations beyond the limit.

No.4142

Message name Recovery from exceeded number of locked stations in Inter-SCS Safety Communication

Printing example SCS0101 Number of Locks about Inter-SCS Safety Communication Within the Limit = 3

Meaning The number of locked stations fell within the limit (3 in the above example), which is defined in SYS_FORCE_ BD FB as the number of stations allowed for forcing. (This is the recovery message of No.4141.)

Cause Operation from the SENG

Remark Forcing function, Inter-SCS Safety Communication, SYS_FORCE_BD FB

No.4143

Message name Start of automatic scan period extension

Printing example SCS0101 Scan Period Extended from the Original Scan Period 100ms to 200ms

Meaning Automatic extension of the scan period of the application logic execution started. (In the above example, the original scan period of 100 ms was extended to 200 ms.)

Cause The application caused heavy load on the SCS.

Remark SYS_SCANEXT FB, automatic scan period extension

No.4144

Message name Cancellation of automatic scan period extension

Printing example SCS0101 Scan Period Recovered to the Original Scan Period 100ms

Meaning Automatic extension of the scan period of the application logic execution is cancelled. (In the above example, the scan period recovered to its original period of 100 ms.)

Cause The load on the SCS caused by the application was reduced.

Remark SYS_SCANEXT FB, automatic scan period extension

No.4145

Message name Abnormal calculation occurred

Printing example 1 SCS0101 Calculation Error (XXXXXX) Program=PG01

Printing example 2 SCS0101 Calculation Error (XXXXXX) Program=PG01 FU/FB=UFB01

Meaning Abnormal calculation occurred in the application logic.

XXXXXX indicates the type of abnormal calculation. The types are as follows:

Div by Zero :	Division by zero
Access to the Outside of Array :	Access to the outside of an array
FPU Overflow :	Overflow in the floating-point calculation
Cast Overflow :	Overflow in casting

At “Program=”, the name of the program (POU name) where the abnormal calculation occurred is indicated. If the abnormal calculation occurred in a user-defined FU/FB, the POU name of that FU/FB is indicated at “FU/FB=.”

Cause Error in the application

Remark SYS_CERR FB

No.4146

Message name Recovery from abnormal calculation

Printing example 1 SCS0101 Calculation Recover (XXXXXX) Program=PG01

Printing example 2 SCS0101 Calculation Recover (XXXXXX) Program=PG01 FU/FB=UFB01

Meaning Indicates a recovery from the abnormal calculation occurred in the application logic.

XXXXXX indicates the type of abnormal calculation. The types are as follows:

Div by Zero :	Division by zero
Access to the Outside of Array :	Access to the outside of an array
FPU Overflow :	Overflow in the floating-point calculation
Cast Overflow :	Overflow in casting

At “Program=”, the name of the program (POU name) where the abnormal calculation occurred is indicated. If the abnormal calculation occurred in a user-defined FU/FB, the POU name of that FU/FB is indicated at “FU/FB=.”

Cause The error in the application was corrected.

Remark SYS_CERR FB

No.4151

Message name Information of retainable data initialization

Printing example SCS0101 Retain Data Initialized

Meaning Retainable data have been initialized.

Cause

- Database with different CRC codes or generation time was offline-downloaded to the SCS.

- NVRAM (nonvolatile memory) has been initialized.

Action Set the setting values of the external communication function blocks with data retaining function again.

Remark Data retaining function, external communication function blocks with data retaining function (ECWR_B, ECWR_I, ECWR_R), ACCUM FB, AGA_R FB

No.4152

Message name Online change of scan period

Printing example SCS0101 Scan Period Changed to 200ms

Meaning The scan period of the application logic was changed by online change download.

Cause Operation from the SENG

Remark Online change download

No.4153

Message name Information of Inter-SCS Safety Communication data lock time-up

Printing example SCS0101 Inter-SCS Safety Communication Data Lock Elapsed the Specified Period = 08:00:00

Meaning Inter-SCS Safety Communication lock exceeded the time limit (8 hours in the above example) specified in SYS_FORCE_BD FB.

Action Check whether all Inter-SCS Safety Communication locks have been cancelled and cancel unnecessary locks.

Remark Forcing function, Inter-SCS Safety Communication, SYS_FORCE_BD FB

No.4154

Message name Information of forced cancellation of Inter-SCS Safety Communication data locks

Printing example SCS0101 All Inter-SCS Safety Communication Data Unlocked.

Meaning Locks of all the Inter-SCS Safety Communication data (reception/transmission) in the station were forcibly cancelled.

Cause Locks of all the Inter-SCS Safety Communication data were cancelled by using the SYS_FORCE_BD FB.

Remark Forcing function, Inter-SCS Safety Communication, SYS_FORCE_BD FB

No.4155

Message name Information of SCS Link Transmission status change.

Printing example SCS0101 SCS Link Transmission Data Status Set to TRUE Old=FALSE Stn(SCS)=03

Meaning The data status of SCS Link Transmission (such as from station 03) has been changed (For an example, changed from FALSE to TRUE). The (SCS) in the message text indicates the station type defined on the SCS Link Transmission builder.

Remark Forcing function

No.4156

Message name Information of SCS Link Transmission definition change

Printing example SCS0101 SCS Link Transmission Definition Changed

Meaning SCS Link Transmission definitions were changed by online change download.

Cause Online change download was executed from the SENG.

No.4157

Message name Information of SCS Link Transmission wiring change

Printing example SCS0101 SCS Link Transmission Wiring Changed

Meaning SCS Link Transmission wirings were changed by online change download.

Cause Online change download was executed from the SENG.

No.4158

Message name Information of SCS Link Transmission lock time-up

Printing example SCS0101 SCS Link Transmission Data Lock Elapsed the Specified Period = 08:00:00

Meaning SCS Link Transmission lock continued exceeding the time limit (8 hours in the above example) specified in SYS_FORCE_LT FB.

Action Check whether all SCS Link Transmission locks have been cancelled, and cancel unnecessary locks.

Remark Forcing function, SCS Link Transmission, SYS_FORCE_LT FB

No.4159

Message name Information of forced cancellation of SCS Link Transmission locks

Printing example SCS0101 All SCS Link Transmission Data Unlocked

Meaning Locks of all the locked SCS Link Transmission were forcibly cancelled.

Cause Locks of all SCS Link Transmission were cancelled by operation using SYS_FORCE_LT FB.

Remark Forcing function, SCS Link Transmission, SYS_FORCE_LT FB

No.4160

Message name Invalid password for Manual Operation FB

Printing example SCS0101 TAG001 Specified Invalid Password

Meaning The password string specified for Manual Operation FB (MOB_21, MOB_11, MOA) from the HIS is invalid.

Cause The password entered from the HIS and the password set in Manual Operation FB did not match.

Action	Enter the correct password for Manual Operation FB again.
Remark	Manual Operation FB (MOB_21, MOB_11, MOA)

No.4161

Message name	Information of Output IOM Shutdown
Printing example 1	SCS0101 All Output IOM Shutdown
Meaning 1	All output channels in the station were shut down by SYS_ALLSD.
Printing example 2	SCS0101 IOM Output Shutdown N-IO NODE 01 UNIT 01 SLOT 02
Meaning 2	The specified N-IO output module was shut down by SYS_N_IOSD. The location of the N-IO output module (N-IO node 1, unit 1, slot 2 in the above example) is also included in the message.
Printing example 3	SCS0101 Output IOM Shutdown NODE 01 SLOT 02
Meaning 3	The specified FIO output module was shut down by SYS_IOSD. The location of the output module (FIO node 1, slot 2 in the above example) is included in the message.
Remark	SYS_ALLSD, SYS_IOSD, SYS_N_IOSD

No.4162

Message name	Information of communication I/O definition change
Printing example 1	SCS0101 Communication Definition Changed
Printing example 2	SCS0101 Safety Subsystem Communication Definition Changed
Meaning	The communication I/O definitions of the communication module were changed by online change download.
Cause	Online change download was executed from the SENG.
Remark	Subsystem communication, safety subsystem communication

No.4163

Message name	Information of communication I/O wiring change
Printing example 1	SCS0101 Communication I/O Wiring Changed
Printing example 2	SCS0101 Safety Subsystem Communication I/O Wiring Changed
Meaning	The communication I/O wirings were changed by online change download.
Cause	Online change download was executed from the SENG.
Remark	Subsystem communication, safety subsystem communication

No.4164

Message name	Information of disabling security level change
Printing example	SCS0101 Security Levels Change Disabled
Meaning	The security level change of the SCS by a password-authenticated operation performed from SENG is disabled.
Remark	SYS_SEC_CTL FB

No.4165

Message name Information of enabling security level change

Printing example SCS0101 Security Levels Change Enabled

Meaning The security level change of the SCS by a password-authenticated operation performed from SENG is enabled.

Remark SYS_SEC_CTL FB

No.4166

Message name Information of communication module lock time-up

Printing example SCS0101 Communication Module Lock Elapsed the Specified Period = 08:00:00

Meaning The communication module lock continued exceeding the time limit (8 hours in the above example) specified in SYS_FORCE_SC FB.

Action Check whether all communication module locks have been cancelled, and cancel unnecessary locks.

Remark Forcing function, subsystem communication, SYS_FORCE_SC FB

No.4167

Message name Information of forced cancellation of communication module locks

Printing example SCS0101 All Communication Modules Unlocked

Meaning Locks of all communication modules were forcibly cancelled.

Cause Locks of all communication modules were cancelled by operation using SYS_FORCE_SC FB.

Remark Forcing function, subsystem communication, SYS_FORCE_SC FB

No.4168

Message name Information of tag name change by online change download

Printing example SCS0101 Online Change Download Tag Name = TAG001 Changed

Meaning The tag name (TAG001 in the above example) of FB was changed by online change download.

Cause Online change download was executed from the SENG.

Remark Password FB (PASSWD), override FB (OVR_B, OVR_I, OVR_R, OVR_IB, OVR_IR, GOV_B, and GOV_IB), manual operation FB (MOB_21, MOB_11, MOB_RS, and MOA), and FB for fire and gas devices (HSDTR and GASDTR)

No.4169

Message name NVRAM diagnosis error

Printing example SCS0101 RIGHT NVRAM Diagnosis Error

Meaning An error was detected during diagnosis of NVRAM (nonvolatile memory) in a CPU module (right side in the above example).

Cause NVRAM may be faulty.

Action Replace the applicable CPU module.

No.4170

Message name Flash memory diagnosis error

Printing example SCS0101 RIGHT Flash Memory Diagnosis Error

Meaning An error was detected during self-diagnosis of flash memory in a CPU module (right side in the above example).

Cause Part of data stored in flash memory was destroyed, or flash memory may be faulty.

Action If the SCS is in a single CPU module configuration, the SCS will not be able to start when this CPU restarts next time. It is necessary to change the CPU module right away.

If the SCS is configured with redundant CPU modules, the control will switch to the other module after detecting this error, and the module where the error occurs is restarted as a standby module.

If the error is caused by damage to the data in the flash memory, data in the control side will be copied to the standby module where the error occurs, and that module will then recover from abnormal to normal status.

If the error is caused by the physical damage of the flash memory, this system alarm will occur even after the damaged CPU is switched to standby. Under this circumstance, it is necessary to change the damaged CPU module.

No.4172

Message name Information of resource change by online change download

Printing example SCS0101 Online Change Download Resource Changed (Total POU=10)

Meaning The resource was changed by online change download. The resource defines total number of POU (10 in the above example).

Cause Online change download was executed from the SENG.

Action Check and confirm that the total number of POU indicated in this message is equal to the total number of POU indicated by Database Validity Check Tool.

No.4173

Message name Completion of writing to flash memory

Printing example SCS0101 Writing XXXXXX to Flash Memory Succeeded

Meaning Writing to flash memory in a CPU module was normally completed.

XXXXXX: Indicates the data written. The items of the data are as follows.

Security Password :	Security password
System Database :	System database
Integration Database :	Integration database
Variable Database :	Variable database
Difference Data :	Difference data

Cause When online change download from SENG to SCS was executed or the password was changed, data was normally written to flash memory.

No.4174

Message name Failed to write to flash memory

Printing example SCS0101 Writing XXXXX to Flash Memory Error

Meaning Write data error was detected during check at flash memory write in a CPU module.

XXXXXX: Indicates the data attempted to be written. The items of the data are as follows.

Security Password :	Security password
System Database :	System database
Integration Database :	Integration database
Variable Database :	Variable database
Difference Data :	Difference data

Cause Flash memory may be faulty.

Action If the SCS is in a single CPU module configuration, the CPU module continues the operation even if this error occurs. However, the SCS will not start properly when this CPU module restarts next time. It is necessary to change the CPU module as soon as possible.

On a dual-redundant CPU module configuration SCS, if this writing error to flush memory occurs on one of the CPU modules, the CPU module will be failed and operation is continued with the other CPU module. It is necessary to change the failed CPU module right away. If writing to the flash memories in both CPU modules fails, the SCS will not be able to start when the CPU restarts. Under this circumstance, it is necessary to change both CPU modules right away.

Remark Flash memory diagnosis

No.4175

Message name Failed to update external communication data

Printing example SCS0101 External Data Refresh Failed

Meaning The SCS has failed to update external communication data. This data is referenced in communications with CENTUM stations and Modbus, so when this error occurs, data will not be updated in those stations.

Cause The CPU processing time allocated for the external communication function processing was not sufficient. As a result, processing to update the external communication data is not performed.

Action Reduce the communication load on the SCS. If this error occurs regularly, review the balance between the application logic amount and the scan period.

No.4177

Message name Information of SCS security level change

Printing example SCS0101 Security Level Changed to 1

Meaning The security level of the SCS was changed (1 in the above example).

Cause The security level of the SCS was changed. The security level can be changed from the SENG or SYS_SECURE FB.

Note Be sure to revert the security level to “2.”

No.4178

Message name Information of security level time-up

Printing example SCS0101 Security Level = 1 Elapsed the Specified Period = 08:00:00

Meaning The security level is set to “1” for the duration exceeding the time limit (8 hours in the above example) specified in SYS_SECURE FB.

Cause The security level has not been reverted.

Action Revert the security level to “2.”

Remark SYS_SECURE FB

Note When the security level is “0,” the message is not generated.

No.4179

Message name Information of communication I/O module output enable operation

Printing example SCS0101 Communication Modules Output Enabled

Meaning The communication modules are enabled for output.

Remark I/O Channel Status dialog box, SYS_STAT_SC FB

Note This message is irrelevant to enabling the output of output modules. You can be notified of the output enable operation for output modules by Message No. 4181.

No.4180

Message name Information of password change

Printing example SCS0101 Security Level = 1 Password was Changed

Meaning The password for the SCS security level (1 in the above example) was changed.

Cause The password was changed from the SENG.

Note The message of No. 4173 is also generated after this alarm.

No.4181

Message name Information of output enable operation

Printing example SCS0101 Output Enabled

Meaning The output enable operation for the SCS was performed from the SENG.

When all the output module’s output channels go into “output-enabled” state, the SCS’s operating mode changes to “Running.”

Remark I/O Channels Status dialog box, SYS_STAT_FB

No.4182

Message name Information of FIO output module start operation

Printing example SCS0101 IOM Started NODE 01 SLOT 02

Meaning An FIO output module (FIO node 1, slot 2 in the above example) was started from the SENG.

Remark SCS State Management window

No.4183

Message name Request to upload SOE to SENG

Printing example SCS0101 SOE Save Request

Meaning This notification prompts to upload the event information collected on the SCS to SENG.

Cause This message is generated every time 12,000 events have occurred on the SCS.

Action Start SOE Viewer on SENG and upload events from SCS.

Remark SOER function

Note This system alarm is generated even if SOE Viewer is started periodically. Events can be uploaded from the SCS by starting SOE Viewer and displaying the latest event.

No.4184

Message name Notification on saving SOE trip signal file in SCS

Printing example SCS0101 SOE Trip Signal File No.= 01 Saved

Meaning The SOE trip signal file (No. 01 in the above example) was saved in SCS.

Action Start SOE Viewer on SENG and upload the events in the file.

Remark SOER function

Note When uploading the events is complete, the trip signal files need to be reset. Up to two trip signal files can be held in the SCS. The trip signal files can be reset by starting the Message Cache Tool and initializing the trip information.

No.4185

Message name Information of variable value change

Printing example 1 SCS0101 Variable Set to 10.0 Old = 5.0 Variable = VAR001

Printing example 2 SCS0101 Variable Set to TRUE Old = FALSE Variable = VAR001 NODE 1 SLOT 2

Printing example 3 SCS0101 Variable Set to TRUE Old = FALSE Variable = VAR001 N-IO NODE 01 UNIT 01 SLOT 02 CH 03

Printing example 4 SCS0101 Variable Set to TRUE Old = FALSE Variable = VAR001 NODE 1 SLOT 2 CH 3

Printing example 5 SCS0101 Variable Set to TRUE Old = FALSE Variable = VAR001 Stn=02 No=025

Meaning The value of the variable (VAR001 in the above example) was changed from the SENG. For a communication I/O, a variable corresponds to the communication module location (FIO node 1, slot 2 in printing example 2) is also included in the message. For an I/O variable, the channel location corresponding to the variable (N-IO node 1, unit 1, slot 2, channel 3 in printing example 3, and FIO node 1, slot 2, channel 3 in printing example 4) is also included in the message.

The VAR001 in the above printing example 5 is the instance name of the function block that accesses the data of SCS Link Transmission. The related station number and bit number are also printed.

Remark Forcing function

No.4186

Message name Information of lock time-up

Printing example SCS0101 Lock Elapsed the Specified Period = 08:00:00

Meaning Lock continued exceeding the time limit (8 hours in the above example) specified in SYS_FORCE FB.

Action Check whether all locks have been cancelled, and cancel unnecessary locks.

Remark Forcing function, SYS_FORCE FB

No.4187

Message name Information of forced cancellation of locks

Printing example SCS0101 All Variables Unlocked

Meaning Locks of all variables were forcibly cancelled.

Cause Locks of all variables were cancelled by operation using SYS_FORCE FB.

Remark Forcing function, SYS_FORCE FB

No.4188

Message name Start of online change download

Printing example SCS0101 Online Change Download (System Database) Start

Meaning Online change download to the system database was started.

Remark Download function

No.4189

Message name Completion of online change download

Printing example SCS0101 Online Change Download (System Database) Complete

Meaning Online change download to the system database was normally completed.

Remark Download function

No.4190

Message name Online change download error

Printing example SCS0101 Online Change Download (System Database) Error = 5340-0001

Meaning Online change download to the system database ended with an error.

Cause/Action Causes and actions vary depending on the error code.

Table 2.1-6 Message No. 4190 - Error Causes and Actions

Error code	Cause	Action
5340-****	The security level stays “2.”	Set the security level to “1” and then execute online change download again.
Others	Internal error	Record the message content and report to Yokogawa’s service department.

No.4191

Message name Completion of I/O definition rewriting

Printing example 1 SCS0101 IOM Definition Changed N-IO NODE 01 UNIT 01 SLOT 02

Meaning 1 I/O definition was changed by online change download to the system database. The location of the I/O module (N-IO node 1, unit 1, slot 2 in the example) is also included in the message.

If the numbers following "SLOT" and "UNIT" are 00, it means that the node definition information has been changed. The node definition information is changed when you do the following:

- Change comments of the node
- Operation such as addition and deletion of the I/O modules including addition/deletion of the node

If only the number following "SLOT" is 00, it means that the unit definition information has been changed. The unit definition information is changed when you do the following:

- Change base plates
- Operation such as addition and deletion of the I/O modules

Printing example 2 SCS0101 IOM Definition Changed NODE 01 SLOT 02

Meaning 2 I/O definition was changed by online change download to the system database. The location of the I/O module (FIO node 1, slot 2 in the example) is also included in the message.

If the number following "SLOT" is 00, it means that the node definition information has been changed. The node definition information is changed when you do the following:

- Change comments of the node
- Add or delete I/O modules of the node
- Change slots of the I/O modules of the node
- Change the model of the I/O modules of the node

No.4192

Message name Information of override state time-up

Printing example SCS0101 Override Elapsed the Specified Period = 08:00:00

Meaning Override continued exceeding the time limit (8 hours in the above example) specified in SYS_OVR FB.

Action Check whether overrides were released, and release unnecessary overrides.

Remark SYS_OVR FB

No.4193

Message name Information of forced release of all overrides

Printing example SCS0101 All Overrides Released

Meaning The overrides for all variables were forcibly released.

Cause The overrides for all variables were forcibly released by operation using SYS_OVR FB.

Remark SYS_OVR FB

No.4194

Message name Information of override enabled state time-up

Printing example SCS0101 Enabled OVR FB Elapsed the Specified Period = 08:00:00

Meaning The override enabled state continued exceeding the time limit (8 hours in the above example) specified in SYS_OVR FB.

Cause Check override FB in the override enabled state, and release unnecessary override enabled state.

Remark SYS_OVR FB

No.4195

Message name Information of communication I/O data status change

Printing example SCS0101 Communication Data Status Set to TRUE Old = FALSE NODE 01 SLOT 02 Definition 001

Meaning The value of data status of communication I/O (FIO node 1, slot 2, communication definition 1 in the above example) was changed (from FALSE to TRUE in the above example) from the SENG.

Remark Forcing function

No.4196

Message name Invalid password for PASSWD FB

Printing example SCS0101 TAG001 PASSWD FB Specified Invalid Password

Meaning The password string specified for PASSWD FB from the HIS is invalid.

Cause The password entered from the HIS and the password set in PASSWD FB did not match.

Action Specify the correct password for PASSWD FB and enter it again.

Remark PASSWD FB

No.4197

Message name Information on active PASSWD FB time-up

Printing example SCS0101 Activated PASSWD FB Elapsed the Specified Period = 10:00:00

Meaning PASSWD FB has been active exceeding the time limit (10 hours in the above example) specified in SYS_PSWD.

Action Deactivate PASSWD FB that is not required to be active.

Remark SYS_PSWD FB

No.4198

Message name Information on forced reset of PASSWD FB

Printing example SCS0101 All PASSWD FB Reset to OFF

Meaning The outputs of all active PASSWD FBs were forcibly set to OFF.

Cause The outputs of all active PASSWD FBs were forcibly inactivated (reset to OFF) by operation using SYS_PSWD FB.

Remark SYS_PSWD FB

No.4199

Message name Override communication error

Printing example SCS0101 TAG001 Override Communication Error (Instance = OVR001)

Meaning Despite an attempt to operate override on the FB OVR001 (in the above example) with the tag name TAG001 (in the above example) from HIS, communication error has occurred.

Cause A temporary communication error occurred, and the SCS detected the problem of the communication data.

Action Execute override operation again.

Remark Override FB

No.4201

Message name Information of node maintenance port enable operation

Printing example SCS0101 NODE Maintenance Port Enable N-IO NODE 01

Meaning An operation to enable the maintenance port of the N-IO node (1 in the above example) of the safety control station (station name = SCS0101) was performed.

No.4202

Message name Information of node maintenance port disable operation

Printing example SCS0101 NODE Maintenance Port Disable N-IO NODE 01

Meaning An operation to disable the maintenance port of the N-IO node (1 in the above example) of the safety control station (station name = SCS0101) was performed.

No.4203

Message name Information of node maintenance port disable operation for all N-IO nodes

Printing example SCS0101 NODE Maintenance Port Disable All N-IO NODE

Meaning An operation to disable the maintenance ports of all N-IO nodes of the safety control station (station name = SCS0101) was performed.

No.4205

Message name Information of node maintenance port enabled state

Printing example SCS0101 NODE Maintenance Port Enabled N-IO NODE 01

Meaning The maintenance port of the N-IO node (1 in the above example) of the safety control station (station name = SCS0101) was enabled.

No.4206

Message name Information of node maintenance port disabled state

Printing example SCS0101 NODE Maintenance Port Disabled N-IO NODE 01

Meaning The maintenance port of the N-IO node (1 in the above example) of the safety control station (station name = SCS0101) was disabled.

No.4207

Message name Information of HSDTR FB or GASDTR FB reset operation

Printing example 1 SCS0101 TAG001 Reset Requested (Reset ID = 1)

Meaning 1 An operation to reset the HSDTR FB or GASDTR FB that corresponds to the tag name (TAG001 in the above example) was performed from HIS. For a reset operation for GASDTR FB, information in the parentheses “(Reset ID = 1)” is not displayed.

Printing example 2 SCS0101 DTR001 Reset Requested (Reset ID = 1)

Meaning 2 An operation to reset HSDTR FB or GASDTR FB (DTR001 in the above example) was performed from an external switch. For a reset operation for GASDTR FB, information in the parentheses “(Reset ID = 1)” is not displayed.

Remark HSDTR FB, GASDTR FB

No.4208

Message name Communication error in HSDTR FB or GASDTR FB reset operation

Printing example SCS0101 TAG001 Reset Request Communication Error

Meaning An operation to reset the HSDTR FB or GASDTR FB that corresponds to the tag name (TAG001 in the above example) was performed from HIS, but resulted in a communication error.

Cause A temporary communication error occurred, and the SCS detected the problem of the communication data.

Action Perform the reset operation again.

Remark HSDTR FB, GASDTR FB

No.4209

Message name Safety subsystem communication error

Printing example SCS0101 SS-SCOM Error FIO NODE 01 SLOT 01 PORT 01 CG01 Code=5A01

Meaning An error occurred in the indicated fire and gas communication (in the above example, FIO node 1, slot 1, port 1, communication group name CG01).

Communication group name is a name that is set in the Communication Group column of the Safety Communication I/O Editor.

Cause This message is generated when the following errors are detected: Check the error codes for more detail.

- Failure of fire and gas devices, such as gas detectors (GS01)
- The safety control station received abnormal safety data from a fire and gas device.
- The fire and gas device could not receive safety data from the safety control station properly.
- Response to a request from the safety control station to the fire and gas device could not be received.
- Initialization of fire and gas communication started due to online change downloading for the SCS.

Action Take an action based on the error message. Message No.4211 may be generated at the same time. If generated, also take action for No.4211.

Remark Safety subsystem communication

Note If a recovery message is not generated even after removing the possible cause of the error, the alarm is active for another cause. Check the cause of error in the IOM Report, and remove it.

Error code The error code represents the type of error. The following table describes the error codes.

Table 2.1-7 Message No. 4209 - Error Code List

Code (hexa-decimal)	Error	Cause	Action
5A01	A fire and gas device failed.	A fire and gas device failed.	Replace the fire and gas device.
5A02	A problem occurred in the fire and gas communication path, and the safety control station received bad safety data from the fire and gas device.	The safety layer of the fire and gas device is not operating properly.	Contact the manufacturer of the fire and gas device.

Continues on the next page

Table 2.1-7 Message No. 4209 - Error Code List (Table continued)

Code (hexa-decimal)	Error	Cause	Action
5A03	A problem occurred in the fire and gas communication path, and the fire and gas device could not receive safety data from the safety control station.	• A problem occurred in the communication path between the safety control station and fire and gas device. • There is an error in the PROFIsafe setting of ProSafe-RS or the fire and gas device.	• Check the communication path between the safety control station and fire and gas device. • Check the PROFIsafe setting of ProSafe-RS or the fire and gas device. • If a message No.4211 is generated at the same time, the cause may be an abnormality in the communication path. Refer to the action for message No.4211 as well.
5A04	A problem occurred in the fire and gas communication path, and the response to a request from the safety control station to the fire and gas device could not be received.	• A problem occurred in the communication path between the safety control station and fire and gas device. • There is an error in the PROFIsafe setting of ProSafe-RS or the fire and gas device. • The safety layer of the fire and gas device is not operating properly.	• Check the communication path between the safety control station and fire and gas device. • Check the PROFIsafe setting of ProSafe-RS or the fire and gas device. • Contact the manufacturer of the fire and gas device.
5A05	The safety control station started initialization of fire and gas communication.	Online change download was performed for the safety control station after changing definitions regarding fire and gas communication.	If the recovery alarm is not generated even after the expected PROFIsafe initialization time has elapsed, check the error code in the IOM Report and take an action based on the error code.

No.4210

Message name Recovery from safety subsystem communication error

Printing example SCS0101 SS-SCOM Recover FIO NODE 01 SLOT 01 PORT 01 CG01

Meaning Fire and gas communication error has been recovered. (This is a recovery message for No. 4209.)

Remark Safety subsystem communication

No.4211

Message name Safety subsystem communication path error

Printing example SCS0101 SS-SCPATH Error FIO NODE 01 SLOT 01 PORT 01 CG01 Code=A3B0

Meaning An error occurred in the communication path between the indicated fire and gas communication module and the safety subsystem device (in the above example, FIO node 1, slot 1, port 1, communication group name CG01).

Communication group name is a name that is set in the Communication Group column of the Safety Communication I/O Editor.

Cause This message is generated when the following errors are detected:

- Error in the definition information downloaded in the fire and gas communication module
- Error in the communication with PROFINET IO-Device
- Error in Field Wireless Management Station (YFGW410)
- Error in Field Wireless Access Point (YFGW510)

Action Take an action based on the error message. Message No.4209 may be generated at the same time. If generated, also take action for No.4209.

Remark Safety subsystem communication

Note If a recovery message is not generated even after removing the possible cause of the error, the alarm is active for another cause. Check the cause of error in the IOM Report, and remove it.

Error code The error code represents the type of error. The table explains each error code and the action you can take to fix the error.

Table 2.1-8 Message No. 4211 - Error Code List

Code (hexa-decimal)	Error	Cause	Action
A393	BAD_BY_DEVICE received from PROFINET IO-Device	Error occurred in PROFINET IO-Device.	Refer to the manual of PROFINET IO-Device.
A394	BAD_BY_SLOT received from PROFINET IO-Device	Error occurred in PROFINET IO-Device.	Refer to the manual of PROFINET IO-Device. This error code is not reported when the PROFINET IO-Device is YFGW410.
A395	BAD_BY_SUBSLOT received from PROFINET IO-Device	When the PROFINET IO-Device is YFGW410, possible causes are as follows: • GS01 has not joined the wireless network, or GS01 is not sending data to YFGW410. • There is an error in the PROFINET setting of ProSafe-RS or YFGW410. When the PROFINET IO-Device is not YFGW410: • Refer to the manual of PROFINET IO-Device.	Take the following actions when the PROFINET IO-Device is YFGW410: • Refer to the manual of YFGW410. • Check the PROFINET setting of ProSafe-RS or YFGW410. When the PROFINET IO-Device is not YFGW410: • Refer to the manual of PROFINET IO-Device.
A396	Status other than BAD_BY_DEVICE, BAD_BY_SLOT, and BAD_BY_SUBSLOT received from PROFINET IO-Device	• Error occurred in S2LP131. • A problem occurred in the communication path between S2LP131 and PROFINET IO-Device. • Error occurred in PROFINET IO-Device.	• Replace the S2LP131. • Check the communication path between S2LP131 and PROFINET IO-Device. • Refer to the manual of PROFINET IO-Device.
A3B0	No response from PROFINET IO-Device	• A problem occurred in the communication path between S2LP131 and PROFINET IO-Device. • There is an error in the PROFINET setting of ProSafe-RS or PROFINET IO-Device.	• Check the communication path between S2LP131 and PROFINET IO-Device. • Check the PROFINET setting of PROFINET IO-Device.

Continues on the next page

Table 2.1-8 Message No. 4211 - Error Code List (Table continued)

Code (hexa-decimal)	Error	Cause	Action
A3B7	Invalid data type set in Safety Communication I/O Editor	Invalid data type is set in the Data Type column of the Safety Communication I/O Editor.	Check the data type that is set in the Data Type column of the Safety Communication I/O Editor.
A3E9	YFGW410 control right switchover	Error occurred in the active YFGW410 of redundant YFGW410.	Check the previously active YFGW410, which is now in the standby state. Note that, for a control right switchover, a recovery message is generated after two seconds.
A3EA	Error in the GW1 system of YFGW410	Error occurred in the GW1 system of YFGW410.	Check the YFGW410 for the GW1 system. For the action to be taken for YFGW410, refer to the manual or YFGW410.
A3EB	Error in the GW2 system of YFGW410	Error occurred in the GW2 system of YFGW410.	Check the YFGW410 for the GW2 system. For the action to be taken for YFGW410, refer to the manual or YFGW410.
A3EC	Unstable active/standby state of YFGW410	Error occurred in redundant YFGW410.	Check the YFGW410. For the action to be taken for YFGW410, refer to the manual or YFGW410.
A3F0	YFGW510 error	• YFGW510 failed. • A problem occurred in the communication path between YFGW510 and YFGW410. • There is an error in the YFGW510 setting.	• Replace the YFGW510. • Check the communication path between YFGW510 and YFGW410. • Refer to the manual of YFGW510.

No.4212

Message name Recovery from safety subsystem communication path error

Printing example SCS0101 SS-SCPATH Recover FIO NODE 01 SLOT 01 PORT 01 CG01

Meaning The communication between the indicated fire and gas communication module and the safety subsystem device recovered. (This is a recovery message for No. 4211.)

Remark Safety subsystem communication

No.4213

Message name Safety subsystem communication I/O lock

Printing example SCS0101 Safety Subsystem Communication I/O Locked NODE 01 SLOT 02 CG01

Meaning Specified fire and gas communication I/O (in the above example, FIO node 1, slot 2, communication group name CG01) was locked by operation from the SENG. Communication group name is a name that is set in the Communication Group column of the Safety Communication I/O Editor.

Remark Forcing function, safety subsystem communication

Note Be sure to unlock the safety subsystem communication I/O definition that was locked.

No.4214

Message name Cancellation of safety subsystem communication I/O lock

Printing example SCS0101 Safety Subsystem Communication I/O Unlocked NODE 01 SLOT 02 CG01

Meaning Specified fire and gas communication I/O (in the above example, FIO node 1, slot 2, communication group name CG01) was unlocked by operation from the SENG.

Communication group name is a name that is set in the Communication Group column of the Safety Communication I/O Editor.

Remark Forcing function, safety subsystem communication

No.4215

Message name Number of safety subsystem communication I/O locks exceeded

Printing example SCS0101 Number of Locks about Safety Subsystem Communication I/O Exceeds the Limit = 3

Meaning The total number of locked safety subsystem communication I/O exceeded the limit count (3 in the above example) specified in SYS_FORCE_SF FB.

Cause This is an operation from the SENG. The number of locks is too many.

Action Unlock some safety subsystem communication I/O.

Remark Forcing function, safety subsystem communication, SYS_FORCE_SF FB

Note Unlock safety subsystem communication I/O within the limit count.

No.4216

Message name Recovery from exceeded number of safety subsystem communication I/O locks

Printing example SCS0101 Number of Locks about Safety Subsystem Communication I/O Within the Limit = 3

Meaning The total number of locked safety subsystem communication I/O fell below the limit count (3 in the above example) specified in SYS_FORCE_SF FB. (This is a recovery message for No. 4215.)

Cause This is an operation from the SENG.

Remark Forcing function, safety subsystem communication, SYS_FORCE_SF FB

No.4217

Message name Safety subsystem communication I/O data status change

Printing example SCS0101 Safety Subsystem Communication I/O Status Set to TRUE Old = FALSE NODE 01 SLOT 02 CG01

Meaning Data status value of fire and gas communication I/O (in the above example, FIO node 1, slot 2, communication group name CG01) was changed from the SENG. (Changed from FALSE to TRUE in the above example.)

Communication group name is a name that is set in the Communication Group column of the Safety Communication I/O Editor.

Remark Forcing function, safety subsystem communication

No.4219

Message name Safety subsystem communication I/O lock time-up

Printing example SCS0101 Safety Subsystem Communication I/O Lock Elapsed the Specified Period = 08:00:00

Meaning Fire and gas communication I/O lock continued exceeding the time limit (8 hours in the above example) specified in SYS_FORCE_SF FB.

Action Check whether all fire and gas communication I/O locks have been canceled, and cancel unnecessary locks.

Remark Forcing function, safety subsystem communication, SYS_FORCE_SF FB

No.4220

Message name Forcible cancellation of all safety subsystem communication I/O locks

Printing example SCS0101 All Safety Subsystem Communication I/O Unlocked

Meaning Locks of all safety subsystem communication I/O were forcibly canceled.

Cause Locks of all safety subsystem communication I/O were canceled by operation using SYS_FORCE_SF FB.

Remark Forcing function, safety subsystem communication, SYS_FORCE_SF FB

No.4221

Message name Alarm for the operation data reset switch of CPU module

Printing example SCS0101 RIGHT Operation Data Reset Switch Alarm

Meaning The operation data reset switch of the CPU module (right side in the above example) in the safety control station (station name = SCS0101) remains in “RESET” status.

Cause The operation data reset switch is in “RESET” status.

Action Change the status of operation data reset switch to “HOLD”.

No.4222

Message name Recovery from alarm for the operation data reset switch of CPU module

Printing example SCS0101 RIGHT Operation Data Reset Switch Recover

Meaning The operation data reset switch of the CPU module (right side in the above example) in the safety control station (station name = SCS0101) became in “HOLD” status. (This is a recovery message of No.4221.)

3. Details of Output Messages in Common with CENTUM

This section describes the details of output messages used in common with CENTUM.

3.1 Safety Control Station Error Occurrence and Recovery Messages (Message Numbers 0001 through 0094)

This section describes the messages relating to errors that occur on the safety control station. There are messages relating to occurrences of errors and recoveries from errors.

No.0001

Message name Reset start of safety control station

Printing example SCS0101 RIGHT Manual Reset Start

Meaning A CPU module (right side in the above example) of the safety control station (station name = SCS0101) was reset and started.

Cause Start operation from the SENG or from the front switch of the CPU module

No.0003

Message name Safety control station automatic reset start

Printing example SCS0101 RIGHT Automatic Reset Start

Meaning An error occurred in the displayed CPU module (right side in the above example) of the safety control station (station name=SCS0101), which caused the safety control station to be automatically reset started.

Cause CPU module is faulty.

No.0005

Message name Power ON initial cold start of safety control station

Printing example SCS0101 Power ON (Cold Start)

Meaning The safety control station (station name = SCS0101) performed the initial cold start processing after it was powered ON.

Cause Recovery from power failure

Note The safety control station always performs the initial cold start processing after recovery from power failure.

No.0009

Message name Transfer of control right of safety control station

Printing example SCS0101 Control Transfer

Meaning A transfer of control right occurred in the redundant safety control station (station name = SCS0101).

Cause

- The CPU module on one side was stopped.
- An error occurred in the CPU module on one side.

Action The CPU module on the standby side takes over control. Replace the CPU module that was stopped.

No.0011

Message name Fail information of safety control station

Printing example SCS0101 RIGHT Fail (xxxxxxxx Code= yyyy yyyy yyyy yyyy)

Meaning A CPU module (right side in the above example) of the safety control station (station name = SCS0101) failed.

Cause The causes are indicated by “causes (xxxxxxxx)” and a code. For more information, see the table.

Action If the CPU module that stopped is operating normally after automatic restart, continue operation. If the CPU module that stopped does not recover after automatic restart, replace the CPU module.

Table 3.1-1 Message No. 0011 - Causes

Item	Causes xxxxxxxx	Code (hex 16 digits) yyyy yyyy yyyy yyyy	Description	Auto restart
CPU module stopped	SW STOP	-	Stop by operation of the front switch of the CPU module	No
	V STOP		Stop instruction via control bus	No
	DC FAIL	-	Stop due to power failure	No
		(*1)	Transient error detection	Yes
	CPU DOWN	(*1)	An error occurred during CPU module error check.	Yes
	SELF-STOP		Stop after software detected an error	No
	UN-KNOWN		Stop due to unknown cause	No
	RESTART		Restart after software detected an error	Yes

*1: Refer to the table “Cause and Solution for Each Code.”

Table 3.1-2 Cause and Solution for Each Code

Code (hex 16 digits) yyyy yyyy yyyy yyyy	Cause	Solution
0001 yyyy 0001 00yy	This message occurs when there is a mismatch between the outputs of the two main processors in the processor module.	If this error message is displayed, report the display contents of causes (xxxxxxxx) and the code to Yokogawa’s service department. If the processor module restarts and returns to normal after issuing this alarm, continue to use the module.
0001 yyyy 0002 y000	This message occurs when there is no output from one main processor when comparing the output between two main processors in the processor module.	
0100 yyyy 0000 2000 0001 yyyy 0000 A000	This message occurs when a transient error due to a soft error is detected in the processor module.	
0000 5090 yyyy yyyy	Division by zero occurred when running the application logic.	Check to see if the application logic contains division by zero or not, and correct the application logic if it contains.
0000 5091 yyyy yyyy	The application logic is trying to access an array datum beyond the scope of the array.	Check the application and find out which logic program is accessing the out-of-range array data and correct the error.

Continues on the next page

Table 3.1-2 Cause and Solution for Each Code (Table continued)

Code (hex 16 digits) yyyy yyyy yyyy yyyy	Cause	Solution
0000 50A9 yyyy yyyy	The database inconsistence is detected. It may be caused by restarting the SCS without releasing the brake point.	Run offline downloading.
4000 3BF1 0255 8082 (*1)	The firmware (Revision F4) in the CPU module is too old to support the system with Optical ESB Bus Repeater modules.	For a system that contains Optical ESB Bus Repeater modules, the firmware of CPU with the proper revision number should be used.
4000 3BF1 yyyy yyyy	An error has been detected in the I/O unit of the CPU module. SCSV1-S : There may be a failure in the I/O unit of the CPU module. SCSP2-S, SCSP3-S, SCSL2-S: There may be a failure in the I/O unit of the CPU module or the I/O communication is posing heavy load on the CPU.	If one of the redundant CPU modules has stopped, message No. 0787 is generated at the same time. Refer to the explanation of message No. 0787.
0000 5010 yyyy yyyy	The CPU model and station model are inconsistent.	Match the CPU model and station model with each other.
FFFF 000B 0000 000F	The calculation in a running application overflowed.	Check the application and find out what caused the calculation overflow and then modify it.
Others	Others	If this error message is displayed, report the display contents of causes (xxxxxxxx) and the code to Yokogawa's service department.

*1: This code is not generated in SCSP2-S, SCSP3-S, and SCSL2-S.

No.0013

Message name AC power supply failure of safety control station

Printing example SCS0101 AC Fail (Time 05.02.01 18:45)

Meaning AC power of the safety control station (station name = SCS0101) failed and was then recovered. The date and time indicated are when the power failed. This message is output after the power is recovered.

Cause The voltage of AC power supply dropped, or a power failure occurred.

Note The SCS has been initialized and then started.

No.0015

Message name Self-diagnosis error of clock inside CPU module

Printing example SCS0101 RTC Diagnose Error Code=0001

Meaning An error was detected during self-diagnosis of the clock inside the safety control station (station name = SCS0101).

Code=0001: Check pattern mismatch

Code=0002: Inappropriate date/time value

Code=0003: Date/time not updated

Action Replace the CPU module.

No.0017

Message name ROM checksum error of CPU module

Printing example SCS0101 RIGHT ROM Sum Check Error

Meaning A ROM checksum error was detected in the indicated CPU module (right side in the above example) of the safety control station (station name = SCS0101).

Action Replace the CPU module.

No.0021

Message name Internal task error of safety control station

Printing example SCS0101 Internal Error TASK=TSK1 Code=100 Error=1000 - E0F0

Meaning An error state was detected during the execution of a task (TSK1 in the above example) in the safety control station (station name = SCS0101). “TASK”, “Code” and “Error” indicate detailed error information.

Cause This is a software problem.

Action Report the message content to Yokogawa’s service department.

No.0023

Message name Mapping block fatal error

Printing example SCS0101 Block TAG001 Return Error 8E04 and stop

Meaning An execution disabled error was detected during the execution of a mapping block (TAG001 in the above example) in the safety control station (station name = SCS0101).

Cause There is a problem in the integration DB. “Error” indicates detailed error information.

Action Report the message content to Yokogawa’s service department.

No.0025

Message name Function control word error

Printing example SCS0101 No Block Control Word for Block Type=1804

Meaning The internal program that corresponds to the block type code of the safety control station (station name = SCS0101) does not exist. “Type” indicates detailed internal information.

Cause This is an internal error at task initialization.

Action Report the message content to Yokogawa’s service department.

No.0027

Message name Mapping block record information error

Printing example SCS0101 TAG001 Block Bad Record No = 3

Meaning There is a bad record in the mapping block (TAG001 in the above example) of the safety control station. “No” indicates the bad record number in the database.

Cause The mapping block and the record block number do not match.

Action Report the block type and record number where an error occurred to Yokogawa's service department.

Note Do not perform online change download after this alarm occurred.

No.0033

Message name Online downloading abnormal end

Printing example SCS0101 Online Download Error Code=9402 - 0000

Meaning Online change download of the safety control station (station name = SCS0101) ended with an error. "Error Code" indicates detailed internal information.

Cause/Action Perform the appropriate action based on the cause that is indicated for the detailed error codes.

Table 3.1-3 Message No. 0033 - Error Code List

Code	Error Contents	Cause	Action
9402 9403 9404 9405	Online change downloading abnormal end	The SCS was reset and started during online change download.	Execute offline download.
Others	Internal error	Internal error	Report the display content of the code to Yokogawa's service department.

No.0041

Message name Safety control station fan alarm

Printing example SCS0101 Fan (SCU N1) Alarm

Meaning A cooling fan of the safety control station (station name = SCS0101) is abnormal. One of the following items is displayed in the parentheses in the above example.

SCU N1: Left side fan

SCU N2: Right side fan

Cause The cooling fan stopped or its revolution is abnormal.

Action Replace the failed fan unit.

Remark HKU function

No.0042

Message name Recovery from safety control station fan alarm

Printing example SCS0101 Fan(SCU N1) Recover

Meaning The cooling fan of the safety control station (station name = SCS0101) recovered. The content in the parentheses in the above example is the same as message No. 0041. (This is a recovery message of No. 0041.)

Remark HKU function

No.0043

Message name Safety control station temperature alarm

Printing example SCS0101 Temperature(RIGHT BATTERY) Alarm

Meaning This is a temperature rise alarm of the safety control station (station name = SCS0101). One of the following items is displayed in the parentheses in the above example.

RIGHT BATTERY:	Battery of the right side CPU module
LEFT BATTERY:	Battery of the left side CPU module
AIR IN:	Air inlet
AIR OUT:	Air outlet

Cause The CPU module temperature exceeded the specified value.

Action After checking the operation of the cooling fans, report to Yokogawa's service department as necessary.

Remark HKU function

No.0044

Message name Recovery from safety control station temperature alarm

Printing example SCS0101 Temperature(RIGHT BATTERY) Recover

Meaning The temperature of the safety control station (station name = SCS0101) recovered normally. The content in the parentheses in the above example is the same as message No. 0043. (This is a recovery message of No. 0043.)

Remark HKU function

No.0045

Message name Power supply module alarm of safety control station

Printing example SCS0101 RIGHT PSU Alarm

Meaning The power supply module of a CPU node (right side in the above example) of the safety control station (station name = SCS0101) is abnormal.

Cause Power supply module failure

Action Replace the applicable power supply module.

No.0046

Message name Recovery from power supply module alarm of safety control station

Printing example SCS0101 RIGHT PSU Recover

Meaning The power supply module of a CPU node (right side in the above example) of the safety control station (station name = SCS0101) recovered normally. (This is a recovery message of No. 0045.)

No.0047

Message name Battery alarm of CPU module

Printing example SCS0101 RIGHT Battery Alarm

Meaning An error occurred on the battery of the CPU module (right side in the above example) in the safety control station (station name = SCS0101.)

Cause If the CPU module has a battery ON/OFF switch, the battery failed or the switch was turned “OFF.” If the CPU module does not have a battery ON/OFF switch, the battery failed.

Action If the CPU module has a battery ON/OFF switch, check that the switch is turned “ON.” If the above message is generated even though the switch is “ON”, replace the battery.

If the CPU module does not have a battery ON/OFF switch, replace the battery.

Remark HKU function

No.0048

Message name Recovery from battery alarm of CPU module

Printing example SCS0101 RIGHT Battery Recover

Meaning A battery of the CPU module (right side in the above example) of the safety control station (station name = SCS0101) recovered normally. (This is a recovery message of No. 0047.)

Remark HKU function

No.0053

Message name Safety control station cabinet temperature alarm

Printing example SCS0101 Temperature Alarm N-IO NODE 01 Temp(HI)

Meaning The temperature in the cabinet storing N-IO node 1 of the safety control station (station name = SCS0101) is out of the normal range. One of the following items is displayed in the parentheses in the above example.

HI: High Alarm

LO: Low Alarm

Action After checking the cooling fans of the applicable cabinet, report to Yokogawa’s service department as necessary.

No.0054

Message name Recovery from safety control station cabinet temperature alarm

Printing example SCS0101 Temperature Recover N-IO NODE 01 Temp(HI)

Meaning The temperature in the cabinet of the safety control station recovered normally. The content in the parentheses in the above example is the same as message No. 0053. (This is a recovery message of No. 0053.)

No.0055

Message name Information of same frame reception in online change download communication

Printing example SCS0101 Received Same Online Download Frame Code=1 Frame=3

Meaning The same communication frame was received twice during the execution of online change download. “Code” and “Frame” indicate detailed internal information.

Action Execute online change download again.

No.0057

Message name Information of online change download error

Printing example SCS0101 Online Download Error Call Code=9601 - 0000 Data=91,0,0,0

Meaning An error occurred during the execution of online change download of the safety control station (station name = SCS0101). “Code” and “Data” indicate detailed internal information.

Cause This error occurs if error data cannot be saved on the safety control station side.

Action It is necessary to determine an action to take based on the “Code” and “Data” information. Report the display contents of “Code” and “Data” to Yokogawa’s service department.

Note Do not execute online change download after this alarm occurred.

No.0059

Message name Information of recovery from node power failure

Printing example 1 SCS0101 N-IO NODE Power On N-IO NODE 02

Printing example 2 SCS0101 FIO NODE Power On FIO NODE 02

Meaning A node (2 in the above example) of the safety control station (station name = SCS0101) recovered from power failure.

No.0063

Message name ESB bus error

Printing example SCS0101 FIO-BUS Fail FIO BUS No.1

Meaning An error occurred on one side (No. 1 in the above example) of the ESB buses of the safety control station (station name = SCS0101).

With the SCSP3 and SCSL2, this message does not appear.

Cause This is an ESB bus error on one side.

Action ESB Bus Interface module, ESB bus coupler module, or ESB bus failure may be considered as an error cause. Take appropriate action in the following:

- Check to see if the ESB bus cables are connected correctly. Check for incorrect connection or bad connection of the cables, or check the terminators of the bus.
- Check to see if one ESB Bus Interface module is causing a bus error of the entire buses according to the following procedure.

  Pull out the ESB bus connector of each ESB Bus Interface module that connects to the corresponding bus, one by one, from the node.

Wait for two to three seconds, and if “Recover” is not printed, insert the ESB bus connector again, and pull the bus connector of the next node.

If “Recover” is printed, the bus connector of the ESB Bus Interface module that was pull out at that time is faulty, so replace that module.

- If no recovery was made even after the bus connectors of all nodes were pulled out, the ESB bus coupler module may be faulty. In such a case, replace the ESB bus coupler module.
- If no recovery was still made, press the [START/STOP] button on the CPU module’s front panel on the control side twice, and switch the control right of the CPU module. Replace the CPU module after restarting.

If the bus does not recover even after these operations, the error may be related to the ESB bus cable (T-shape connector and so on). Replace the ESB bus cable.

Note This message is generated if all safety node units become abnormal.

This message is also generated if all safety node units become abnormal in a system configuration that includes the Optical ESB Bus Repeater module. However, if all safety node units directly connected to ESB bus coupler module without going through the Optical Repeater module become abnormal in this system configuration, this message is not generated so long as any safety node unit connected via the Optical Repeater module is normal.

No.0064

Message name Normal recovery of ESB bus

Printing example SCS0101 FIO-BUS Recover FIO BUS No.1

Meaning The ESB bus indicated in the message recovered normally. (This is a recovery message of No. 0063.)

No.0065

Message name Failure of N-ESB bus module or ESB Bus Interface module

Printing example 1 SCS0101 NBS Fail N-IO NODE 02 NBS RIGHT

Meaning 1 An error occurred in an N-ESB bus module (right side in the above example) of an N-IO node (2 in the above example) of the safety control station (station name = SCS0101).

Cause 1 One of the following causes may be considered.

- N-ESB bus module is faulty.
- Connection route to the N-ESB bus module has problem.
- For the N-I/O nodes that are connected via Optical ESB Bus Repeater modules, the Optical ESB Bus Repeater module related hardware such as ESB Bus Repeater module or Fiber-optic cable is faulty.

Action 1 Replace the N-ESB bus module and check to see if the problem is resolved. If not, other locations may be abnormal. If all N-IO nodes connected to the N-ESB bus of the same system are abnormal, the N-ESB bus coupler module or N-ESB bus cable may be faulty. If all the N-IO nodes routed through the Optical ESB Bus Repeater related devices become abnormal, the Optical ESB Bus Repeater module or Fiber-optic cable may be faulty. Moreover, if the Optical ESB Bus Repeater modules are mounted in the unit for mounting the Optical ESB Bus Repeater modules, the error may be caused by the failure of a power supply module of the unit for mounting the Optical ESB Bus Repeater

modules. Identify the abnormal location from the message, LED ON status, etc., and replace the applicable device.

Printing example 2 SCS0101 SBS Fail FIO NODE 02 SBS RIGHT

Meaning 2 An error occurred in an ESB Bus Interface module (right side in the above example) of an FIO node (2 in the above example) of the safety control station (station name = SCS0101).

Cause 2 One of the following causes may be considered.

- ESB Bus Interface module becomes abnormal.
- Connection route to the ESB Bus Interface module becomes abnormal.
- For the safety node units that are connected via Optical ESB Bus Repeater modules, the Optical ESB Bus Repeater related module related hardware (Optical ESB Bus Repeater module, Fiber-optic cable, etc.) is faulty.

Action 2 If no ESB bus error message is output, the ESB Bus Interface module may be faulty. Replace the applicable ESB Bus Interface module. If all the safety node units routed through the Optical ESB Bus Repeater related devices become abnormal and all the safety node units routed through such Optical Repeater become abnormal, error may have occurred in the Optical ESB Bus Repeater module or Fiber-optic cable. Moreover, if the Optical ESB Bus Repeater modules are mounted in the unit for mounting the Optical ESB Bus Repeater modules, the error may be caused by the failure of a power supply module of the unit for mounting the Optical ESB Bus Repeater modules. Identify the abnormal location from the message, LED ON status, etc., and replace the applicable device.

If all nodes connected to the SCSP3 and SCSL2 (except for the N-IO nodes connected via the N-ESB bus) are abnormal, the ESB Bus Interface module, ESB bus coupler module, or ESB bus may be faulty. Execute the action under No. 0063.

No.0066

Message name Normal recovery of N-ESB bus module or ESB Bus Interface module of node

Printing example 1 SCS0101 NBS Recover N-IO NODE 02 NBS RIGHT

Meaning 1 An N-ESB bus module (right side in the above example) of an N-IO node (2 in the above example) of the safety control station (station name = SCS0101) recovered normally. (This is a recovery message of No. 0065.)

Printing example 2 SCS0101 SBS Recover FIO NODE 02 SBS RIGHT

Meaning 2 An ESB Bus Interface module (right side in the above example) of an FIO node (2 in the above example) of the safety control station (station name = SCS0101) recovered normally. (This is a recovery message of No. 0065.)

No.0067

Message name Failure of power supply of node

Printing example 1 SCS0101 PSU Fail N-IO NODE 02 PSU 1 (POWER OFF)

Meaning 1 An error occurred in a power supply unit (1 in the above example) of an N-IO node (2 in the above example) of the safety control station (station name = SCS0101). One of the following items is displayed in the parentheses in the above printing example 1.

POWER OFF: The power supply unit stopped functioning.

OVERVOLTAGE: The output voltage of the power supply unit is too high.

Cause 1 Faulty power supply unit of the node interface unit

Action 1 The actions corresponding to the items shown in ( ) are as follows:

POWER OFF:	The power supply of the applicable node interface unit may be faulty or the power feed system may be faulty. Check the condition of the power supply unit of the applicable node interface unit and the power feed system.
OVER-VOLTAGE:	Power supply unit of the applicable node interface unit is faulty. Replace the power supply unit.

Printing example 2 SCS0101 PSU Fail FIO NODE 02 PSU RIGHT

Meaning 2 An error occurred in a power supply module (right side in the above example) of an FIO node (2 in the above example) of the safety control station (station name = SCS0101).

Cause 2 Faulty power supply module of the FIO node

Action 2 Replace the power supply module of the applicable node.

Note 2 If I/O module or N-ESB bus coupler module is defined to the CPU node, this message is generated as FIO node 1 when an error occurs in a PSU for the CPU node.

No.0068

Message name Normal recovery of power supply of a node

Printing example 1 SCS0101 PSU Recover N-IO NODE 02 PSU 1 (POWER OFF)

Meaning 1 The power supply unit of the node interface unit of the N-IO node indicated in the message (2 in the above example) recovered normally. The content in the parentheses in printing example 1 is the same as message No. 0067. (This is a recovery message of No. 0067.)

Printing example 2 SCS0101 PSU Recover FIO NODE 02 PSU RIGHT

Meaning 2 The power supply module of the FIO node indicated in the message (2 in the above example) recovered normally. (This is a recovery message of No. 0067.)

No.0069

Message name Error before database download to I/O module

Printing example SCS0101 IOM Download Error = A701

Meaning Database download to the I/O module (IOM) can not be started.

Cause/Action The cause and action vary depending on the content of the error.

- A701

  This message occurs when attempting to download to an IOM while another IOM download is still running. Only one IOM download can be performed at one time, so please wait for the other IOM download to complete before running an IOM download operation again.

- A72C

  Automatic IOM download to a standby side I/O module is running. This error occurs if IOM download to the same I/O module is manually execu-

ted from the SENG or online change download is executed to make changes in I/O parameter settings while automatic IOM download is running.

- 5135

  This message occurs when attempting to download to an IOM even though it is running normally.

- Others

  Report the error display content to Yokogawa's service department.

No.0073

Message name Error in the F-SB bus connecting the N-IO I/O unit and node interface unit

Printing example SCS0101 IOM-BUS Error N-IO NODE 01 UNIT 01 BUS No.01

Meaning An error occurred in the F-SB bus connecting the N-IO I/O unit (1 in the above example) of N-IO node 1 of the safety control station (station name = SCS0101) and the node interface unit.

Action The F-SB bus may be faulty. Check to see if the F-SB bus is connected properly. Check the F-SB bus for incorrect connection, bad connection, etc.

No.0074

Message name Normal recovery of the F-SB bus connecting the N-IO I/O unit and node interface

Printing example SCS0101 IOM-BUS Recover N-IO NODE 01 UNIT 01 BUS No.01

Meaning The F-SB bus connecting the N-IO I/O unit (1 in the above example) of N-IO node 1 of the safety control station (station name = SCS0101) and the node interface unit recovered from a communication error (this is a recovery message of No. 0073).

No.0081

Message name Failure of I/O module

Printing example 1 SCS0101 IOM Fail N-IO NODE 01 UNIT 01 SLOT 01 Code = 5101

Printing example 2 SCS0101 IOM Fail FIO NODE 01 SLOT 01 Code = 5101

Meaning An error occurred in the I/O module or N-ESB bus coupler module. The message includes the module position (N-IO node 1, unit 1, slot 1 in printing example 1; FIO node 1 (CPU node), slot 1 in printing example 2).

Cause Refer to the error code descriptions.

Action Replace the applicable I/O module.

Table 3.1-4 Message No. 0081 - AIO/DIO Module and N-ESB bus coupler module Errors

Error code	Description of error
5101	The communication between the CPU and an I/O module or the CPU and an N-ESB bus coupler module encountered a no-response error. This error is caused either by an abnormality of the module or the communication route to the module.

Continues on the next page

Table 3.1-4 Message No. 0081 - AIO/DIO Module and N-ESB bus coupler module Errors (Table continued)

Error code	Description of error
5102	The model of the I/O module or N-ESB bus coupler module defined on the SENG does not match the model of the module that is actually mounted. Check the model of the module.
5103	The setting information defined on the SENG and the I/O module setting information do not match. Execute IOM download.
5104	A hardware error of the I/O module was detected. Check detailed error causes in the IOM Report.
5105	A setting error of the I/O module. Check detailed error causes in the IOM Report (field side connector disconnection, field power supply/wiring problem, etc.)
5106	The I/O module recovered from an error state. Check detailed error causes in the IOM Report.
5107	The error that actuated the output shutoff switch occurred. Check detailed error causes in the IOM Report. When this error occurred, start the I/O module after recovering from the error.
5108, 5109, 5111, 5112, 5113, 511D, 511E	A communication data check error was detected between the CPU and the I/O module. A failure of the I/O module or a problem of the communication path up to the I/O module may be the cause. Error codes 5108, 5109, 511D, and 511E are displayed only for N-IO.
5114, 5115	An error was detected in the redundant control part of the I/O module. Replace the I/O module. However, when two I/O modules in single configuration are changed to dual-redundant configuration and online change download is performed, this error may be detected if a connector cable is plugged to only one of the two modules. In this case, plug the connector cables to both modules. Recovery from this error is notified with system alarm message No.0082 “Normal recovery of I/O module”, and there is no need to replace the I/O modules.
5116, 5117	An I/O module error was detected. Replace the I/O module.
5118	An SCS internal error (SCS database error) was detected.

Table 3.1-5 Error Details of Message No.0081 – Errors on ALR111/ALR121/ALE111 Modbus Slave and ALE111 DNP3 Slave

Error Code	Cause/Action
C580	The communication between CPU and I/O modules encounters a no-response error. This error may be caused by the I/O module abnormality, communication route abnormality or an abnormality other than C581 to C583 depicted.
C581	The communication program is not downloaded to the communication module. Run IOM download.
C582	The communication program in the communication module is not the program for Modbus slave communication/DNP3 slave function. Run IOM download.
C583	The physically installed communication module shows a different model name from the communication module defined in SENG. Check the model of the communication module.

Table 3.1-6 Message No.0081 - ALR111/ALR121/ALE111 Subsystem Communication and S2LP131 Safety Subsystem Communication Errors

Error Code	Cause/Action
A33D	No response from the communication module due to communication module abnormality. Replace the communication module.
A33E	Error occurred in the communication route between CPU and node.
C581	The communication program is not downloaded to the communication module. Run IOM download.

Continues on the next page

Table 3.1-6 Message No.0081 - ALR111/ALR121/ALE111 Subsystem Communication and S2LP131 Safety Subsystem Communication Errors (Table continued)

Error Code	Cause/Action
C582	The communication program in the communication module is not the program for the communication defined in SENG. Run IOM download.
C583	The physically installed communication module shows a different model name from the communication module defined in SENG. Check the model of the communication module.
C585	Error is found by self-diagnosis. Replace the communication module.
C58A	The PROFINET definition defined by PROFINET Configurator and the PROFINET definition in the fire and gas communication module do not match. Run IOM download to the communication module.
C58D	An error was detected in the communication board of the fire and gas communication module. Replace the communication module.
C58E	A device with the same IP address as a communication module exists in the same subnet. After resolving the duplicate IP address, execute IOM download to the communication module.
C598	The communication module is reset due to online change download or IOM download.
C599	Downloading to database.
C59A	Downloading communication program.
C5C1	Error found after resetting the communication module. Replace the communication module.
C5C6	Failed to download the communication program. Waiting time for shifting to the downloading mode of the communication program exceeded the time limit. Start IOM download again.
C5C7	Failed to download the communication program. Processing time for downloading the communication program exceeded the time limit. Start IOM download again.
C5E2	Communication module encountered an error and stopped. Replace the communication module.

No.0082

Message name Normal recovery of I/O module

Printing example 1 SCS0101 IOM Recover N-IO NODE 01 UNIT 01 SLOT 01

Printing example 2 SCS0101 IOM Recover FIO NODE 01 SLOT 01

Meaning The I/O module or N-ESB bus coupler module recovered normally. The message includes the module position (N-IO node 1, unit 1, slot 1 in printing example 1; FIO node 1, slot 1 in printing example 2). (This is a recovery message of No. 0081.)

No.0083

Message name I/O module database error occurred

Printing example 1 SCS0101 IOM Configuration Error N-IO NODE 01 UNIT 01 SLOT 01

Printing example 2 SCS0101 IOM Configuration Error FIO NODE 01 SLOT 01

Meaning An error occurred in the I/O module database. The message includes the I/O module position (N-IO node 1, unit 1, slot 1 in printing example 1; FIO node 1, slot 1 in printing example 2).

Cause The database on the I/O module and the database on the SCS do not match. The following causes may be considered.

- IOM download has not been executed.
- IOM failure.

Action If this error occurred after replacing a module or at startup, the database might not have been downloaded to the I/O module. Execute IOM download.

If this error occurred during I/O module operation, the I/O module may be faulty. Replace the I/O module.

No.0085

Message name I/O module communication error occurred

Printing example 1 SCS0101 IOM Communication Error N-IO NODE 01 UNIT 01 SLOT 01 BUS No.01 RIGHT

Meaning 1 A communication error occurred on bus 1 between the right-side node interface unit and the I/O module mounted in slot 1 of unit 1 of N-IO node 1 of the safety control station (station name = SCS0101). (If this error occurs on both buses, an IOM Failure state will result.)

Cause 1 The node interface unit or its base plate may be faulty. If the message is generated for both the right side and left side, either communication interface of the I/O module may be faulty.

Action 1 Replace the applicable node interface unit or its base plate. If the message is generated for both the right side and left side, be sure to replace the applicable I/O module.

Printing example 2 SCS0101 IOM Communication Error FIO NODE 01 SLOT 01 RIGHT

Meaning 2 An error occurred in one of the SB buses (right side in the above example). An error occurred when accessing the I/O module mounted in slot 1 of FIO node 1 in the safety control station (station name = SCS0101).

Cause 2 If this error occurred on all input modules within the same FIO node, an I/O module may be faulty, or the backboard bus of the FIO node may be faulty. Or, an ESB bus (right side in the above example) or an ESB Bus Interface module (right side in the above example) may be faulty, or they may not be connected properly.

Action 2 Report to Yokogawa's service department.

No.0086

Message name Recovery from I/O module communication error

Printing example 1 SCS0101 IOM Communication Recover N-IO NODE 01 UNIT 01 SLOT 01 BUS No.01 RIGHT

Meaning 1 The communication on bus 1 between the right-side node interface unit and the I/O module mounted in slot 1 of unit 1 of N-IO node 1 of the safety control station (station name = SCS0101) recovered. (This is a recovery message of No. 0085.)

Printing example 2 SCS0101 IOM Communication Recover FIO NODE 01 SLOT 01 RIGHT

Meaning 2 Communication recovered from the error with the I/O module mounted in slot 1 of FIO node 1 of the safety control station (station name = SCS0101). (This is a recovery message of No. 0085.)

No.0087

Message name Node error occurred

Printing example 1 SCS0101 NODE Fail N-IO NODE 02

Meaning 1 An error occurred in N-IO node 2 of the safety control station (station name = SCS0101).

Cause 1 One of the following causes may be considered.

- A power failure occurred in the N-IO node, or both of the two N-ESB buses are faulty.
- Both N-ESB bus modules are faulty.
- For the N-I/O nodes connected via Optical ESB Bus Repeater modules, the Optical ESB Bus Repeater related hardware such as Optical ESB Bus Repeater module or Fiber-optic cable is faulty.

Printing example 2 SCS0101 NODE Fail FIO NODE 02

Meaning 2 An error occurred in FIO node 2 of the safety control station (station name = SCS0101).

Cause 2 One of the following causes may be considered.

- A power failure occurred in the safety node unit, or both of the two ESB buses are faulty.
- Both ESB Bus Interface modules are faulty.
- For the safety node units connected via Optical ESB Bus Repeater modules, the Optical ESB Bus Repeater related hardware such as Optical ESB Bus Repeater module or Fiber-optic cable is faulty.

Action Report to Yokogawa's service department.

No.0088

Message name Normal recovery of node

Printing example 1 SCS0101 NODE Recover N-IO NODE 02

Printing example 2 SCS0101 NODE Recover FIO NODE 02

Meaning The node indicated in the message recovered normally. (This is a recovery message of No. 0087.)

No.0089

Message name Subsystem communication error

Printing example SCS0101 SS-COM Error FIO NODE 01 SLOT 01 PORT 01 STN001 Code= A3B0

Meaning A communication error occurred between the indicated communication module and the subsystem.

Cause/Action The error details can be found in the instruction manuals of the connected subsystem. See the manuals for error details.

Or, take an action based on the error message.

Table 3.1-7 Message No. 0089 - Errors from Use of ALR111, ALR121

Code	Error	Cause/Action
A391	Driver Busy	Occurs when sending or receiving.
A392	Communication Line Busy	This message occurs when carrier detection fails due to the CD signal line has been ON for more than the transmission enable monitoring time (*1).
A393	Communication Line Not Ready	This message occurs when, at the time of transmission, the CS signal line or DR signal line has been OFF for more than the transmission enable monitoring time.(*1)
A394	Data size is too large for sending.	
A395	The port for sending is not declared.	
A397	Underrun	
A398	Interval of characters became timeout	This message occurs when the interval of characters exceeds the specified time.
A399	Reception buffer overflow	
A39A	Reception parity error	
A39B	Reception overrun	
A39C	Reception frame error	
A39D	Number of characters beyond range	
A39F	Other errors	
A3B0 to A3FF	Reserved for subsystems	For more information, see the instruction manuals of subsystems.

*1: The transmission-watching timer monitors the waiting time of the transmission line become ready for transmission. When RS is sent, and the waiting time for transmission exceeds the specified time period, the transmission becomes error. The transmission waiting time is normally set to 1000 ms.
The conditions for transmission are as follows:
- CD line off (When CD check is enabled)
- CS (CTS) line on
- DR line on (When DR check is enabled)

Table 3.1-8 Message No. 0089 - Errors from Use of ALE111

Code	Error
A309	Incorrect descriptor for designated socket.
A30D	Unauthorized access
A30E	Socket descriptor address specified in the created socket function is not correct.
A316	Arguments of the function are incorrect
A320	Connection is shutdown when transmitting to the connected socket.
A324	Connection process is in progress following a non-blocking connect request. The connection process will complete after a while.
A325	The previous non-block connect is not completed.
A328	The data size is too large to be sent.
A329	Socket and protocol are not consistent.
A32B	The specified protocol is not supported.
A32D	The function is not supported by the designated socket.
A330	The specified address is already occupied.
A331	0 is specified to the port number.
A333	Cannot reach network from this host.

Continues on the next page

Table 3.1-8 Message No. 0089 - Errors from Use of ALE111 (Table continued)

Code	Error
A335	Connected destination severed the connection.
A338	The socket is already connected
A339	The socket is not connected
A33C	Timeout before connection is established
A33D	Connection is denied by destination.
A3B0 to A3FF	Reserved for each subsystem. For more information, see the instruction manuals of subsystems.

Remark Subsystem communication

No.0090

Message name Subsystem communication recovered

Printing example SCS0101 SS-COM Recover FIO NODE 01 SLOT 01 PORT 01 STN001

Meaning The communication between the indicated communication module and the subsystem recovered from the error.

Remark Subsystem communication

No.0093

Message name CPU node's housekeeping unit error

Printing example SCS0101 RIGHT HKU Error Code=0001

Meaning The CPU node's housekeeping unit of the safety control station (station name = SCS0101) is faulty. "Code" indicates detailed internal information.

Action Report to Yokogawa's service department.

Remark HKU function

No.0094

Message name Normal recovery of CPU node's housekeeping unit

Printing example SCS0101 RIGHT HKU Recover Code=0001

Meaning The CPU node's housekeeping unit of the safety control station (station name = SCS0101) recovered normally. (This is a recovery message of No. 0093.)

Remark HKU function

3.2 Safety Control Station Status Change Related Messages (Message Numbers 0425 through 0480)

This section describes the messages relating to status changes of the safety control station.

No.0425

Message name Start of online upgrade

Printing example SCS0101 Online Upgrade Start

Meaning An online upgrade has been started.

Cause An operation was performed by the online upgrade tool.

Remark Online upgrade function

No.0426

Message name Normal completion of online upgrade

Printing example SCS0101 Online Upgrade Complete

Meaning The online upgrade completed properly.

Cause An operation was performed by the online upgrade tool.

Remark Online upgrade function

No.0427

Message name Online upgrade error

Printing example SCS0101 Online Upgrade Error CODE = 1234 DET = 1234

Meaning The online upgrade ended with an error.

Cause An operation was performed by the online upgrade tool.

Remark Online upgrade function

No.0447

Message name Node maintenance port enabled notification

Printing example SCS0101 N-IO NODE Maintenance Port Enabled

Meaning The maintenance port of the N-IO node of the safety control station (station name = SCS0101) became enabled and the security level of the N-IO node is lowered.

Action When the operation via the maintenance port is finished, access the maintenance port setting for the N-IO from the NIU maintenance port setting tool and disable the port.

No.0448

Message name Node maintenance port disabled notification

Printing example SCS0101 N-IO NODE Maintenance Port Disabled

Meaning The maintenance port of the N-IO node of the safety control station (station name = SCS0101) became disabled.

No.0450

Message name Copy program and database on control side of safety control station to stand-by side

Printing example SCS0101 Copy

Meaning The copying of the program and database on the control side of the safety control station to the standby side has been started.

Cause This message is displayed when the CPU module on the standby side of the safety control station (station name = SCS0101) was started.

No.0451

Message name Information of switching of control side of safety control station

Printing example SCS0101 RIGHT Control

Meaning The CPU module on the right or left side (right side in the above example) of the safety control station (station name = SCS0101) has been set to the control side.

No.0452

Message name Information of switching of standby side of safety control station

Printing example SCS0101 LEFT Stand-By

Meaning The CPU module on the right or left side (left side in the above example) of the safety control station (station name = SCS0101) has been set to the standby side.

No.0455

Message name Node maintenance notification

Printing example SCS0101 NODE Maintenance N-IO NODE 01

Meaning An N-IO node (1 in the above example) of the safety control station (station name = SCS0101) entered the maintenance mode.

Action To cancel the maintenance mode, perform a cancellation operation by using the maintenance tool that is connected to the N-ESB bus module of the applicable node, or unplug the USB cable connecting the maintenance tool.

No.0456

Message name Node maintenance cancellation notification

Printing example SCS0101 NODE Maintenance Release N-IO NODE 01

Meaning The maintenance mode of an N-IO node (1 in the above example) of the safety control station (station name = SCS0101) was canceled.

No.0459

Message name Information of I/O module service side

Printing example 1 SCS0101 IOM In Service N-IO NODE 01 UNIT 01 SLOT 01

Printing example 2 SCS0101 IOM In Service FIO NODE 01 SLOT 01

Meaning One of the redundant I/O modules (N-IO node 1, unit 1, slot 1 in printing example 1; FIO node 1, slot 1 in printing example 2) gained the control right.

No.0460

Message name Information of I/O module out service

Printing example 1 SCS0101 IOM Out Service N-IO NODE 01 UNIT 01 SLOT 01

Printing example 2 SCS0101 IOM Out Service FIO NODE 01 SLOT 01

Meaning One of the redundant I/O modules (N-IO node 1, unit 1, slot 1 in printing example 1; FIO node 1, slot 1 in printing example 2) switched to the standby side or stopped.

No.0471

Message name Normal completion of online change download

Printing example SCS0101 Online Download (Integration Database) Complete

Meaning Online change download to the safety control station has normally been completed.

No.0474

Message name Information of tag list duplicate error

Printing example SCS0101 Tag Duplication Error Tag = TAG001

Meaning A duplicate tag list name exists in the same safety control station.

Action Report to Yokogawa's service department.

No.0475

Message name Start of database download to I/O module

Printing example 1 SCS0101 IOM Download Start N-IO NODE 01 UNIT 01 SLOT 01

In the case of automatic IOM download:

SCS0101 Automatic IOM Download Start N-IO NODE 01 UNIT 01 SLOT 01

Printing example 2 SCS0101 IOM Download Start FIO NODE 01 SLOT 01

In the case of automatic IOM download:

SCS0101 Automatic IOM Download Start FIO NODE 01 SLOT 02

Meaning Database download to the I/O module indicated in the message has been started.

No.0476

Message name Normal completion of database download to I/O module

Printing example 1 SCS0101 IOM Download Complete N-IO NODE 01 UNIT 01 SLOT 01

In the case of automatic IOM download:

SCS0101 Automatic IOM Download Complete N-IO NODE 01 UNIT 01 SLOT 01

Printing example 2 SCS0101 IOM Download Complete FIO NODE 01 SLOT 01

In the case of automatic IOM download:

SCS0101 Automatic IOM Download Complete FIO NODE 01 SLOT 02

Meaning Database download to the I/O module indicated in the message has normally been completed.

No.0477

Message name Database download error to I/O module

Printing example 1 SCS0101 IOM Download Error N-IO NODE 01 UNIT 01 SLOT 01 Error= xxxx

In the case of automatic IOM download:

SCS0101 Automatic IOM Download Error N-IO NODE 01 UNIT 01 SLOT 01 Error= xxxx

Printing example 2 SCS0101 IOM Download Error FIO NODE 01 SLOT 01 Error= xxxx

In the case of automatic IOM download:

SCS0101 Automatic IOM Download Error FIO NODE 01 SLOT 02 Error= xxxx

Meaning An error occurred during database download to the I/O module indicated in the message. “xxxx” indicates an error code.

Cause/Action The error codes are described below. If an error occurs, remove the cause, and execute IOM download again.

If an error other than the following errors occurred, replace the I/O module and execute IOM download again. If other error occurred again, report details to Yokogawa’s service department.

- Error codes for I/O modules other than ALR111, ALR121, ALE111, and S2LP131.

  A701: Downloading for the I/O module is currently being executed.

  3B1B: The I/O module is faulty.

  CFxx: An error was returned from the I/O module.

  CF10: The type of the I/O module does not match.

- Error codes for ALR111, ALR121, ALE111, and S2LP131

  A33D: The CPU module cannot communicate with the communication module.

  A33E: There is an error or fault in the communication path between the CPU module and the communication module. (Node failure, etc.)

  A731: Simultaneous downloading of multiple communication programs was attempted. Multiple communication programs cannot be added by one online change download. If you try to add them simultaneously, A731 error occurs when downloading is attempted

for the second and subsequent programs. If the error occurs, perform IOM download to the communication module for which the downloading failed from the SCS State Management Window after the online change download is finished.

No.0480

Message name Heavy load on periodical processing

Printing example SCS0101 Too Heavy Load

Meaning The processing time of External Communication Function of the safety control station has exceeded the four times the scan period that is specified for External Communication Function.

Cause The load on the safety control station is too heavy.

Action Correct the application and reduce the load on the safety control station.

3.3 Safety Control Station Related Messages (Message Numbers 0727 through 0787)

This section describes other messages relating to the safety control station.

No.0727

Message name Block mode recovery error information

Printing example SCS0101 Block Mode Change Error Block=TAG001 Code=9601-0000

TAG001: Tag name

9601-0000: Error code

Meaning Block mode recovery failed at the end of downloading.

Action Report the error code to Yokogawa's Service department.

No.0743

Message name Self-diagnostic SEN-BUS Failure

Printing example SCS0101 SEN-BUS Alarm SEN-BUS No.1

Meaning The SEN-BUS in question has failed.

Cause There is a failure in the SEN-BUS in the CPU node or the CPU module mounted.

Action Replace the CPU node or the CPU module mounted.

No.0744

Message name Self-diagnostic SEN-BUS Recovery

Printing example SCS0101 SEN-BUS Recover SEN-BUS No.1

Meaning The SEN-BUS in question has returned to normal. (This is a recovery message of No. 0743.)

No.0749

Message name Self-diagnosis detected an I/O Error

Printing example 1 SCS0101 N-IO Self Diag Error N-IO CODE = 00005119 DET = 00000000

Printing example 2 SCS0101 FIO Self Diag Error FIO CODE = 00005119 DET = 00000000

Meaning I/O error was detected during self-diagnosis.

Cause/Action The action varies depending on the Code and DET. Contact Yokogawa service department with the contents of CODE and DET.

The following describes the contents of CODE and DET.

Table 3.3-1 Message No. 0749 - CODE and DET List

CODE/DET	Errors
CODE = 00005119	An error was detected in the redundant control unit. Switching is not performed even if an error occurred on the control side. Replace the I/O module.
CODE = 00005171	The I/O module does not support the function that is intended to use. Fire and Gas device resetting function: Uses modules prior to SAI143 style S4 Use a supported I/O module. Refer to the IOM Model in the IOM Report to find out the style of the I/O module.
CODE = 00005172	A memory error in I/O module was detected. If the I/O module recovers to normal after this alarm is generated, continue to use the module.
DET = nnss0000	A detail code of CODE = 00005119 and CODE = 00005171. nnss indicates the installation position of the FIO I/O module in error. nn is a node number, and ss is a slot number. All of which are in hexadecimal.
DET = nnus0000	A detail code of CODE = 00005119 and CODE = 00005172. nnus indicates the installation position of the N-IO I/O module in error. nn is a node number, u is a unit number, and s is a slot number. All of which are in hexadecimal.
CODE = 0000511B	An error was detected in the I/O unit of the CPU module.
DET = 0000 Y48x	A detail code of CODE = 0000511B. Y = 0 indicates an error in the right CPU module, and Y = 8 indicates an error in the left CPU module.

No.0750

Message name I/O Recovery from the error detected by self-diagnosis

Printing example 1 SCS0101 N-IO Self Diag Recover N-IO CODE = 00000000 DET = 00000000

Printing example 2 SCS0101 FIO Self Diag Recover FIO CODE = 00000000 DET = 00000000

Meaning Recovery from I/O error detected by self-diagnosis. (This is a recovery message of No. 0749.)

No.0751

Message name Time self-diagnostic testing error

Printing example SCS0101 RIGHT Time Self Diag Error Code=00030021

Meaning A clock error is detected by self-diagnosis while the CPU of either redundant or non-redundant is running.

Cause VEHICLE clock, RTC or GPS clock trouble

Action Replace the CPU module.

No.0753

Message name Communication Overload

Printing example SCS0101 Communication Overload

Meaning Communication load to safety control station exceeded the limit.

Cause There were many communication demands from the operation and monitoring function window or application programs to the safety control station.

Action If the windows for the indicated safety control station are displayed on the CENTUM HIS, the windows need to be closed. Modifying the application programs may also reduce the communication load to the safety control station.

No.0767

Message name	ESB bus error on either bus
Printing example 1	SCS0101 N-IO-BUS Fail N-IO RIGHT BUS No.01
Meaning 1	An error occurred in the communication on bus 1 from the right-side bus interface (IO controller in the CPU module or the N-ESB bus coupler module) of the N-IO of the safety control station (station name = SCS0101). (Communication with all nodes on the bus 1 side became abnormal.) For SCSP3, "N-IO" is shown as in printing example 1. "N-IO" is also shown when only FIO nodes are used in the SCSP3.
Cause 1	Since an error occurred only in one CPU module, the IO controller in the CPU module, backboard of the CPU node, or N-ESB bus coupler module may be faulty.
Action 1	Replace the CPU module, CPU node, or N-ESB bus coupler module.
Printing example 2	SCS0101 FIO-BUS Fail FIO RIGHT BUS No.1
Meaning 2	A communication error (bus1 in the above example) occurred in standby side CPU module (right side in the above example) of the safety control station (station name = SCS0101). (Communication with all FIO nodes on bus 1 side became abnormal.)
Cause 2	The CPU module, backboard of the CPU node, or ESB bus coupler module may be faulty.
Action 2	Replace the CPU module, CPU node, or ESB bus coupler module.

No.0768

Message name	Recovery from ESB bus error on either bus
Printing example 1	SCS0101 N-IO-BUS Recover N-IO RIGHT BUS No.01
Meaning 1	The communication on bus 1 from the right-side bus interface of the N-IO of the safety control station (station name = SCS0101) recovered. For SCSP3, "N-IO" is shown as in printing example 1. "N-IO" is also shown when only FIO nodes are used in the SCSP3. (This is a recovery message of No. 0767.)
Printing example 2	SCS0101 FIO-BUS Recover FIO RIGHT BUS No.1
Meaning 2	A communication error (bus1 in the above example) in standby side CPU module (right side in the above example) of the safety control station (station name = SCS0101) recovered. (This is a recovery message of No. 0767.)

No.0769

Message name	Error in the diagnosis of the safety control station cabinet by external equipment
Printing example	SCS0101 External Equipment Error N-IO NODE 01
Meaning	An error was detected in the diagnosis, by external equipment, of the cabinet storing N-IO node 1 of the safety control station (station name = SCS0101).
Action	Check the type of error through, for example, the display of the external equipment for the applicable cabinet, and then take an action according to the error. For details, check the manual of the applicable external equipment.

No.0770

Message name Recovery from error in the diagnosis of the safety control station cabinet by external equipment

Printing example SCS0101 External Equipment Recover N-IO NODE 01

Meaning An error detected in the diagnosis, by external equipment, of the cabinet storing N-IO node 1 of the safety control station (station name = SCS0101) recovered (this is a recovery message of No. 0769).

No.0787

Message name Self-diagnosis detected I/O error in CPU module

Printing example SCS0101 I/O Diagnosis Error IO RIGHT CODE=02518000 00000000

Meaning A self-diagnosis error occurred in a CPU module (right side in the above example) of the safety control station (station name = SCS0101).

Cause/Action Perform the appropriate action based on the cause that is indicated for the detailed error codes.

Table 3.3-2 Message No. 0787 - Error Code Detail

CODE(hexadecimal, 16 digits)		Factor	
Error code (Upper 8 digits)	Error detail (Lower 8 digits)		
0251 8000	0000 0000	A CPU module error was detected.	Replace the CPU module.
0255 8082	0000 0270 (*1)	This code indicates that the revision of the firmware (F4) in the CPU module is obsolete for the system configured with Optical ESB Bus Repeater modules.	If a system contains Optical ESB Bus Repeater module, the proper revision of CPU should be used.
xxxx0471	xxxx xxxx	SCSP2-S, SCSP3-S, SCSL2-S: An error was detected in the I/O operation and monitoring diagnosis of the CPU. The CPU module have failed or the load in the I/O communication band is too heavy.	If many I/O modules are installed on the ESB bus extended with optical cables, estimate the I/O communication band and check the validity.
xxxx0313	xxxx xxxx	SCSP2-S, SCSP3-S, SCSL2-S: The I/O function part of the CPU may be faulty.	Replace the CPU module.

*1: This code is not generated in SCSP2-S, SCSP3-S, and SCSL2-S.

3.4 Fieldbus Messages (Message Numbers 3401 through 3408)

This section describes the fieldbus-related messages.

"Detail" in the printing examples of Message No. 3401 and No. 3403 shows detailed information of a fieldbus device alert in hexadecimal notation. Plant Resource Manager (PRM) can show text strings representing the expanded versions of Detail information.

The fieldbus-related messages are displayed in the historical report window on the CENTUM HIS.

No.3401

Message name HART device event notification

Printing example SCS0101 HART NODE 01 UNIT 01 SLOT 01 CH 01 Event Device=0123456789 Detail=xxx

Meaning A status change was detected from the HART device (device ID = 0123456789) that is connected to channel 1 of slot 1 of unit 1 of N-IO node 1 of the safety control station (station name = SCS0101) and notified.

Action Check the detailed condition of the HART device through PRM, FieldMate, or a handy terminal.

No.3403

Message name IOM detected a HART device status change

Printing example SCS0101 HART NODE 01 UNIT 01 SLOT 01 CH 01 Device Status Changed Device=0123456789 Detail=xxx

Meaning The IOM detected a status change in the HART device (device ID = 0123456789) that is connected to channel 1 of slot 1 of unit 1 of N-IO node 1 of the safety control station (station name = SCS0101).

Action Check the detailed condition of the HART device through PRM, FieldMate, or a handy terminal.

Remarks This message is generated for status changes including the HART communication errors that are detected by the HART device.

No.3405

Message name Communication error when acquiring HART device status (No response)

Printing example SCS0101 HART NODE 01 UNIT 01 SLOT 01 CH 01 Device Status Communication Error (No Response) Device=0123456789

Meaning When acquiring the status of the HART device (device ID = 0123456789) that is connected to channel 1 of the I/O module installed in slot 1 of unit 1 of N-IO node 1 of the safety control station (station name = SCS0101), no response (time-out) occurred in the communication between the HART device and the analog digital I/O module.

Cause No response is received from the HART device due to one of the following causes:

- Disconnected cable
- Effect of noise

- The range of the received signal is low.
- Output current from the analog digital I/O module is outside the HART communication enable range supported by the HART device.

Action Check the HART device, communication route between the HART device and analog digital I/O module, or I/O parameter settings (tight shut/full open output settings, etc.)

Remarks If no problem is found in the communication route from the HART device to the analog digital I/O module, the HART circuit in the analog digital I/O module may be faulty. Depending on the faulty location in the HART circuit, the control right over the analog digital I/O module may not switch even in a redundant configuration. In this case, switch the module control right by using the IOM control right switching tool and check if the communication recovers. If the communication recovered to normal, the HART circuit in the standby module is likely faulty, so replace the module.

No.3407

Message name Communication error when acquiring HART device status

Printing example SCS0101 HART NODE 01 UNIT 01 SLOT 01 CH 01 Device Status Communication Error Device=0123456789 Code=XXX

Meaning A communication error occurred when acquiring the status of the HART device (device ID = 0123456789) connected to the analog digital I/O module mounted in slot 1 of unit 1 of N-IO node 1 of the safety control station (station name = SCS0101).

Cause The HART device or the communication route between the HART device and the analog digital I/O module likely encountered a problem.

Action Take an action based on the cause associated with the detailed error code.

Remarks If no problem is found in the communication route from the HART device to the analog digital I/O module, the HART circuit in the analog digital I/O module may be faulty. Depending on the faulty location in the HART circuit, the control right over the analog digital I/O module may not switch even in a redundant configuration. In this case, switch the module control right by using the IOM control right switching tool and check if the communication recovers. If the communication recovered to normal, the HART circuit in the standby module is likely faulty, so replace the module.

Table 3.4-1 Detailed Error Codes (D6xx)

Code (Hex.)	Meaning	Cause	Action
D643	Cannot transmit or receive due to incorrect frames on the HART line.	Possibly caused by an inconsistent device on the HART line or by effect of noise.	Check the HART device or the communication route between the HART device and analog digital I/O module.
D644	A framing error or an overrun error occurred when receiving one byte.	Possibly caused by effect of noise.	Check the HART device or the communication route between the HART device and analog digital I/O module.
D645	A parity error occurred when receiving one byte.	Possibly caused by effect of noise.	Check the HART device or the communication route between the HART device and analog digital I/O module.

Continues on the next page

Table 3.4-1 Detailed Error Codes (D6xx) (Table continued)

Code (Hex.)	Meaning	Cause	Action
D648	Delimiter error	Possibly caused by effect of noise.	Check the HART device or the communication route between the HART device and analog digital I/O module.
D649	The length of the received frame does not match the given frame length. Or, a character-gap timeout occurred.	This error occurs when the device discontinues transmission, and thus possibly caused by the device.	Check the detailed condition of the HART device through PRM, FieldMate, or a handy terminal.
D64A	A checksum error was found in the received frame.	Possibly caused by effect of noise.	Check the communication route between the HART device and analog digital I/O module.
D64D	Unexpected response	Possibly caused by the device.	Check the detailed condition of the applicable HART device using the PRM, FieldMate or handy terminal.
D64F	Other errors	Error other than D643 to D64D. Possibly caused by the device.	Check the HART device or the communication route between the HART device and analog digital I/O module.
D6CD	A frame of unexpected size was received during status acquisition from the HART device.	The HART device has the specification of the version that is not supported by the analog digital I/O module.	Enable event notification on the HART device, or change the I/O parameter settings so as to disable communication for HART device status acquisition.(*1)

*1: You must take action based on whether the HART device supports event notification. For whether or not Event Notification for the applicable HART device is supported, check the specification of the HART device or vendor of the HART device.

No.3408

Message name Normal recovery of HART device status acquisition communication

Printing example SCS0101 HART NODE 01 UNIT 01 SLOT 01 CH 01 Device Status Communication Recover Device=0123456789

Meaning Communication between the HART device (device ID = 0123456789) connected to channel 1 of the analog digital I/O module installed in slot 1 of unit 1 of N-IO node 1 of the safety control station (station name = SCS0101) and analog digital I/O module recovered normally when acquiring the status of the HART device.

Appendix 1. Alarm Class

The following table shows the alarm class that is added to each Diagnostic Information Message.

Table Appendix 1-1 Alarm Class

Message number	Message name	Alarm class
0001	Reset start of safety control station	2
0003	Safety control station automatic reset start	2
0005	Power ON initial cold start of safety control station	2
0009	Transfer of control right of safety control station	2
0011	Fail information of safety control station	2
0013	AC power supply failure of safety control station	2
0015	Self-diagnosis error of clock inside CPU module	2
0017	ROM checksum error of CPU module	2
0021	Internal task error of safety control station	2
0023	Mapping block fatal error	2
0025	Function control word error	2
0027	Mapping block record information error	2
0033	Online downloading abnormal end	2
0041	Safety control station fan alarm	2
0042	Recovery from safety control station fan alarm	3
0043	Safety control station temperature alarm	2
0044	Recovery from safety control station temperature alarm	3
0045	Power supply module alarm of safety control station	2
0046	Recovery from power supply module alarm of safety control station	3
0047	Battery alarm of CPU module	2
0048	Recovery from battery alarm of CPU module	3
0053	Safety control station cabinet temperature alarm	2
0054	Recovery from safety control station cabinet temperature alarm	3
0055	Information of same frame reception in online change download communication	2
0057	Information of online change download error	2
0059	Information of recovery from node power failure	1
0063	ESB bus error	1, or 2
0064	Normal recovery of ESB bus	3
0065	Failure of N-ESB bus module or ESB Bus Interface module	2
0066	Normal recovery of N-ESB bus module or ESB Bus Interface module of node	3
0067	Failure of power supply of node	2
0068	Normal recovery of power supply of a node	3
0069	Error before database download to I/O module	1, or 2

Continues on the next page

Table Appendix 1-1 Alarm Class (Table continued)

Message number	Message name	Alarm class
0073	Error in the F-SB bus connecting the N-IO I/O unit and node interface unit	2
0074	Normal recovery of the F-SB bus connecting the N-IO I/O unit and node interface	3
0081	Failure of I/O module	1, or 2
0082	Normal recovery of I/O module	3
0083	I/O module database error occurred	2
0085	I/O module communication error occurred	2
0086	Recovery from I/O module communication error	3
0087	Node error occurred	1
0088	Normal recovery of node	3
0089	Subsystem communication error	2
0090	Subsystem communication recovered	3
0093	CPU node's housekeeping unit error	2
0094	Normal recovery of CPU node's housekeeping unit	3
0425	Start of online upgrade	4
0426	Normal completion of online upgrade	4
0427	Online upgrade error	2
0447	Node maintenance port enabled notification	2
0448	Node maintenance port disabled notification	3
0450	Copy program and database on control side of safety control station to standby side	4
0451	Information of switching of control side of safety control station	4
0452	Information of switching of standby side of safety control station	4
0455	Node maintenance notification	4
0456	Node maintenance cancellation notification	4
0459	Information of I/O module service side	4
0460	Information of I/O module out service	4
0471	Normal completion of online change download	4
0474	Information of tag list duplicate error	2
0475	Start of database download to I/O module	4
0476	Normal completion of database download to I/O module	4
0477	Database download error to I/O module	2
0480	Heavy load on periodical processing	4
0727	Block mode recovery error information	2
0743	Self-diagnostic SEN-BUS Failure	2
0744	Self-diagnostic SEN-BUS Recovery	3
0749	Self-diagnosis detected an I/O Error	1, or 2
0750	I/O Recovery from the error detected by self-diagnosis	3
0751	Time self-diagnostic testing error	1

Continues on the next page

Table Appendix 1-1 Alarm Class (Table continued)

Message number	Message name	Alarm class
0753	Communication Overload	2
0767	ESB bus error on either bus	2
0768	Recovery from ESB bus error on either bus	3
0769	Error in the diagnosis of the safety control station cabinet by external equipment	2
0770	Recovery from error in the diagnosis of the safety control station cabinet by external equipment	3
0787	Self-diagnosis detected I/O error in CPU module	1, or 2
4101	Inter-SCS safety communication error information	1
4102	Inter-SCS safety communication error recovery information	3
4103	Variable lock	4
4104	Cancellation of variable lock	4
4105	I/O module lock	4
4106	Cancellation of I/O module lock	4
4107	All input module locks	4
4108	Cancellation of all input module locks	4
4109	All output module locks	4
4110	Cancellation of all output module locks	4
4111	All module locks	4
4112	Cancellation of all module locks	4
4113	Number of locks exceeded	2
4114	Recovery from exceeded number of locks	3
4115	Override setting	4
4116	Cancellation of override	4
4117	Information of change to override enabled state	4
4118	Information of change to override disabled state	4
4119	Number of overrides exceeded	2
4120	Recovery from exceeded number of overrides	3
4121	Number of enabled overrides exceeded	2
4122	Recovery from exceeded number of enabled overrides	3
4123	Number of active PASSWD FBs exceeded	2
4124	Recovery from exceeded number of active PASSWD FBs	3
4125	I/O module channel error occurred	1
4126	Recovery from I/O module channel error	3
4127	Setting PASSWD FB to ON	4
4128	Setting PASSWD FB to OFF	4
4129	GPS interface unit error	2
4130	Recovery of GPS interface unit	3
4131	Communication module lock	4
4132	Cancellation of Communication module lock	4
4133	Information of a diagnosis error in the received data of SCS Link Transmission.	1, or 2

Continues on the next page

Table Appendix 1-1 Alarm Class (Table continued)

Message number	Message name	Alarm class
4134	Information of a diagnosis error recovery in the received data of SCS Link Transmission.	3
4135	SCS Link Transmission data lock	4
4136	Cancellation of SCS Link Transmission data lock	4
4137	Number of Locked Stations in SCS Link Transmission Excee-ded	2
4138	Recovery from exceeded number of locked stations in SCS Link Transmission	3
4139	Inter-SCS Safety Communication data lock	4
4140	Cancellation of Inter-SCS Safety Communication data lock	4
4141	Number of locked stations in Inter-SCS Safety Communica-tion exceeded	2
4142	Recovery from exceeded number of locked stations in Inter-SCS Safety Communication	3
4143	Start of automatic scan period extension	1
4144	Cancellation of automatic scan period extension	3
4145	Abnormal calculation occurred	1
4146	Recovery from abnormal calculation	3
4151	Information of retainable data initialization	4
4152	Online change of scan period	4
4153	Information of Inter-SCS Safety Communication data lock time-up	2
4154	Information of forced cancellation of Inter-SCS Safety Com-munication data locks	4
4155	Information of SCS Link Transmission status change.	4
4156	Information of SCS Link Transmission definition change	4
4157	Information of SCS Link Transmission wiring change	4
4158	Information of SCS Link Transmission lock time-up	2
4159	Information of forced cancellation of SCS Link Transmission locks	4
4160	Invalid password for Manual Operation FB	4
4161	Information of Output IOM Shutdown	4
4162	Information of communication I/O definition change	4
4163	Information of communication I/O wiring change	4
4164	Information of disabling security level change	4
4165	Information of enabling security level change	4
4166	Information of communication module lock time-up	2
4167	Information of forced cancellation of communication module locks	4
4168	Information of tag name change by online change download	4
4169	NVRAM diagnosis error	2
4170	Flash memory diagnosis error	2
4172	Information of resource change by online change download	4
4173	Completion of writing to flash memory	4

Continues on the next page

Table Appendix 1-1 Alarm Class (Table continued)

Message number	Message name	Alarm class
4174	Failed to write to flash memory	2
4175	Failed to update external communication data	2
4177	Information of SCS security level change	4
4178	Information of security level time-up	2
4179	Information of communication I/O module output enable operation	4
4180	Information of password change	4
4181	Information of output enable operation	4
4182	Information of FIO output module start operation	4
4183	Request to upload SOE to SENG	4
4184	Notification on saving SOE trip signal file in SCS	4
4185	Information of variable value change	4
4186	Information of lock time-up	2
4187	Information of forced cancellation of locks	4
4188	Start of online change download	4
4189	Completion of online change download	4
4190	Online change download error	2
4191	Completion of I/O definition rewriting	4
4192	Information of override state time-up	2
4193	Information of forced release of all overrides	4
4194	Information of override enabled state time-up	2
4195	Information of communication I/O data status change	4
4196	Invalid password for PASSWD FB	4
4197	Information on active PASSWD FB time-up	2
4198	Information on forced reset of PASSWD FB	4
4199	Override communication error	2
4201	Information of node maintenance port enable operation	4
4202	Information of node maintenance port disable operation	4
4203	Information of node maintenance port disable operation for all N-IO nodes	4
4205	Information of node maintenance port enabled state	2
4206	Information of node maintenance port disabled state	3
4207	Information of HSDTR FB or GASDTR FB reset operation	4
4208	Communication error in HSDTR FB or GASDTR FB reset operation	2
4209	Safety subsystem communication error	1
4210	Recovery from safety subsystem communication error	3
4211	Safety subsystem communication path error	1
4212	Recovery from safety subsystem communication path error	3
4213	Safety subsystem communication I/O lock	4
4214	Cancellation of safety subsystem communication I/O lock	4

Continues on the next page

Table Appendix 1-1 Alarm Class (Table continued)

Message number	Message name	Alarm class
4215	Number of safety subsystem communication I/O locks exceeded	2
4216	Recovery from exceeded number of safety subsystem communication I/O locks	3
4217	Safety subsystem communication I/O data status change	4
4219	Safety subsystem communication I/O lock time-up	2
4220	Forcible cancellation of all safety subsystem communication I/O locks	4
4221	Alarm for the operation data reset switch of CPU module	2
4222	Recovery from alarm for the operation data reset switch of CPU module	3

Revision Information

Title : Messages Reference Manual

Manual No. : IM 32P02B10-01EN

Dec. 2023/9th Edition/R4.10 or later

Introduction	Updated descriptions.

Jan. 2022/8th Edition/R4.07

No.0749	Updated descriptions.

Feb. 2021/7th Edition/R4.06

No.0011, No.0063, No.0065, No.0066, No.0081, No.0082, No.0085, No.0087, No.0749, No.0767, No.0787, No.4125, No. 4211	Updated descriptions.

Dec. 2019/6th Edition/R4.05

Introduction	Updated descriptions about registered trademarks and trademarks.
No.0047, No.0787	Updated descriptions.
No.0425 to No.0427, No.4221, No.4222	Added.
No.4151	Updated descriptions.
Appendix 1	Added No.0425 to No.0427, No.4221, and No.4222.

Aug. 2018/5th Edition/R4.04

Introduction	Updated description of registered trademarks of YOKOGAWA.

Oct. 2017/4th Edition/R4.03.10

No.4131, No.4132, No.4162, No.4163, No.0477, No.0081	Updated descriptions.
No.4209 to No.4217, No.4219, No.4220	Added.
Appendix 1	Added No.4209 to No.4217, No.4219, and No.4220.

May 2017/3rd Edition/R4.03

Introduction	Deleted Windows Vista from explanation of trademarks.
No.4126, No.0749	Updated descriptions.
No.4207, No.4208	Added.
Appendix 1	Added No.4207 and No.4208.

Oct. 2016/2nd Edition/R4.02

Introduction	Updated descriptions in "■ Safety, Protection, and Modification of the Product," "■ Symbols," and "■ Trademark Acknowledgments." Added a new term in "■ Full Names and Simplified Terms."
No.3405, No.3407, No.4125	Updated descriptions.

Dec. 2015/1st Edition/R4.01

Newly published.

■ For Questions and More Information Online Query: A query form is available on the following URL for online query. http://www.yokogawa.com/iss
■ Written by Yokogawa Electric Corporation
■ Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Attachment 9.9 Engg Reference Manual

IM32P04B10-01EN

User's Manual

ProSafe-RS
ProSafe-RS Lite

Engineer's Reference Manual

IM 32P04B10-01EN

YOKOGAWA
Yokogawa Electric Corporation

IM 32P04B10-01EN
9th Edition

Introduction

This manual explains the tools and functions used when engineering ProSafe-RS. This manual primarily explains the functions and operation of Automation Design Suite. Usage and precautions for tool used when creating applications run on SCS are described in the format of a reference. In order to look up the details of functions related to engineering and maintenance, you can read the corresponding chapters for necessary information.

If you are using the Field Commissioning Support Package, replace “FieldMate Validator” in the User's Manual with “Field Commissioning Support Package.”

This manual consists of the following parts:

- Part A - Overview of Automation Design Suite
  This section explains the purpose of use along with an overview of functions of Automation Design Suite.
- Part B - Basic operations of Automation Design Organizer
  This section explains the roles and basic operations of Automation Design Organizer.
- Part C - Automation Design Server administration functions and history management
  This section explains the functions for management of Automation Design servers and Automation Design projects, Safety I/O Editor of Automation Design Organizer, IOM Definition Editor, SCS Manager, builders, tools groups such as SCS Maintenance Support Tool, the functions for recording and managing the changes applied to the generation manager along with when and by whom such changes were applied, and the function for checking this history information.
- Part D - ModPack change management
  This section explains the functions for preparing backups of SCS Projects, saving the Revision history of SCS Projects, recording the history of users using SENG functions, and managing SCS master projects.
- Part E - Access Control/Operation History Management functions
  This section explains the functions for recording and browsing the operation history of SENG software and the functions for user-based restrictions of operations of SENG software.
- Part F - Tools and functions used with engineering of ProSafe-RS
  This manual explains the tools and functions used when performing engineering.

9th Edition : Nov. 2022 (YK)
All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Safety Precautions for Use

Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Be sure to confirm the specifications and required settings of the devices that are used in combination with the Product by referring to the instruction manual or other documents of the devices.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:



Indicates that caution is required. This symbol for the Product indicates the possibility of dangers such as electric shock on personnel and equipment, and also indicates that the user must refer to the User's Manuals for necessary actions. In the User's Manuals, this symbol is used together with a word "CAUTION" or "WARNING" at the locations where precautions for avoiding dangers are described.

<French> Signale qu'il faut faire preuve de prudence. Ce symbole pour le produit signale la possibilité d'un danger pour le personnel et l'équipement comme un choc électrique, et signale également que l'utilisateur doit se référer au Manuel de l'utilisateur afin de prendre les mesures nécessaires. Dans le Manuel de l'utilisateur, ce symbole est utilisé conjointement avec la mention «CAUTION» ou «WARNING» aux endroits où sont décrites les précautions pour éviter les dangers.



Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.

<French> Signale qu'il faut faire preuve de prudence avec la surface brûlante. Les appareils sur lesquels est apposé ce symbole risquent de devenir brûlants. Tout contact physique ou matériel avec ces appareils risque de provoquer des brûlures ou des dommages.



Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.



Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.

Indicates an AC supply.

Indicates a DC supply.

| Indicates that a component such as a power supply switch is turned ON.

○ Indicates that a component such as a power supply switch is turned OFF.

Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

Warning and Disclaimer

- Except as specified in the warranty terms, YOKOGAWA shall not provide any warranty for the Product.
- YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Product.

Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the Software Product's merchantability or suitability for any particular purpose, except as specified in the warranty terms.
- Purchase the appropriate number of licenses of the Software Product according to the number of computers to be used.
- No copy of the Software Product may be made for any purpose other than backup; otherwise, it is deemed as an infringement of YOKOGAWA's Intellectual Property rights.
- Keep the software medium of the Software Product in a safe place.
- No reverse engineering, reverse compiling, reverse assembling, or converting the Software Product to human-readable format may be performed for the Software Product.
- No part of the Software Product may be transferred, converted, or sublet for use by any third-party, without prior written consent from YOKOGAWA.

Documentation Conventions

Symbols

The following symbols are used in the User's Manuals.

 WARNING	Indicates precautions to avoid a danger that may lead to death or severe injury.
 CAUTION	Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.
IMPORTANT	Indicates important information required to understand operations or functions.
TIP	Indicates additional information.
	Indicates referenced content. In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

Typographical Conventions

The following typographical conventions are used throughout the User's Manuals.

Commonly Used Conventions throughout the User's Manuals

- Δ Mark
  Indicates that a space must be entered between character strings.
  Example:

  ```
  .ALΔPIC010Δ-SC
  ```

- Character string enclosed by braces { }
  Indicates character strings that may be omitted.

  Example:

  ```
  .PRΔTAG{Δ.sheet name}
  ```

Conventions Used to Show Key or Button Operations

- Characters enclosed by brackets [ ]
  When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a button name in a window, or an item in a list box displayed in a window.

  Example:

  To alter the function, press the [ESC] key.

Conventions of a User-defined Folder

- User-defined folder name enclosed by parenthesis ( )
  User definable path is written in a pair of parentheses.

  Example:

  ```
  (RS Project Folder)\SCS0101
  ```

If the RS Project Folder is `C:\MYRSPJT`, the above path becomes `C:\MYRSPJTSCS0101`.

Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.
If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

Definitions of Node and Module Terms

In the User's Manuals, nodes and modules are referred to by using collective terms, another terms, or abbreviations based on the following definitions:

- Definitions of nodes
  - Node: A node is a collective term for an FIO node and an N-IO node.
  - FIO node: This is a collective term for a safety control unit, a safety node unit, and a unit for optical ESB bus repeater module.
  - CPU node: This is another term for a safety control unit. The abbreviation of safety control unit is SCU.
  - I/O node: This is another term for a safety node unit. The abbreviation of safety node unit is SNU.
  - N-IO node: This is a collective term for a node interface unit and an N-IO I/O unit. The abbreviation of node interface unit is NIU.
- Definitions of modules
  - I/O module: This is a collective term for an FIO I/O module and an N-IO I/O module.
  - FIO I/O module: This is a collective term for an analog I/O module and a digital I/O module for FIO, and a communication module.
  - N-IO I/O module: This is a collective term for the modules that can be mounted on an N-IO I/O unit.
  - AIO/DIO module: This is a collective term for an analog I/O module, a digital I/O module, and a universal type I/O module.
  - Analog I/O module: This is a collective term for an analog input module and an analog output module.
  - Digital I/O module: This is a collective term for a digital input module and a digital output module.
  - Universal type I/O module: This is a collective term for the I/O modules for which the channel signal category can be changed by software.

- Input module: This is a collective term for an analog input module, digital input module, and a universal type I/O module with defined input channels.
- Output module: This is a collective term for an analog output module, digital output module, and a universal type I/O module with defined output channels.
- Communication module: This is a collective term for a serial communication module, an Ethernet communication module, and a fire and gas communication module.

Full Names and Simplified Terms

In the User's Manuals, simplified terms listed in the following table are used.

Table Info-1 Full Names and Simplified Terms

Full Name	Simplified Term
Automation Design Suite	AD Suite
Automation Design Organizer	AD Organizer
Automation Design Server	AD Server
Automation Design project	AD project
Automation Design Master Database	ADMDB
Automation Design Suite Administration Tool	ADS Administration Tool
iDefine for ProSafe-RS	iDefine
Modification Package	ModPack
SCSV1-S (SCS supporting the SSC10S/SSC10D safety control units)	SCSV1
SCSP1-S (SCS supporting the SSC50S/SSC50D safety control units)	SCSP1
SCSP2-S (SCS supporting the SSC60S/SSC60D safety control units)	SCSP2
SCSP3-S (SCS supporting the S2SC70S/S2SC70D safety control units)	SCSP3
SCSL2-S (SCS supporting the L1SC70S/L1SC70D safety control units)	SCSL2
SCSU1-S (SCS supporting the SSC57S/SSC57D safety control units)	SCSU1

Copyright and Trademark Notices

All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, PRM, Exaopc, FieldMate Validator, and STARDOM are registered trademarks or trademarks of Yokogawa Electric Corporation.
- The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

Engineer's Reference Manual

IM 32P04B10-01EN 9th Edition

CONTENTS

PART-A Overview of Automation Design Suite..... A-1

A1. Software configuration of AD Suite and storage of engineering data.. ..... A1-1

A2. Overview of AD Suite functions..... A2-1

A2.1 Basic functions..... A2-2

A2.2 ModPack change management.....A2-3

A3. Examples of system configuration..... A3-1

A4. Application capacity of AD Suite.....A4-1

Engineer's Reference Manual

IM 32P04B10-01EN 9th Edition

CONTENTS

PART-B Basic operations of Automation Design Organizer B-1

B1. Software used with I/O list engineering B1-1

B2. Starting and ending AD Organizer B2-1

B3. Window layout of AD Organizer B3-1

B3.1 Tool window area B3-3

B3.1.1 Navigation window B3-4

B3.1.2 Properties window B3-7

B3.1.3 Message window B3-8

B3.1.4 Revision History window B3-9

B3.1.5 Work Status List window B3-10

B3.1.6 Check-in window B3-11

B3.1.7 Operation in the tool window area B3-13

B3.1.8 Compare the details of engineering data B3-15

B3.2 Document window area B3-17

B3.2.1 Display and operations of the document window area B3-18

B3.3 Status bar area B3-22

B4. Operating AD Organizer B4-1

B4.1 Modifying an AD project subject to editing B4-2

B4.2 Editing a file with AD Organizer B4-3

B4.2.1 Check-out B4-5

B4.2.2 Edit B4-7

B4.2.3 Save B4-8

B4.2.4 Check-in B4-9

B4.3 Changing the data display method of AD Organizer B4-11

B4.3.1 Performing a search B4-12

B4.3.2 Sorting rows by a specified column B4-16

B4.3.3 Displaying filtered data B4-17

B4.3.4 Operating the columns B4-20

B4.4 Overview of grid rule definitions B4-23

Engineer's Reference Manual

IM 32P04B10-01EN 9th Edition

CONTENTS

PART-C Automation Design Server administration functions and history management..... C-1

C1. AD Server administration functions..... C1-1

C1.1 Tools for management of AD Server and AD projects..... C1-2

C1.1.1 Communication setting of the AD Server and Encryption setting of the ADMDB..... C1-5

C1.1.2 Changing the Communication setting of the AD Server and the Encryption setting of the ADMDB..... C1-6

C1.1.3 ADMDB location setting..... C1-8

C1.1.4 Setting the location of the ADMDB..... C1-14

C1.1.5 Backing up and restoring RS projects..... C1-17

C1.1.6 Backing up and restoring Library projects..... C1-19

C1.1.7 Backing up and restoring the ADMDB..... C1-20

C1.1.8 Viewing the history of backup and export operations..... C1-26

C1.2 Management of AD projects..... C1-27

C1.2.1 Creating and deleting AD projects..... C1-28

C1.2.2 Controlling access to AD projects..... C1-30

C1.2.3 Export and import AD projects..... C1-38

C1.2.4 Prohibiting and permitting modification of AD project data..... C1-42

C1.2.5 Forcibly canceling the checked-out status of currently checked-out files..... C1-44

C2. History management..... C2-1

C2.1 Overview of history management..... C2-2

C2.2 Modification file saving function..... C2-3

C2.2.1 Operation history of SCS Manager, builders, and tools..... C2-4

C2.2.2 Operation history of Generation Manager..... C2-6

C2.2.3 Operation history of Revision History Utility..... C2-7

C2.3 Operation logging function..... C2-8

C2.4 Start/Stop function..... C2-9

C2.5 Updating function..... C2-10

C2.6 Operations of the revision history function..... C2-11

C2.6.1 Window of Revision History Utility..... C2-12

C2.6.2 Operations of the Revision History Utility window..... C2-14

C2.6.3 Precautions regarding operation of SCS Manager and Generation Manager....C2-15
C2.7 History management using the editors of AD Organizer.... C2-16
C2.8 Setting labels....C2-17
C2.9 Displaying the revision history and labels.... C2-18
C2.9.1 Displaying the Revision History window.... C2-19
C2.9.2 Displaying the detailed information of a change set.... C2-22
C2.9.3 Displaying a list view and detail view of files.... C2-24
C2.9.4 Displaying the detailed information of a label.... C2-25
C2.9.5 Associating ModPacks with Change Sets.... C2-27

Engineer's Reference Manual

IM 32P04B10-01EN 9th Edition

CONTENTS

PART-D ModPack change management..... D-1

D1. Overview of ModPack change management..... D1-1

D1.1 Workflow for handling a change..... D1-3

D1.2 Windows that are used in change management..... D1-5

D1.2.1 ModPack Navigator..... D1-6

D1.2.2 ModPack List window..... D1-8

D1.2.3 ModPack Editor..... D1-9

D1.3 Access control on ModPack operation..... D1-15

D2. Operating ModPack change management..... D2-1

D2.1 Creating ModPacks..... D2-2

D2.2 Configuring the basic information..... D2-3

D2.3 Registering the assets to be modified..... D2-4

D2.4 Assigning the users who implement the change..... D2-6

D2.5 Implementing the change..... D2-7

D2.6 Testing the modified application..... D2-10

D2.7 Attaching files..... D2-11

D2.8 Validating the change..... D2-12

Engineer's Reference Manual

IM 32P04B10-01EN 9th Edition

CONTENTS

PART-E Access Control/Operation History Management functions.....E-1

E1. Configuration.....E1-1

E2. Access Control/Operation History Management function..... E2-1

E2.1 Overview of Access Control/Operation History Management..... E2-2

E2.1.1 Overview of access control for engineers..... E2-4

E2.1.2 Structure of Access Control/Operation History Management function E2-5

E2.1.3 Access Control/Operation History Management target operation list.. ..... E2-7

E2.2 Setting up Access Control/Operation History Management..... E2-10

E2.2.1 Settings for access control..... E2-12

E2.2.2 Setup related to Operation History Management..... E2-15

E2.2.3 Registering engineers..... E2-19

E2.2.4 Starting Operation History Management..... E2-33

E2.2.5 Window configuration of Engineers' Account Builder..... E2-34

E2.3 Operations of SENG that use Access Control/Operation History Management..... E2-36

E2.3.1 Engineer operations under access control..... E2-37

E2.3.2 Operations performed by administrators..... E2-41

E2.4 Browsing operation history data..... E2-51

E2.4.1 Browsing and printing operation logs..... E2-52

E2.4.2 Browsing and printing modification files..... E2-59

E2.4.3 Steps to browse backed-up operation history database..... E2-67

E2.4.4 Lists of Viewer Tool buttons..... E2-68

E2.5 Detailed information of Access Control/Operation History Management.... ..... E2-70

E2.5.1 Operation history database structure..... E2-71

E2.5.2 Access rights category list..... E2-72

E2.5.3 Information recorded in operation logs..... E2-76

Engineer's Reference Manual

IM 32P04B10-01EN 9th Edition

CONTENTS

PART-F Tools and functions used with engineering of ProSafe-RS F-1

F1. Display SCS information F1-1

F2. Self Document F2-1

F2.1 Document Generator F2-6

F2.2 Selection of printing targets F2-9

F2.3 Customizing print settings F2-14

F2.3.1 Customizable print settings F2-15

F2.3.2 Editing header and footer F2-19

F2.4 Selection of printing targets (Backward-compatible mode) F2-26

F2.5 Customizing print settings (backward-compatible mode) F2-30

F2.6 Confirmation by print preview F2-34

F3. Database Validity Check Tool F3-1

F4. Master Database Restoring Function F4-1

F5. Version control F5-1

F5.1 Main window of Version Control Tool F5-2

F5.2 Registration of SCS projects for version control F5-7

F5.3 Checking in project data F5-10

F5.4 Checking out project data F5-13

F5.5 Deleting of versions F5-17

F5.6 Deleting all check-in data related to a project F5-18

F5.7 Viewing version information F5-19

F5.8 Printing version information F5-21

F5.9 Changing the top path of a check-in folder F5-22

F6. Project Comparing Tool F6-1

F6.1 Overview of project comparison F6-2

F6.2 Window configuration of Project Comparing Tool F6-3

F6.3 Comparing two SCS projects F6-6

F6.4 Checking contents of detected differences F6-11

F7. Online monitoring F7-1

F8. Forcing function F8-1

F8.1 Variable locking..... F8-6
F8.2 Variable value setting.....F8-10
F8.3 Forcing function block parameters..... F8-13
F8.4 Forcing of SCS link transmission data.....F8-15
F8.5 Forcing of Inter-SCS safety communication.....F8-18
F8.6 Forcing function for subsystem communication data.....F8-22
F8.7 Forcing function for safety subsystem communication data..... F8-25
F8.8 Windows used for forcing of I/O variables.....F8-28
F8.8.1 I/O Lock window.....F8-31
F8.8.2 Locking and unlocking all variables of I/O module..... F8-39
F8.8.3 Set I/O variables of I/O modules..... F8-41
F8.9 SCS Link Transmission Lock window..... F8-44
F8.9.1 Locking and unlocking all SCS link transmission data of a station..... F8-51
F8.9.2 Set values of SCS link transmission data..... F8-52
F8.10 Inter-SCS Communication Lock window..... F8-55
F8.10.1 Locking and unlocking all Inter-SCS safety communication FBs associated with a station..... F8-63
F8.10.2 Set values of Inter-SCS safety communication FBs..... F8-65
F8.11 Communication I/O Lock window..... F8-69
F8.11.1 Structure of the Communication I/O Lock window..... F8-72
F8.11.2 Operations in the Communication I/O Lock window..... F8-83
F9. Software Configuration Viewer..... F9-1
F10. Builder Environment Tool.....F10-1

A. Overview of Automation Design Suite

This section provides an overview of Automation Design Suite.

A1. Software configuration of AD Suite and storage of engineering data

AD Suite is an engineering environment that is designed for developing and maintaining the entire instrumentation system inclusive of safety instruments.

Software configuration of AD Suite

The following figure shows the software configuration of AD Suite.

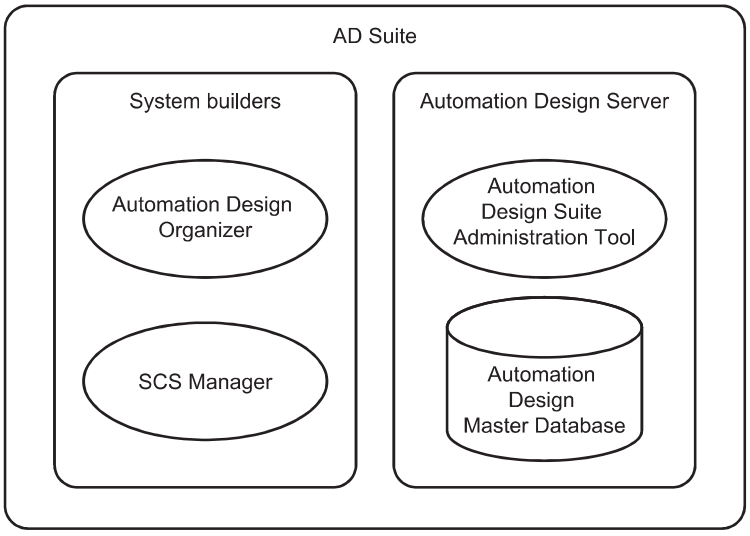


Figure A1-1 Software configuration of AD Suite

Safety system generation function

This function is used for the actual engineering of ProSafe-RS.

- Automation Design Organizer
  Automation Design Organizer (hereinafter referred to as AD Organizer) is an engineering software that uses a safety I/O list for safety systems. With this software it is possible to edit the safety I/O list and define the IOM. You can also export the safety I/O list to FieldMate Validator and import the safety I/O list which have been corrected by FieldMate Validator.

  After exporting the safety I/O list and IOM definition information for iDefine, which is an external engineering tool, and import them to iDefine, you can create application logic with iDefine. The engineering data that was created by using iDefine can be imported to AD Organizer and reflected in SCS projects.

TIP

Application logics that were created by using iDefine can be tested in iDefine. In addition, the SCS project to which the engineering data has been reflected can be connected with the logic simulator, SCS simulator, or the target SCS through the iDefine Test Manager of AD Organizer.

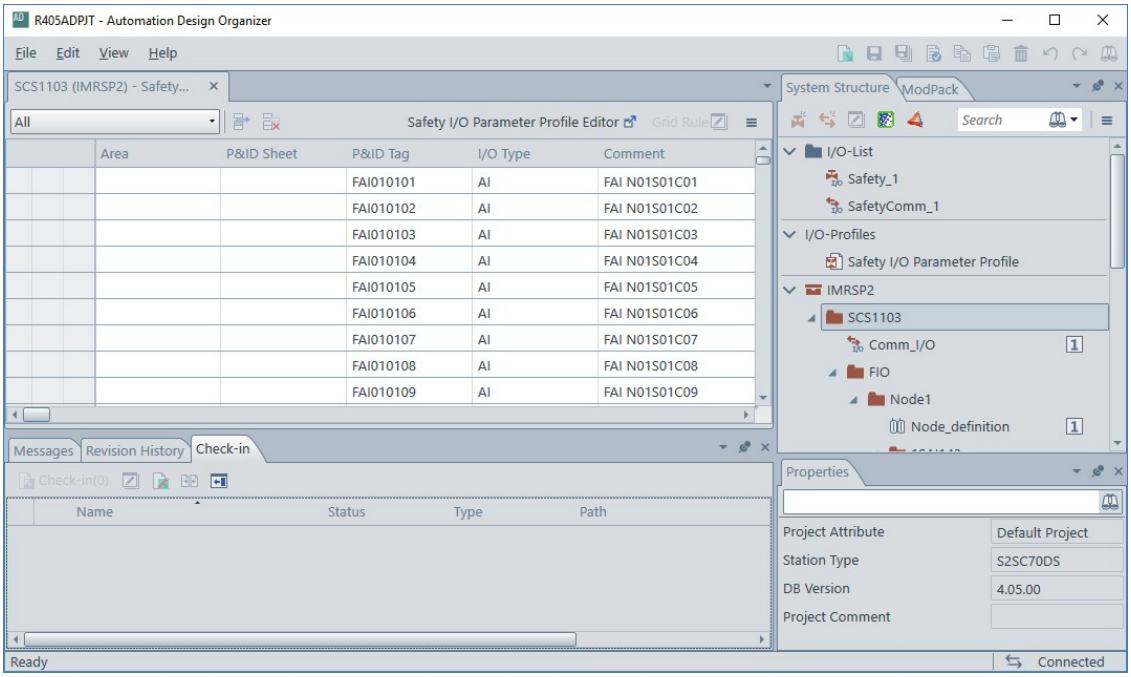


Figure A1-2 AD Organizer

- SCS Manager
  SCS Manager is a group of engineering software which defines items in regard to SCS projects. From the launcher menu, various engineering functions such as builders, SCS related tools, and SCS Maintenance Support Tool can be launched.

  The button to start up the SCS Manager is provided in the system structure navigator of AD Organizer. Select the SCS and click the button to open the target SCS project from the SCS Manager.

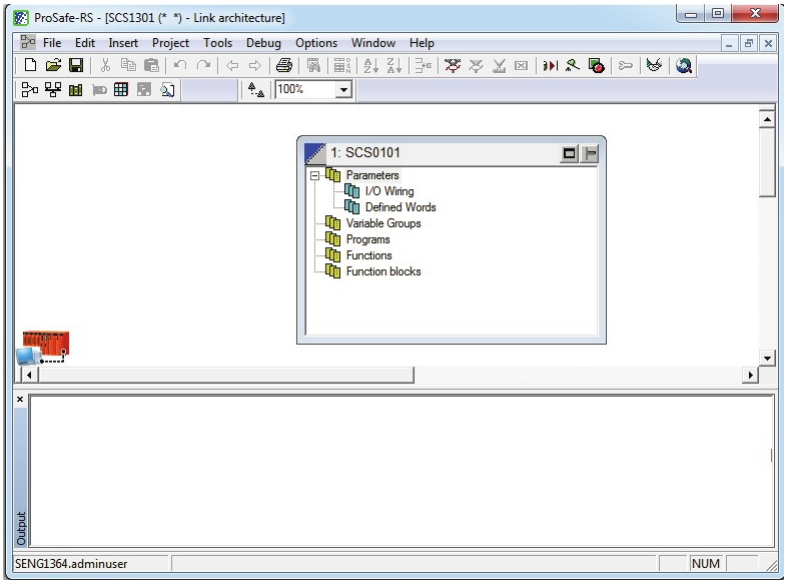


Figure A1-3 SCS Manager

Automation Design Server

Automation Design Server (AD Server) is a data server that manages the engineering data.

- Automation Design Master Database
  The Automation Design Master Database (ADMDB) is a database on which all engineering data is saved. This database also provides a function for history management of the engineering data.

- Automation Design Server Administration Tool
  Automation Design Server Administration Tool (ADS Administration Tool) is the software for management of AD Server.

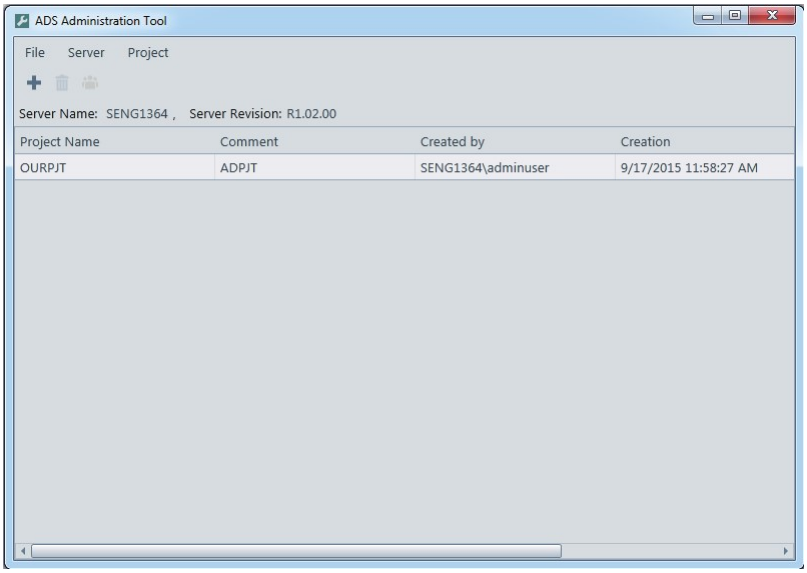


Figure A1-4 ADS Administration Tool

Storage of engineering data

Engineering data that is created or edited with the safety system generation functions is stored in the following projects.

- Automation Design project
  Automation Design projects (AD project) store the engineering data that is edited with AD Organizer. AD projects are created in the ADMDB on AD Server. Multiple AD projects can be created in the ADMDB.
- RS project
  RS projects are data folders for ProSafe-RS projects. These are created using a function provided with Windows. When RS projects that have been created are registered with an AD project, the content engineered by using SCS Manager is retained in the ADMDB making it possible to reference information such as the station configuration and revision history from AD Organizer.

  SCS projects are registered in folders under an RS project.

TIP

Multiple RS projects can be registered to a single AD project.

- SCS project
  In SCS projects, the engineering data that is edited with the builders of SCS Manager based on the safety I/O list and IOM information is stored. SCS projects are saved on a SCS database and the ADMDB.

TIP

SCS projects that have been duplicated with the copy operation in Windows cannot be registered on the ADMDB. Adding the SCS project from System Structure Navigator also causes an error. A copy of an SCS project can be created by exporting the SCS and importing the project upon changing the SCS name. A copy of an SCS project can be registered on the ADMDB by using System Structure Navigator.

The following figure shows the relationship between AD Organizer, SCS Manager, AD projects, RS projects, and SCS projects.

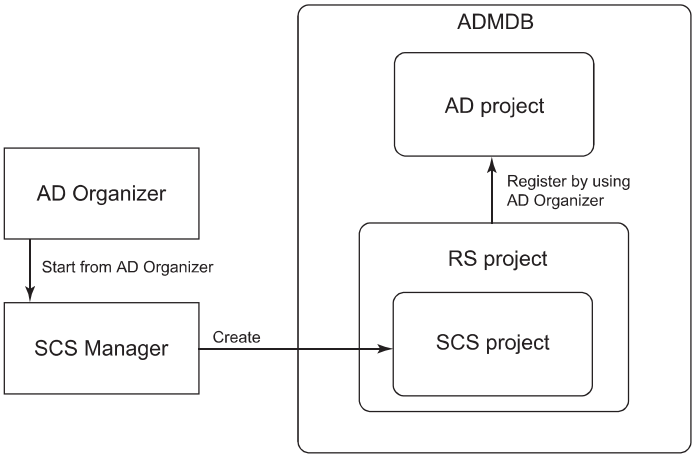


Figure A1-5 Flow of engineering data

AD projects are created using ADS Administration Tool.

RS projects are created by creating RS project folders using the explorer function provided with Windows. RS projects are registered to an AD project by using AD Organizer.

When an RS project is registered in an AD project by using AD Organizer, SCS projects created with SCS Manager can also be modified by using AD Organizer as SCS projects in the RS project folder are registered at the same time.

The revision history of SCS projects is stored in the AD project in which the SCS projects are registered.

For the ADMDB, which stores AD projects, you can use the ADS Administration Tool to specify the folder to place the ADMDB and configure access control to AD Server.

● Safety system generation functions and connection to AD Server

SCS projects are connected to the AD projects on AD Server through builders, which are part of the safety system generation functions. For this reason, the safety system generation functions must be connected to the AD Server when they are used.

Terminology

The following table shows terms used with AD Suite.

Table A1-1 Terms used with AD Suite

No.	Terminology	Description
1	Automation Design Suite (AD Suite)	Indicates the entire engineering environment of ProSafe-RS R4.
2	Automation Design Organizer (AD Organizer)	Engineering software that serves a central role in engineering that uses a safety I/O list.
3	Automation Design Server (AD Server)	A server that manages the engineering data of AD Suite.
4	Automation Design Master Database (ADMDB)	A database on which the engineering data and history of AD Suite is saved. ADMDB is stored in the AD Server.
5	Automation Design project (AD project)	A group of engineering data. The engineering data of AD Suite is managed for each AD project.

Continues on the next page

Table A1-1 Terms used with AD Suite (Table continued)

No.	Terminology	Description
6	Automation Design Server Administration Tool (ADS Administration Tool)	A tool for management of AD Server. This tool can be used to manage AD Server and AD projects and assign operation rights in relation to ModPacks, and so on. With management of AD Server, you can back up and restore the ADMDB. With management of AD projects, you can create AD projects, export and import project data, and configure access control of AD projects.
7	Builder	A generic term for the group of builders that are launched from SCS Manager.
8	Safety I/O list	Data created from plant information as information to use with safety applications. This data is used to create I/O variables. This list handles I/O such as AIO and DIO for ProSafe-RS.
9	Safety communication I/O list	Data created from plant information as information to use with safety applications. This data is used to create communication I/O data. This list handles the I/O of subsystem communication and fire and gas communication for ProSafe-RS.
10	IOM definition	A definition for I/O modules.
11	RS project	RS project folders are created by using the explorer function provided with Windows. These are referred to as RS projects. These are groups of data that store the engineering data that has been edited with a builder or AD Organizer and data that has been converted by RS generation. RS projects registered to an AD project are subject to being saved with the history management function. History management can be updated in units of RS projects.
12	System project	A generic term for RS Projects of ProSafe-RS and VP Projects of CENTUM VP.
13	SCS project	SCS projects are engineering data that has been edited with the builders of SCS Manager and AD Organizer based on the safety I/O list and IOM information.
14	SCS Manager	A collective term for the engineering applications of ProSafe-RS. This is the main window used to define SCS projects. I/O Parameter Builder and I/O Wiring View become display-only when performing I/O list engineering.
15	Safety system generation function	This function is used for the actual engineering of ProSafe-RS.
16	I/O list engineering	I/O list engineering is an engineering method which uses the I/O List Engineering Package and incorporates a safety I/O list into AD Organizer.
17	RS original engineering	RS original engineering is an engineering method that does not use the I/O List Engineering Package. The engineering tools of SCS Manager are used. If an RS project that includes SCS project is registered with AD Server, the history management function of AD Suite can be used.
18	History management	A function that manages the revision history of engineering data.
19	Change management	A function that supports management of the processes of changing engineering data.
20	RS generation	A function that converts the engineering data of AD Organizer into SCS projects.

Continues on the next page

Table A1-1 Terms used with AD Suite (Table continued)

No.	Terminology	Description
21	ModPack	A package that contains a set of information that is related to a certain change is called a Modification Package (ModPack).

A2. Overview of AD Suite functions

This section provides an overview of AD Suite functions.

AD Suite has the following main functions:

Basic functions

The basic functions of AD Suite are as follows.

- History management
  This function saves, to the ADMDB on AD Server, the SCS project files that have been updated through a build or by editing with builders or tools that are started from SCS Manager

  The user specifies whether to start or stop the history function. This function is used when editing with SCS Manager and when processing the reflection of Generation Manager of the build of an SCS project.

  The following functions can be used even without the Access Control / Operation History Management packages:

  - Viewing the history in the Revision History window in AD Organizer.
  - Displaying differences between two files saved as history in the Revision History window in AD Organizer. SCS Manager and various builders are launched in the read-only mode and the differences are displayed in red.
- Management of AD Server and AD projects
  - Location setting of the ADMDB
  - Controlling access to AD projects

ModPack change management

ModPack change management is a function of Change Management Package. This function requests changes of engineering data and manages the actual revision history.

The changes applied to engineering data are managed by associating sets of information referred to as ModPacks with the revision history.

A2.1 Basic functions

This section explains the basic function of AD Suite while providing an overview of the functions.

The basic functions of AD Suite can be used with ProSafe-RS R4.01.00 and later versions. If you use only the basic functions of AD Suite, engineering is performed from SCS Manager.

The basic functions have the following functions:

- History management
- Management of AD Server and AD projects
  - Location setting of the ADMDB
  - Management of access to AD projects

The following figure illustrates the basic functions.

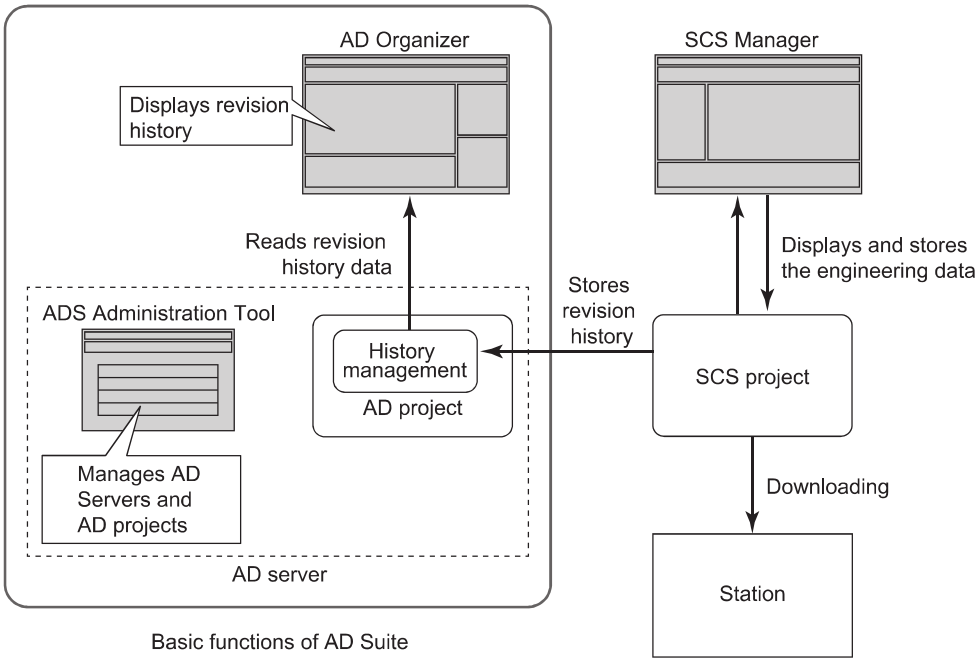


Figure A2.1-1 Basic functions

History management

History management stores the revision history of SCS projects. Whenever a file of an SCS project is updated, the revision history is automatically saved with the history management of AD Server. The revision history that has been saved with the history management can be displayed in AD Organizer.

Management of AD Server and AD projects

AD Server and AD projects are managed with ADS Administration Tool.

This tool comprises functions such as backing up and restoring the ADMDB, creating AD projects, exporting and importing AD project data, setting the location of the ADMDB, and configuring access control to AD Server.

A2.2 ModPack change management

This section provides and overview of the function of ModPack change management.

ModPack change management manages the process of modifying engineering data. The modification process is managed by editing a ModPack, which keeps records of the activities of implementing the change.

ModPack is short for Modification Package which is a set of information that is related to a certain change. A single ModPack can contain various information such as an ID for identifying the change, a status which indicates the status of the change, the user in charge of each change, the locations of the changes to be made, the results of changes, testing methods, and test results. For this reason, those in charge of each change can proceed with the tasks of applying such changes based on the ModPack that has been assigned to them.

ModPack change management can be used in cases both when performing I/O list engineering and when performing RS original engineering.

Change Management Package is required for ModPack Change management.

The following figure illustrates ModPack change management.

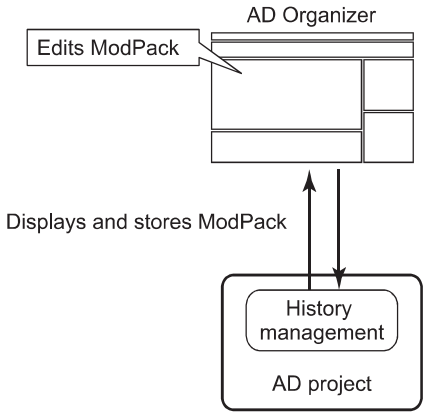


Figure A2.2-1 ModPack change management

A3. Examples of system configuration

This section provides examples of the system configuration of ProSafe-RS inclusive of AD Suite.

The following figure shows an example of the minimum system configuration of ProSafe-RS.

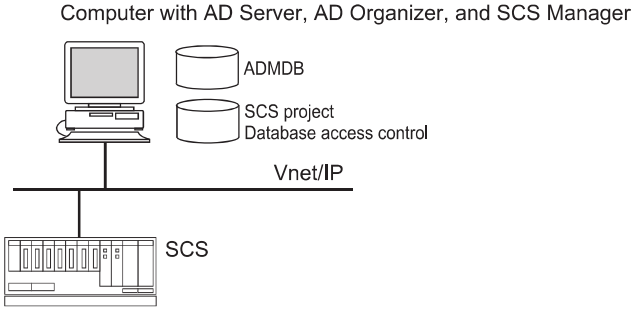


Figure A3-1 Example of minimum system configuration

One or multiple AD projects can be defined with AD Server. Multiple RS projects can be registered to a single AD project. All RS projects corresponding to a station to which the licenses of the same licensed project are assigned must be registered with a single AD project.

The following figure shows an example of a system configuration in which AD Server and AD Organizer are installed on different computers.

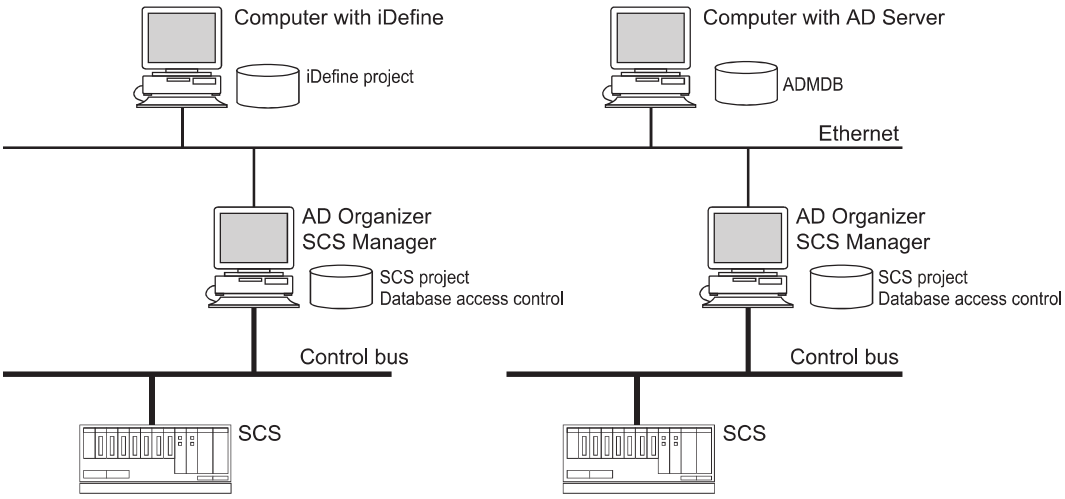


Figure A3-2 Example of a system configuration in which AD Server and AD Organizer are installed on different computers

The following figure shows an example of a system configuration in which CENTUM VP and ProSafe-RS coexist.

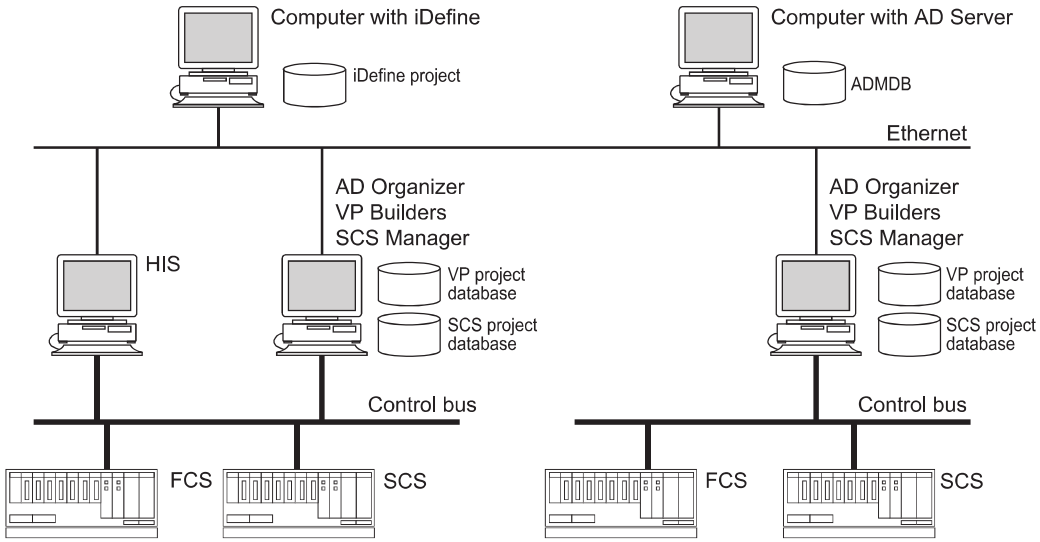


Figure A3-3 Example of a system configuration in which CENTUM VP and ProSafe-RS coexist

With AD Suite, the basic functions of CENTUM VP engineering and the safety system engineering and maintenance functions of ProSafe-RS can coexist on a single computer. As a minimum configuration, in addition to these, you can setup a configuration in which an engineering server function coexists as well.

Also, multiple VP projects and multiple RS projects can be registered to a single AD project.

TIP

iDefine can be installed on the computer on which SCS Manager and AD Organizer have been installed. iDefine and VP Builder cannot coexist on a single computer.

A4. Application capacity of AD Suite

The following show the application capacity of AD Suite.

Table A4-1 Application capacity

Item	Limit
RS project	32
SCS projects in a single RS project	100
P&ID Groups (*1)	100
Safety I/O parameter profile	1000

*1: P&ID Group is a name of a safety I/O list or safety communication I/O list. The name is specified when you create the safety I/O list or safety communication I/O list with System Structure Navigator.

B. Basic operations of Automation Design Organizer

This section describes the basic operations of Automation Design Organizer (hereinafter referred to as AD Organizer).

B1. Software used with I/O list engineering

Software used with I/O list engineering consists of AD Organizer and SCS Manager. You can also integrate with the external engineering tool iDefine.

The following list shows the functions of AD Organizer:

- I/O design
  Function for creating and editing the following lists
  - Safety I/O list
  - Safety communication I/O list
  - IOM definition
- I/O parameter profile
  Function for creating and editing safety I/O parameter profiles
- History management function
  Function for managing modification activities with ModPacks

iDefine has the following functions:

- FSM functionality
  Supports the Functional Safety Management as part of the safety lifecycle as stipulated in IEC61508 and IEC61511.
- Creating application logics
  Creates application logics by using the safety I/O list that was created in AD Organizer.
- Testing application logics
  Tests the application logics that were created.
- Creating documents
  Turns the application logics that were created and test results into documents.

TIP

- The I/O List Engineering Package is required to perform I/O list engineering.
- You can perform engineering by integrating the external engineering tool iDefine with AD Organizer. To use the external engineering tool iDefine, the I/O List Engineering Package and the iDefine Interface Package are required.
- The Change Management Package is required to use ModPacks.

B2. Starting and ending AD Organizer

This section describes how to start and end AD Organizer.

Starting AD Organizer

Follow these steps to start AD Organizer:

1. Log on as a user that has the access rights to add RS projects.
2. Start AD Organizer.
   When AD Organizer is started for the first time, the Select AD Project dialog box appears.
3. Select the computer name or IP address of the computer with AD Server, and click [Connect].
   AD projects that are created in AD Server appear.

TIP

If you want to set a port number, type a single-byte colon ":" and the port number after the computer name or the IP address.

4. Select the AD project and click [Open].

Behavior when AD Organizer fails to connect to AD Server

AD Organizer must be connected to AD Server when it is used. If AD Organizer fails to connect to AD Server, the system behaves as follows:

- When AD Organizer fails to connect to AD Server when it is started, a dialog box for selecting the AD project to connect to is displayed and the system will urge connection to a different AD Server.
- In cases when the connection with AD Server is discontinued after AD Organizer has been started, most functions of AD Organizer cannot be used. In such case, "Disconnected" is indicated as the AD Server connection status in the status bar area. After the connection with AD Server has been restored, the functions can be normally used. In such case, in the menu bar of AD Organizer, select [View] > [Update] and update the window display.

Ending AD Organizer

Follow these steps to end AD Organizer:

1. Click the [Exit] button in AD Organizer.
   The Exit dialog box appears.
2. Click the [OK] button.
   AD Organizer ends.

IMPORTANT

If iDefine or PROFINET Configurator that was started by AD Organizer is operating, a dialog box appears and AD Organizer cannot be ended.

B3. Window layout of AD Organizer

The following figure shows the window layout of AD Organizer:

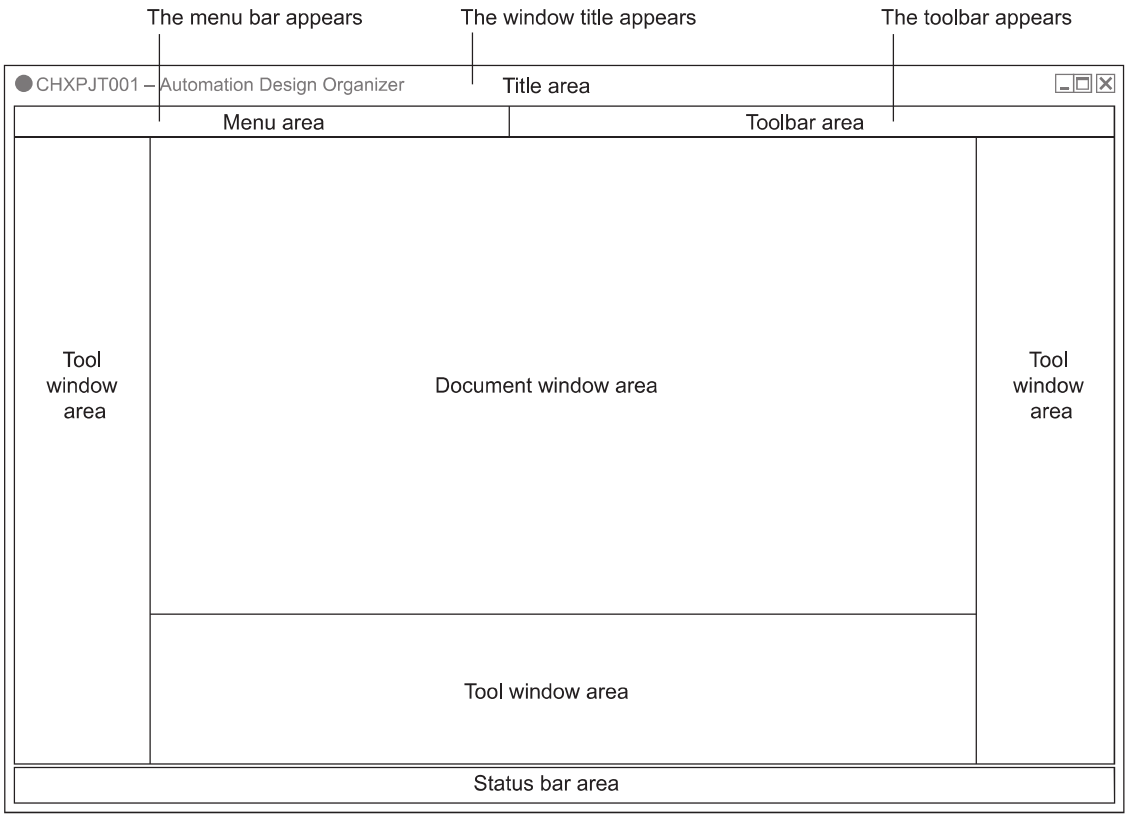


Figure B3-1 Window layout of AD Organizer

Default layout of window layout

The following figure and table show the default layout of the window layout of AD Organizer:

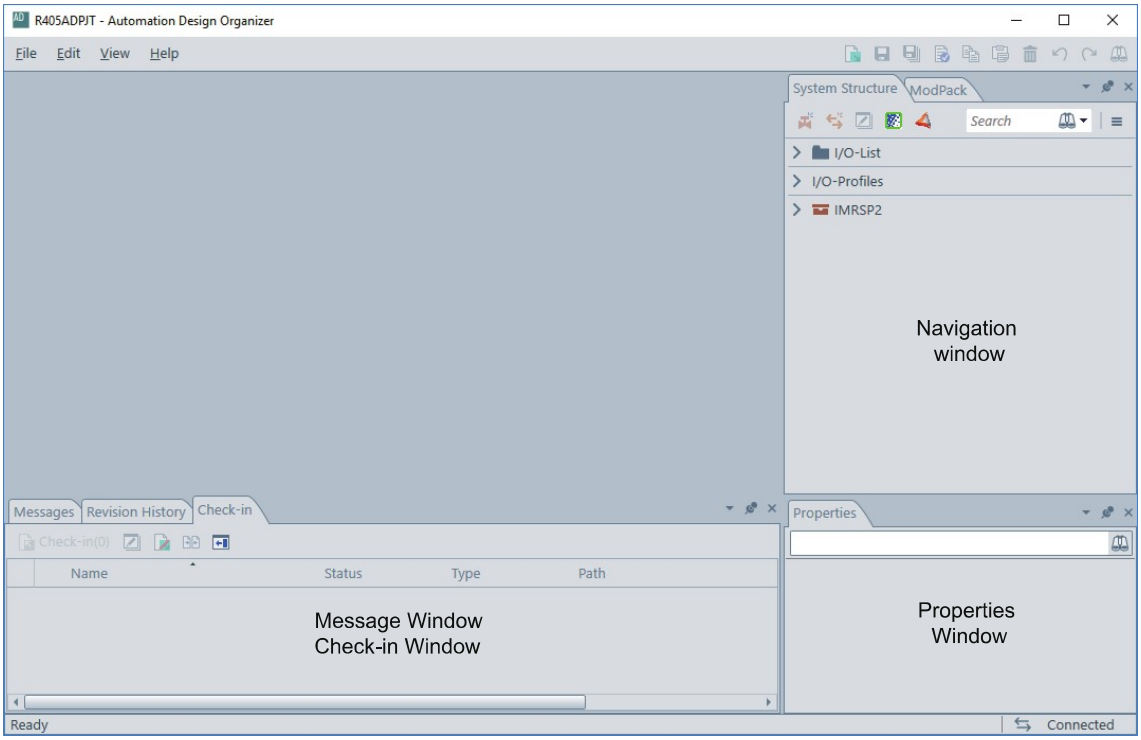


Figure B3-2 Default layout of window layout

Table B3-1 Display positions and window names of the default layout

Display position	Window name	Remarks
Top-right tool window area	Navigation window	The navigator shown as follows is open. • System Structure Navigator • ModPack Navigator
Bottom-right tool window area	Properties window	-
Bottom-center tool window area	Message window Check-in window	-
Document window area	There is nothing displayed	-

The left tool window area is not displayed in the default layout. This will be displayed when the window is moved to the left tool window area.

■ Changing the window layout

The user can change the window layout from the default state. New windows can be opened, the positions of windows can be changed, and windows can be made to float.

SEE ALSO For more information about floating windows, refer to:

"■ Floating a window" on page B3-13

■ Returning the window layout to the default layout

Follow these steps to return the window layout to the default layout.

- In the menu bar, select [View] > [Reset default layout].

B3.1 Tool window area

The following windows are displayed in the tool window area:

- Navigation window
  - System Structure Navigator
  - ModPack Navigator
- Properties window
- Message window
- Revision History window
- Check-in window

B3.1.1 Navigation window

In the navigation window, files and folders are shown as a list in a folder tree.

Double-clicking on a file displayed in the tree displays the file in the document window area.

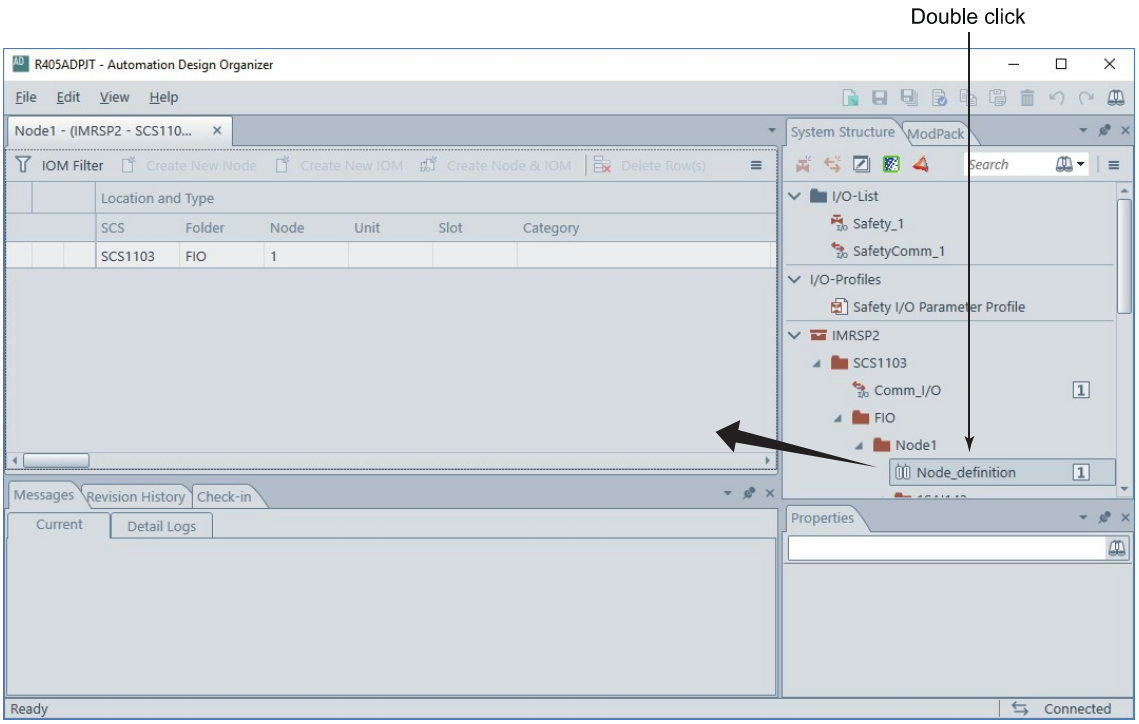


Figure B3.1.1-1 Screen development from the navigation window

The Navigation window consists of the following types:

- System Structure Navigator
- ModPack Navigator

These navigation windows, when first started, are bundled and displayed as tabs in the tool window area on the right side of the document window area.

System Structure Navigator

The following items are displayed in System Structure Navigator.

- Safety I/O list
- Safety communication I/O list
- Node definition
- IOM definition
- Safety I/O parameter profile
- iDefine Configuration folder

The following figure shows System Structure Navigator.

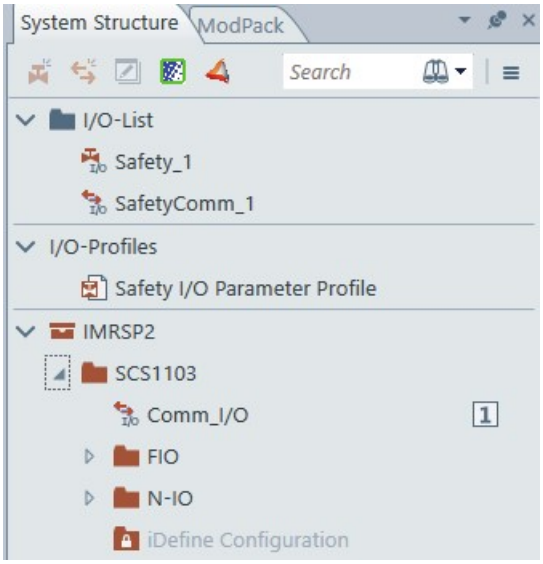


Figure B3.1.1-2 System Structure Navigator

TIP

- An icon resembling a key is displayed for folders that cannot be viewed with AD Organizer, SCS projects that are created with a setting for not performing the I/O list engineering, and the iDefine Configuration folder while the names thereof appear dimmed.
- An icon with an exclamation point appears for SCS projects under the following conditions:
  - An entire SCS project folder has been deleted for an SCS project that was created with I/O list engineering.
  - After an SCS project under the RS project folder registered in an AD project has been deleted, an SCS project of an different station type has been created with the same domain number and station number.

Perform the following operation to display the closed System Structure Navigator again.

- From the menu bar, select [View] > [System Structure Navigator].

ModPack Navigator

In ModPack Navigator, ModPacks are listed for each status.

TIP

The Change Management Package is required in order to use ModPacks.

The following figure shows ModPack Navigator.

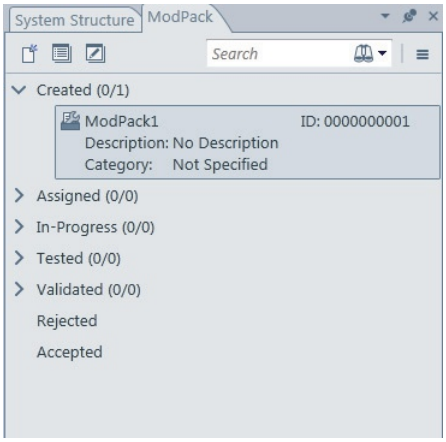


Figure B3.1.1-3 ModPack Navigator

Perform the following operation to display the closed ModPack Navigator again.

- From the menu bar, select [View] > [ModPack Navigator].

Display in the navigation window

In the navigation window, the following icons are shown:

- Check-out icon
  Indicates that files are currently checked-out.
- Work status icon
  Indicates that an RS generation is required.

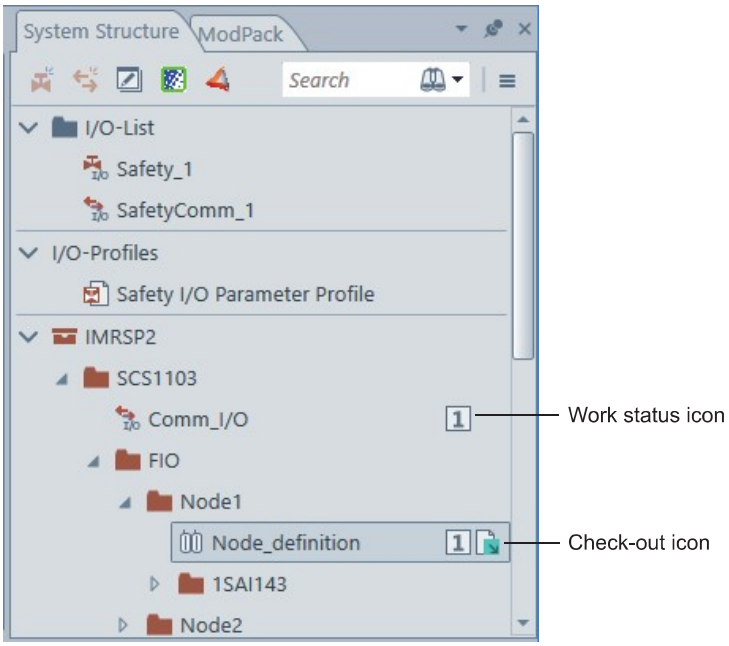


Figure B3.1.1-4 Display example of icons in the navigation window

SEE ALSO

For more information about check-out, refer to:

"■ File management with check-out and check-in" on page B4-3

For more information about RS generation, refer to:

D4., "Overview of RS generation" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

B3.1.2 Properties window

The Properties window displays the properties of files and folders selected in the navigation window.

Properties which can be changed can be edited in the Properties window.

The following figure shows the Properties window.

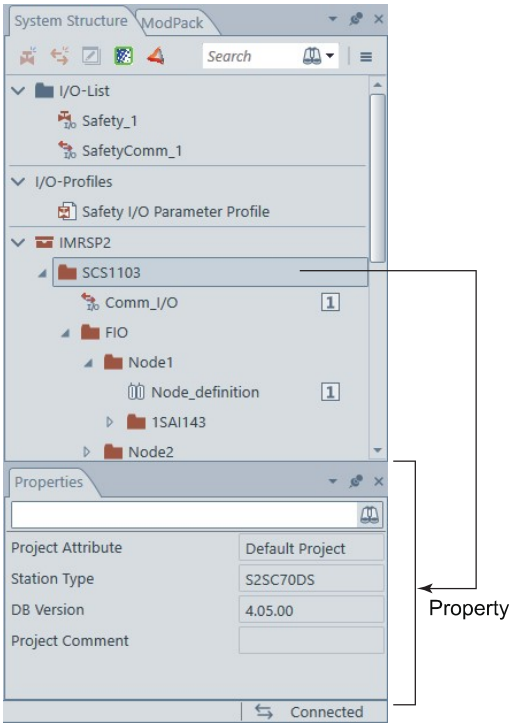


Figure B3.1.2-1 Properties window

Perform the following operation to display the Properties window:

- From the menu bar, select [View] > [Properties Window].

TIP

If an iDefine configuration node is selected, iDefine Project and the Build Revision are shown in the Properties window.

B3.1.3 Message window

The Message Window displays the progress and results of processing in the form of text.

The following figure shows the Message Window.

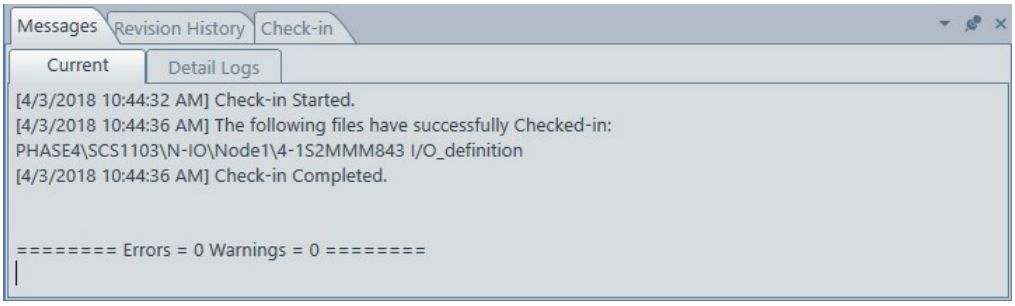


Figure B3.1.3-1 Message window

Perform the following operation to display the closed Message Window again.

- From the menu bar, select [View] > [Message Window].

B3.1.4 Revision History window

The Revision History window displays the revision history of files and information regarding labels.

The following figure shows the Revision History window.

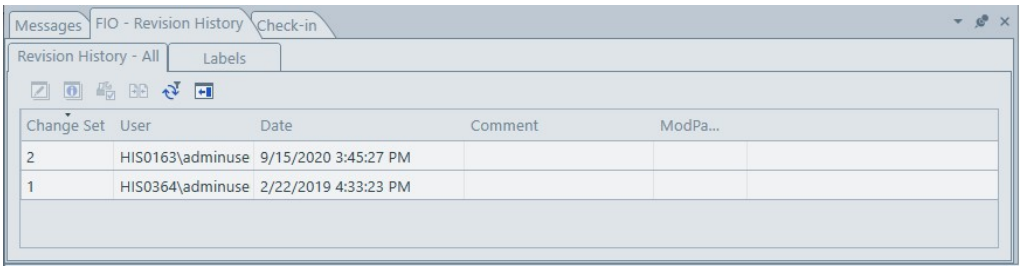


Figure B3.1.4-1 Revision History window

Perform the following operation to display the Revision History window:

- From the menu bar, select [View] > [Revision History Window].

SEE ALSO For more information about the items displayed in the Revision History window, refer to:

C2.9.1, “Displaying the Revision History window” on page C2-19

B3.1.5 Work Status List window

In the Work Status List window, a work file list is displayed. Also, from the Work Status List window, a work file list can be exported.

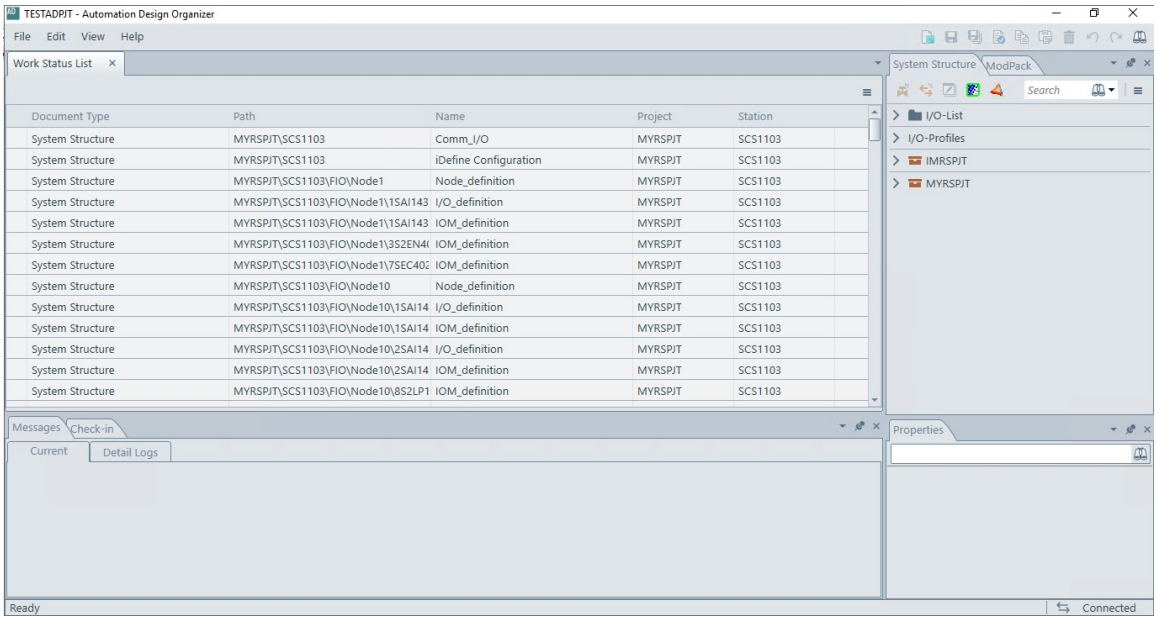


Figure B3.1.5-1 Work Status List window

Displaying the Work Status List window

Perform this step to display the Work Status List window:

- From the menu bar of AD Organizer, select [View] > [Work Status List Window].

Exporting a work file list

Follow these steps to export a work file list:

1. In the Work Status List window, click the Sub menu button and select [Export].
   The Choose a folder dialog box appears.
2. Select the folder to which you want to export the file and click [OK].
   The contents displayed in the Work Status List window are exported as a CSV file.

Format of the exported files

Exported files are created in the following format:

- File format
  CSV format
- Extension
  csv
- File name
  The file name will be as follows:

  `yyyy-MM-dd-hh-mm_WorkStatusList.csv`

  yyyy, MM, dd, hh, and mm indicate year, month, day, hour, and minute, respectively.

  Example: `2020-11-30-17-15_WorkStatusList.csv`

B3.1.6 Check-in window

The Check-in window displays a list of the files that are checked-in.

You can perform the following operations in the Check-in window:

- Check-in
- Discard Check-out
- Start the editor
- Compare with the latest of the server

The following figure shows the Check-in window:

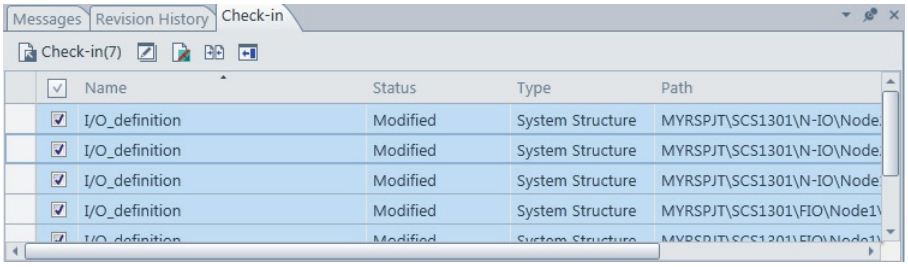


Figure B3.1.6-1 Check-in window

Perform the following operation to display the Check-in window:

- From the menu bar, select [View] > [Check-in Window].
  When a check-in is successful, a new Change Set ID is automatically generated sequentially.

SEE ALSO

For more information about Change Set ID, refer to:

"■ Saving of Change Sets" on page C2-16

For more information about check-in operation, refer to:

"■ Checking in manually" on page B4-9

For more information about check-in cancellation operation, refer to:

"■ Discarding a check-out" on page B4-5

For more information about procedures of operations for comparing files, refer to:

"■ Displaying comparisons with the Check-in window" on page B3-15

■ Items displayed in the Check-in window

The following table shows the items displayed in the Check-in window.

Table B3.1.6-1 Items displayed in the Check-in window

Item	Description	Remarks
Name	File name	-
Status	File status	There are the following types: • Modified • Not Modify
Type	File type	There are the following types: • System Structure • ModPack • Grid Rule
Path	Tier level of tree display	-

Continues on the next page

Table B3.1.6-1 Items displayed in the Check-in window (Table continued)

Item	Description	Remarks
Modified Date	Date and time of the last modification	-

B3.1.7 Operation in the tool window area

This section describes the operation of the tool window area.

Displaying the sub menu

Clicking on the Sub menu button in the top right of the window displays a sub menu.

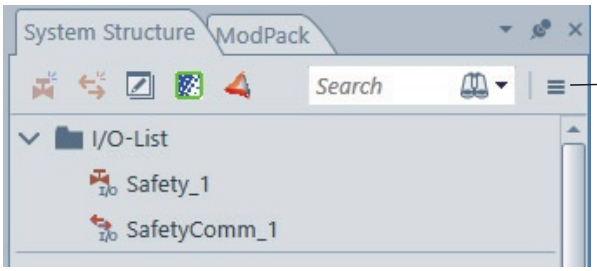


Figure B3.1.7-1 Sub menu button

Floating a window

Perform the following operation to switch the screen of the tool window area to a floating window:

- Right-click on the tab and select [Float].

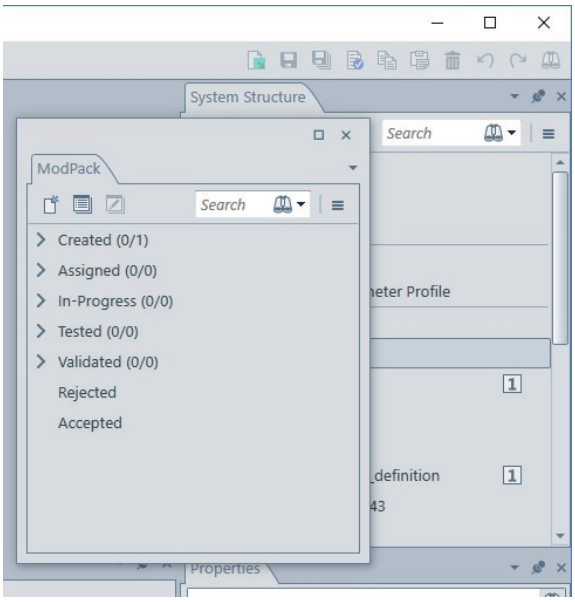


Figure B3.1.7-2 Floating window

Docking a floating window

Follow these steps to dock a floating window:

1. You can drag the floating window and move it above the window you wish to dock the floating window to.
   The region of the window you wish to dock the floating window to is displayed in white.
2. You can drop the floating window in the region displayed in white.

Automatically hiding a window

Perform the following operation to automatically hide a window:

- In the top right of the window, click [Auto Hide].

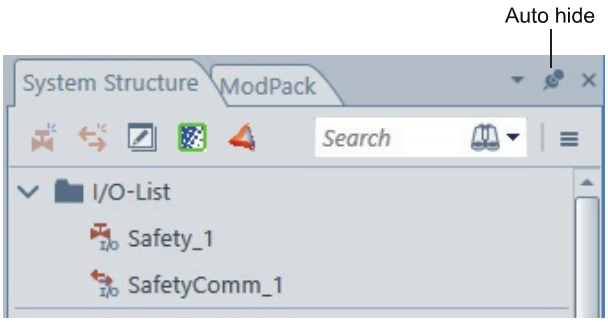


Figure B3.1.7-3 Auto hide

Windows from which the focus is removed are automatically hidden. As an example, the following figure shows the state where the navigation window is hidden.

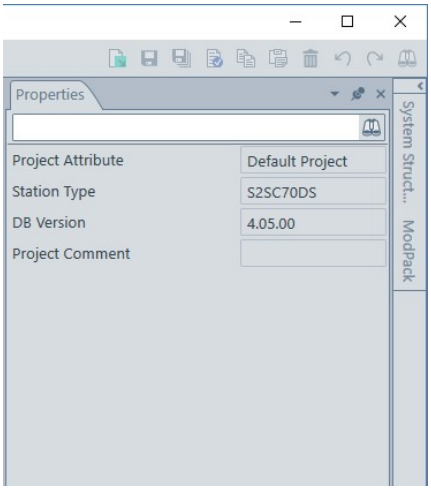


Figure B3.1.7-4 State where the navigation window is hidden

Moving the cursor above the window name at the edge of the screen displays the hidden window.

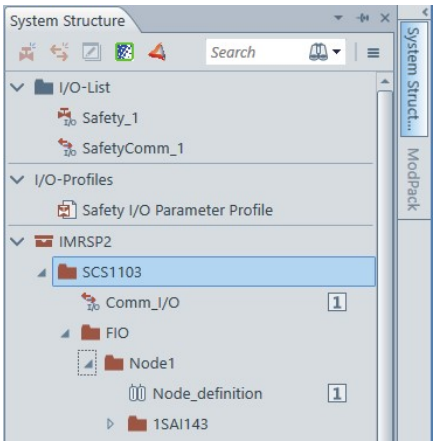


Figure B3.1.7-5 State where a hidden window is displayed

TIP

To cancel this behavior, click [Auto Hide] in the top right of the window.

B3.1.8 Compare the details of engineering data

The following files can be compared in the Check-in window and the Revision History window:

- Comparing the file currently checked out and the file saved to the ADMDB
  The file currently checked out and the latest file saved to the ADMDB can be compared on the local computer.

  The editor window of the latest file saved to the ADMDB appears on the left side, while the editor window of the file currently checked out appears on the right side of the comparison screen. You can edit the file currently checked out.

- Comparing files saved at two points in the past
  In the Revision History window, you can select and compare files saved at two different points.

  Alternately, when only one file is selected in the Revision History window, if the file currently checked out exists on the local computer, the comparison will be between the selected file and the currently checked out file. If no file is currently checked out, the selected file is compared against the latest file saved to the ADMDB.

  The editor window of the older file appears on the left side, while the editor window of the newer file appears on the right side of the comparison screen. If the newer file is currently checked out, you can edit the file.

TIP

To select a file in the Revision History window, select Revision History on the Revision History tab sheet or select Label on the Label tab sheet.

Displaying comparisons with the Revision History window

Follow these steps to display comparisons with the Revision History window:

1. Display the Revision History in the Revision History window.
2. Select the files to compare.
   You can select one or two files. To select the second file, select the file while holding down the [Ctrl] key.
3. Click the [Comparison] tool button.
   The results of the comparison are displayed.

Displaying comparisons with the Check-in window

The file being edited against the latest file checked-in on AD Server can be compared in order to confirm the changes.

Follow these steps to display comparisons with the Check-in window:

1. You can click and select the file you wish to compare in the Check-in window.
2. In the toolbar of the Check-in window, click [Compare with latest server copy].
   The results of the comparison are displayed in the Document window area.

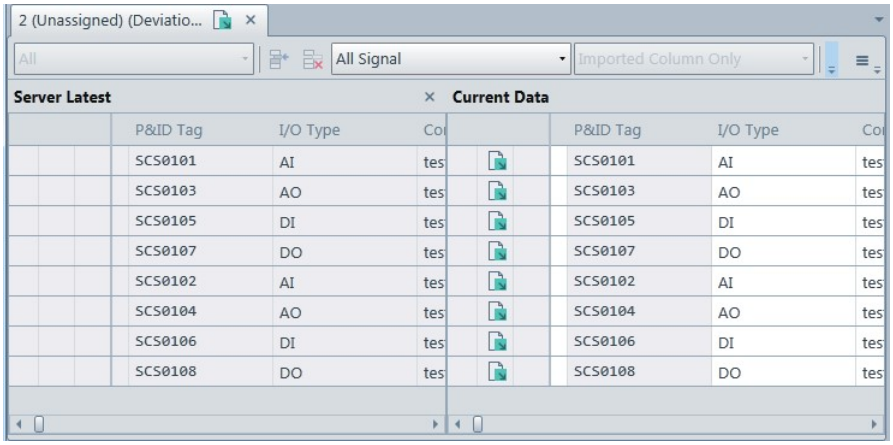


Figure B3.1.8-1 Example of comparison results

B3.2 Document window area

Windows for editing and browsing are displayed as tabs in the document window area. The following shows the windows that are used in each step.

- I/O design
  - Safety I/O Editor
  - Safety Communication I/O Editor
  - IOM Definition Editor
  - Safety I/O Parameter Profile Editor
- Change management
  - ModPack Editor

TIP

A maximum of 10 files can be displayed for editing in the document window area.

B3.2.1 Display and operations of the document window area

This section describes the display and operations of the document window area.

Status display of the tabs

This section describes the status display of the tabs.

Checked-out status

As shown in the following, files that are checked-out are marked with a checked-out status icon in the tabs:

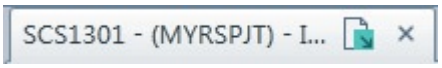


Figure B3.2.1-1 Tab of a file currently checked out

State where changes have not been saved

Tabs of files for which changes made with editing have not been saved are marked with an asterisk (*) before the file name.

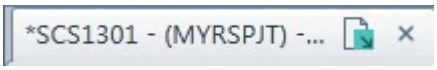


Figure B3.2.1-2 Tab of a file for which changes have not been saved

Operating the tabs

This section describes how to operate the tabs in the document window area.

Operations for floating, docking, and displaying the sub menu are the same as those for the tool window area.

Tab groups

The display of multiple files can be switched with tab operations in the document window. These multiple files for which the display can be switched by using tab operations are referred to as tab groups. The following tab groups contain two files:

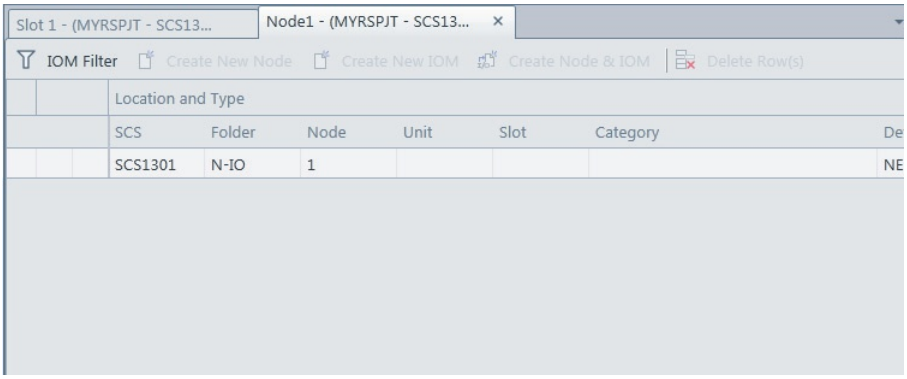


Figure B3.2.1-3 Tab group

Selecting a file to edit from the list of file names

To change the file subject to editing, you can click the tab of the file you wish to edit.

When many tabs are displayed, only a part of the file names may be displayed. In such case, follow these steps to select the file you wish to edit:

1. You can click on the triangular symbol located on the right edge of the tab section.
   A list of the file names belonging to the same tab groups are displayed in the drop-down list.

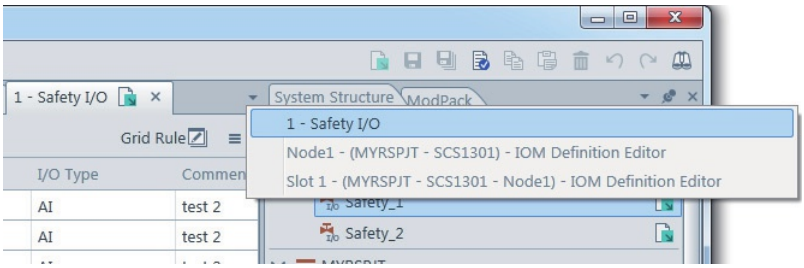


Figure B3.2.1-4 Displaying the list of file names

2. Select the file you wish to edit from the drop-down list.
   The selected file is displayed.

Splitting the document window

You can horizontally or vertically split the document window to display multiple files next to each other.

TIP

You cannot split the display of a single file.

You can perform one of the following operations to split the display of the document window:

- Right-click on the tab and select [New Horizontal Tab Group].
  The document window is split horizontally and a new tab group is created on the bottom. The tab on which you right-clicked moves to the new tab group.

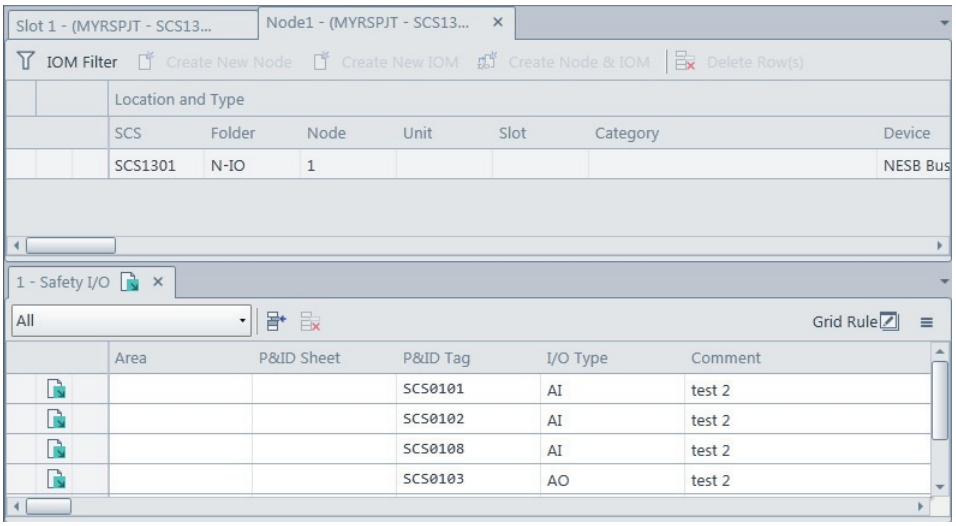


Figure B3.2.1-5 Horizontally split document window

- Right-click on the tab and select [New Vertical Tab Group].
  The document window is split vertically and a new tab group is created on the right. The tab on which you right-clicked moves to the new tab group.

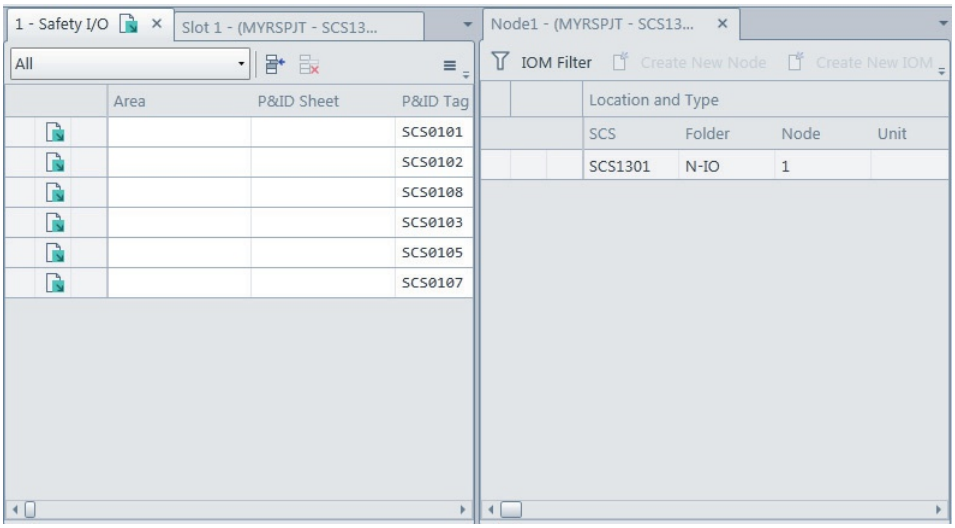


Figure B3.2.1-6 Vertically split document window

TIP

- When splitting the display into more than two, the direction in which the displays are split cannot be mixed. For example, when the display is first split horizontally, you cannot choose an operation other than [New Horizontal Tab Group].
- If two or more files are not included in the tab group before the display is split, right-clicking does not display [New Vertical Tab Group] or [New Horizontal Tab Group].

Moving to a different tab group

To move a tab to a different tab group, perform one of the following operations:

- Right-click on the tab and select [Move to Next Tab Group].
  The selected tab moves to the next tab group.
- Right-click on the tab and select [Move to Previous Tab Group].
  The selected tab moves to the previous tab group.

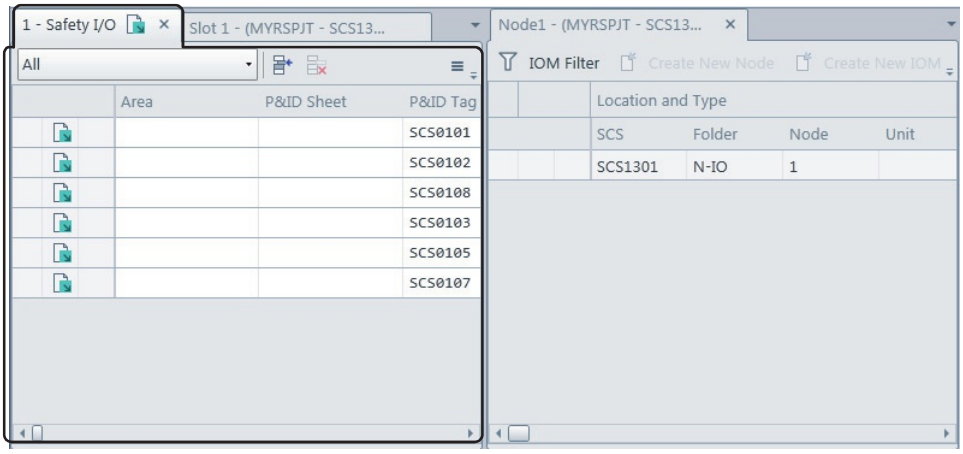


Figure B3.2.1-7 Before the operation for moving the tab group

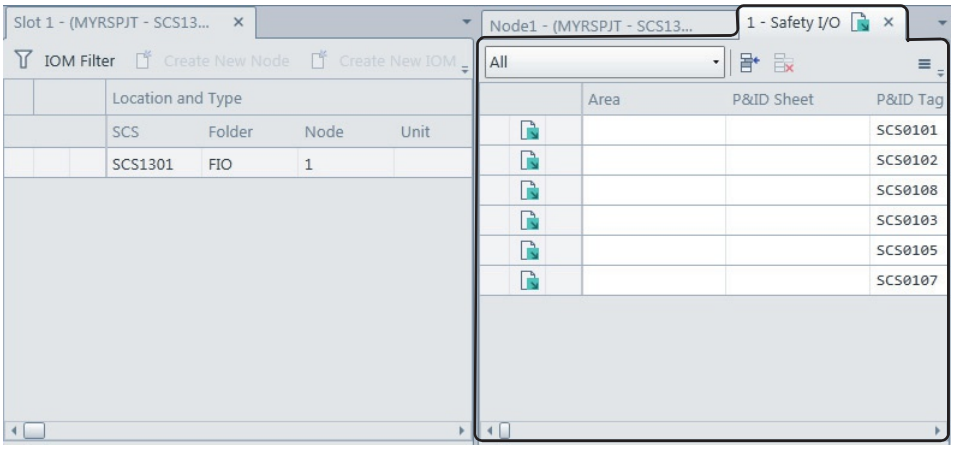


Figure B3.2.1-8 After the operation for moving the tab group

Deleting a tab group

A tab group is deleted when the number of tabs belong to that tab group becomes zero.

To delete a tab group, perform one of the following operations:

- You can move all of the tabs belonging to the tab group you wish to delete to a different tab group.
- You can close all of the tabs belonging to the tab group you wish to delete.

B3.3 Status bar area

In the status bar area, the status of connection with AD Server is displayed in the following manner:

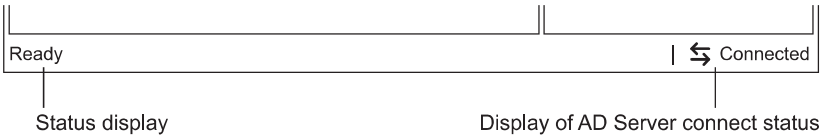


Figure B3.3-1 Status bar area

- Connected
  AD Organizer is connected to AD Server.
- Not connected
  AD Organizer is not connected to AD Server.
- Busy
  AD Organizer is connected to AD Server but is performing another process.

B4. Operating AD Organizer

This section describes the common operations of AD Organizer.

B4.1 Modifying an AD project subject to editing

Follow these steps to modify an AD project with AD Organizer:

1. In the menu bar of AD Organizer, select [File] > [Change AD project].
   The Select AD Project dialog box appears.

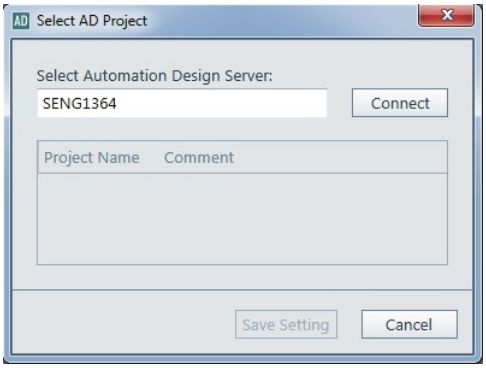


Figure B4.1-1 Select AD Project dialog box

2. Select the computer name or IP address of the computer with AD server, and click [Connect].
   AD projects that are created in AD Server appear.

TIP

If you want to set a port number, type a colon : and the port number after the computer name or the IP address.

3. Click the AD project you wish to edit.
4. Click [Save Setting].
5. Restart AD Organizer.
   The AD project subject to editing is modified.

TIP

The AD project you wish to edit is not modified until AD Organizer is restarted.

B4.2 Editing a file with AD Organizer

To edit a file with AD Organizer, you can perform operations in the order to check-out, edit, save, and check-in.

TIP

How to create a new file differs depending on the file you wish to create.

File management with check-out and check-in

In AD Organizer, multiple users can simultaneously work on a single AD project. However, simultaneous editing of a single file by multiple users is prohibited. The system of check-out and check-in is used to ensure that a single file is edited by only a single user.

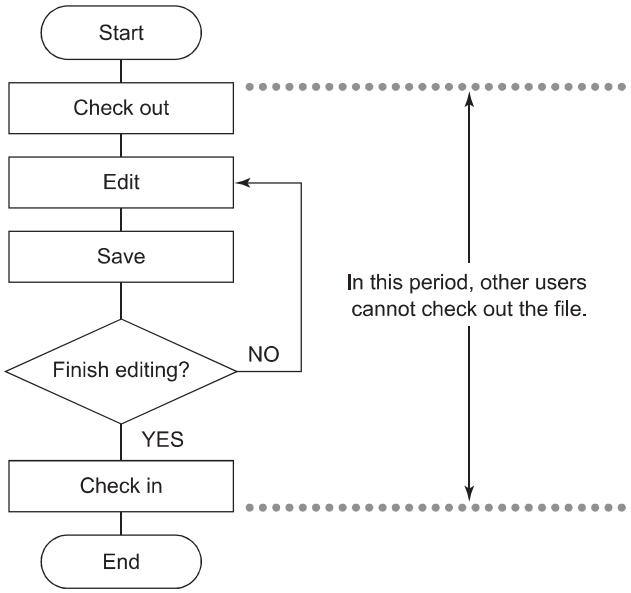


Figure B4.2-1 Flow of file editing using check-out and check-in

Check-out

To edit a file, check-out the file with AD Organizer.

- Files that are not checked-out cannot be edited.
- Files that are checked-out can be edited by only the user that has checked-out the file.
- Other users are not able to check-out this file until the checked-out file is checked-in or until the checked-out status is discarded.

Save

Edited files are saved on the computer running AD Organizer. Simply saving the file does not store the edited file in the AD project. The checked-out status of the file will also be continued.

Check-in

Operating a check-in stores the file saved on the computer running AD Organizer in the AD project on AD Server.

IMPORTANT

Only the checked-in files are subject to RS generation. After completing an edit, you must perform a check-in.

Also when referencing files generated with another editor or window, only the files that have been checked-in are subject to such referencing. Referencing cannot be run when the file subject to the referencing is checked-out.

● Recording check-in information in a ModPack

Instructions and results regarding modification tasks can be recorded in a ModPack.

As results of modification tasks, the check-in information of the file at the time of check-in can be recorded in a ModPack.

SEE ALSO For more information about ModPack, refer to:

D., “ModPack change management” on page D-1

For more information about how to associate change tasks to a ModPack, refer to:

“■ Procedure for modification of objects that are handled by AD Organizer” on page D2-7

■ Manual check-out/check-in and automatic check-out/check-in

Check-out and check-in operations can be performed either manually or automatically. By default, manual check-out/check-in is selected.

TIP This manual explains assuming manual check-in and manual check-out. If you have set up automatic check-out, you will not see the Check-out dialog box, which confirms your check-out. If automatic check-in is not set, check-in operation is required.

Perform this step to switch between manual and automatic check-out/check-in:

- On the menu bar in AD Organizer, select [File] > [Auto Check-Out / Check-In].
  The automatic check-out/check-in is selected. Each time this operation is repeated, check-out/check-in is switched between manual and automatic. When the automatic check-out/check-in is selected, a check mark is added to the [Auto Check-Out / Check-In] menu.

TIP Check-out and check-in cannot be in different operating modes.

SEE ALSO For more information about details of check-out, refer to:

B4.2.1, “Check-out” on page B4-5

For more information about details of check-in, refer to:

B4.2.4, “Check-in” on page B4-9

■ Groups of check-out and check-in

Normally, check-out and check-in are performed in units of files. However, files can be grouped and check-out and check-in can be performed in units of such groups.

B4.2.1 Check-out

This section describes how to check out files and discard the check-out. The check-out method can be selected either manually or automatically check out depending on the settings. By default, manual check-out is selected.

■ Checking out manually

Perform one of the following steps to check out files manually:

- You can right-click on the file you wish to check-out in the navigation window and select [Check-out].
- When the file you wish to check-out is displayed in the document window area, you can click the [Check-out] button on the toolbar.
- By editing a file that has not been checked out, the "Check-out" dialog box appears. Click [Yes] in the "Check-out" dialog box to perform the check-out.

Files that have been checked-out are added to the list in the Check-in window.

TIP

With the following operation, check-out and check-in are automatically run and the data of AD Server is updated.

Table B4.2.1-1 Operations with which check-out and check-in are automatically run

Window name	Operation
System Structure Navigator	Creating and deleting a safety I/O list Creating and deleting a safety communication I/O list
ModPack Navigator	Creating and deleting a ModPack
Properties Window	Modifying properties
Safety I/O Editor Safety Communication I/O Editor IOM Definition Editor	Creating and deleting the following items in relation to System Structure Navigator • Node folder • Node • I/O module folder • I/O module
Revision History window	Assigning a ModPack Editing the check-in comment.

■ Checking out automatically

When the automatic check-out/check-in is selected, you can check out files without the check-out operation. This applies to all the AD Organizer editors.

SEE ALSO

For more information about how to switch between manual and automatic check-out, refer to:

"■ Manual check-out/check-in and automatic check-out/check-in" on page B4-4

■ Discarding a check-out

Follow these steps to discard the check-out of individual files:

1. From the list of files in the Check-in window, select the check box of the file for which you want to discard the check-out.
2. On the toolbar of the Check-in window, click [Discard Check-out].
   The Discard dialog box appears.

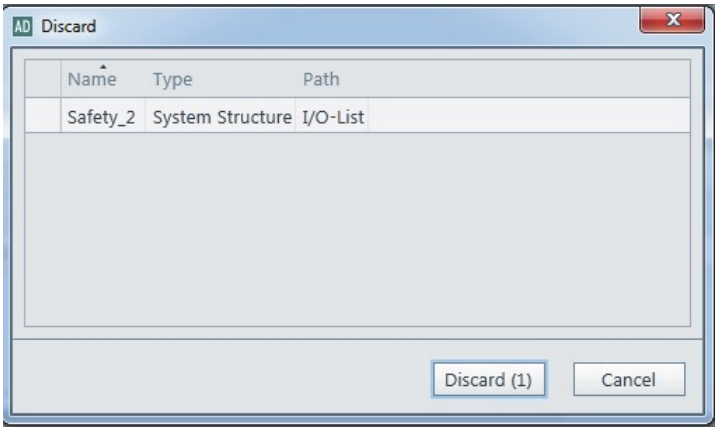


Figure B4.2.1-1 Discard dialog box

TIP

On the [Discard] button, the number of files for which you will discard the check-out is displayed in the brackets. This display example indicates that there is one file for which the checked-out is being discarded.

3. Click [Discard].
   The check-out is discarded and the content edited after the check-out are discarded.

SEE ALSO

For more information about how to cancel the checked-out status of files that are checked out by a certain user all at once, refer to:

C1.2.5, “Forcibly canceling the checked-out status of currently checked-out files” on page C1-44

B4.2.2 Edit

To edit a file that has been checked-out, perform one of the following operations:

- From the list of files in the Check-in window, you can select the file you wish to edit and click [Launch Editor] in the toolbar of the Check-in window.
- In the navigation window, double-click on the file you wish to edit.

TIP If a file that has already been opened with AD Organizer is specified, that window is displayed.

Tasks to perform after the file has been opened differ depending on the file being edited.

Undoing the last editing action

To undo the last editing action, click the [Undo] button on the toolbar. To cancel the undo operation, click the [Redo] button on the toolbar.

TIP Clicking [View] > [Update] initializes the record of operations and makes it impossible to click the [Undo] button.

Checking the validity of a file

Files that have been created or edited by using AD Organizer can be checked for non-configured cells, formats, ranges, duplexing, whether the P&ID tag is unique within the P&ID group, and whether items such as the type of node for every slot are appropriate.

You can check whether these items in the iDefine-config file that was imported by using AD Organizer follow the naming convention rules. The iDefine-config file is a file that was generated from the data that was engineered by using iDefine.

- Variable name
- Variable comment
- Variable group name
- Settings for defined words (Word, Equivalent, Comment)
- POU name
- FU and FB parameter name
- FU and FB parameter comment
- FU and FB parameter short name
- Tag name and variable name for the Tag Name Builder

Follow this step to check the validity of a file being edited:

- On the toolbar, click [Validity Check].

TIP If the file has not been saved after editing, the Save confirmation dialog box appears before the validity check.

The results of the validity check are displayed in the Message window.

When an error is returned with the validity check, you can correct the file by following the message that is displayed.

B4.2.3 Save

This section describes how to save a single file that is currently being edited and how to save all files that have been modified.

Saving a file being edited

To save a file being edited, perform the following operation:

- On the toolbar, click [Save].
  The file will be saved after the validity check is performed.

TIP Files for which an error is returned with the validity check are not saved.

Save all files that have been modified

Follow these steps to save all files in the document window area that have been modified.

1. On the toolbar, click [Save All].
   A dialog box to confirm the save appears.
2. Click [Yes].
   All files that have been modified are saved after a validity check is performed.

TIP Files for which an error is returned with the validity check are not saved.

B4.2.4 Check-in

The Check-in Window is where you can check in files. By setting the check-in method, you can select to check in manually or automatically. By default, manual check-in is selected.

TIP

Files that have not been saved are saved before the check-in.

Prior to check-in, a validity check is performed with the files being checked-in. Files for which an error are returned with the validity check are not checked-in.

When checking in to an SCS project created with I/O list engineering, check in upon placing labels on the safety I/O list, safety communication I/O list, and IOM information.

After check-out, the safety I/O list, safety communication I/O list, and IOM information can be returned by AD Organizer based on these labels.

SEE ALSO

For more information about how to set labels, refer to:

C2.8, “Setting labels” on page C2-17

Checking in manually

Follow these steps to perform a check-in manually:

1. When the Check-in window is not displayed, select [View] > [Check-in Window] from the menu bar.
2. On the Check-in window, you can select the check boxes of the files you wish to check-in.
3. Click the [Check-in] button.

TIP

On the [Check-in] button in the Check-in Window and the [Check-in] button in the Check-in dialog box, the number of files to be checked in is displayed in parentheses. This display example indicates that there are two files which are being checked-in.

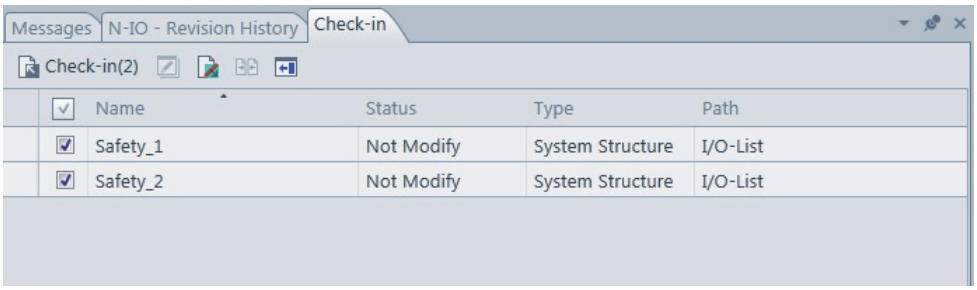


Figure B4.2.4-1 The [Check-in] button in the Check-in window

The Check-in dialog box appears.

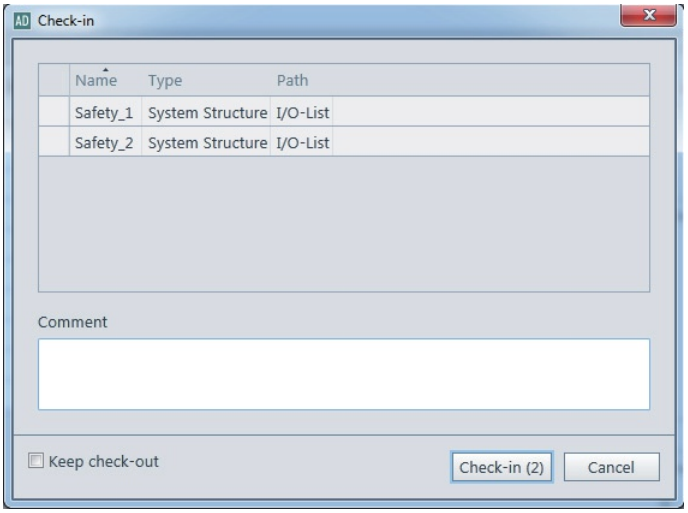


Figure B4.2.4-2 Check-in dialog box

4. Enter a comment.
5. If you wish to continue editing the file after checking in, select the [Keep check-out] check box.
   The file will be checked-out automatically after the check-in, so that you can continue editing of the file.
6. Click the [Check-in] button.
   The check-in is run.

TIP The information of a check-in that has been run can be viewed in the Revision History window.

Checking in automatically

If automatic check-out/check-in is selected, the file is automatically checked in when you save it. The following editors support automatic check-in.

- Safety I/O Editor
- Safety Communication I/O Editor
- IOM Definition Editor

B4.3 Changing the data display method of AD Organizer

By changing the display of AD Organizer, you can find data more easily. This section describes how to find data and how to sort or filter data.

B4.3.1 Performing a search

This section describes how to perform a search with AD Organizer.

Performing a search with the navigation window

This section describes how to perform a search with the navigation window.

Searching for a file name or folder name with the navigation window

Perform the following operations to search for a file name or folder name with the navigation window.

- Enter the name to search for in the search field at the top of the navigation window and press the Enter key.
  If file names or folder names include the search term in its name, the file name or folder names are highlighted as shown in the following figure:

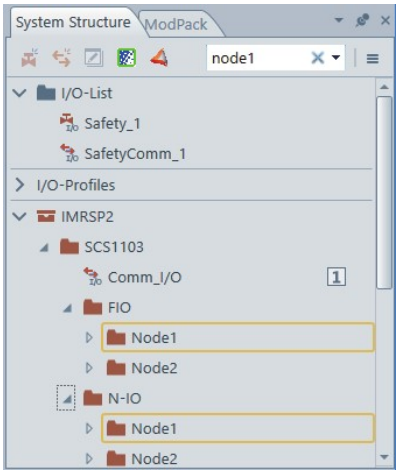


Figure B4.3.1-1 When search results are displayed

If file names or folder names that include the search term in its name exist under the folder and are not expanded, the folder containing the subject of the search is highlighted as shown in the following figure:

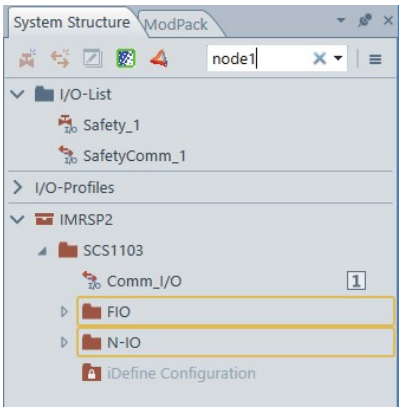


Figure B4.3.1-2 When search results are hidden under a folder

Searching for definition contents with the navigation window

P&ID Tag and I/O Tag can be specified as a search target with System Structure Navigator. The scope of search is the following editors and files:

Table B4.3.1-1 Search scope

Target editor name	Target file name
Safety I/O Editor Safety Communication I/O Editor	Safety_{P&ID Group} SafetyComm_{P&ID Group} Comm_I/O I/O_definition

Perform this step to run the search:

- Enter the search target such as P&ID tag in the search field at the top of the System Structure Navigator and press the [Enter] key.
  Files that include the search target are highlighted as shown in the following figure:

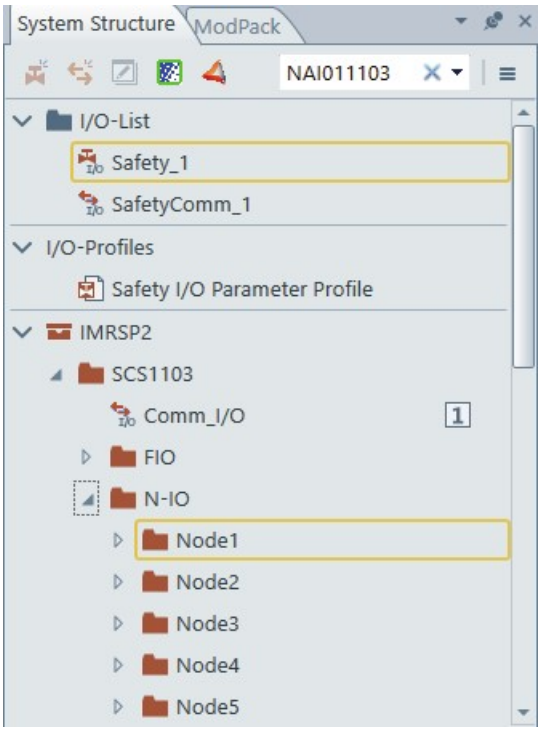


Figure B4.3.1-3 Search results

Searching for a property name in the Properties window

Perform the following operation to search for a property name in the Property window.

- In the search field at the top of the Property window, you can enter the property name you wish to search.
  A search is performed and candidates are displayed every time a character is entered.

Searching for a file being edited in the document window area

Follow these steps to search for a file being edited in the document window area.

1. Click the document window area.
2. On the toolbar, click [Search in Editor].
   The Search in Editor dialog box appears.

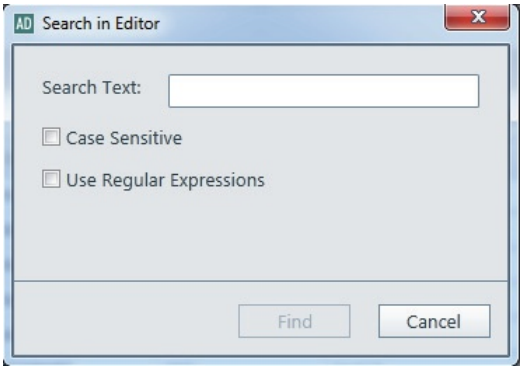


Figure B4.3.1-4 Search in Editor dialog box

3. Select the [Case Sensitive] check box to perform a case-sensitive search.
4. Select the [Use Regular Expressions] check box to use official wording for the search term.
5. Enter the search term in the search dialog and click the [Find] button.
   The search results are displayed.

● Elements of official wording

Elements of regular expression usable are as follows:

- .: It matches any one character.
- [Character group]: It matches any one character included in the bracket.
- \bstring: Look for a word that starts with the specified string.
- string\b: Look for a word that ends with the specified string.
- \bstring\b: Look for a word that matches the specified string.
- [First character - last character]: It matches any of a character in the range of the first character to the last character.
- [^character group]: It matches one character that is not included in the bracket.
- {m,n}: Check that the previously specified element occurs in a range of the minimum m times to the maximum n times.
- {m,}: Check that the previously specified element occurs at the minimum m times.
- {n,}: Check that the previously specified element occurs at the maximum n times.

TIP When you specify "." or "\" as a character, add "\" in front.

■ Searching for a column by column name on the editor

For the following editors, you can search for a column by column heading:

- Safety I/O Editor
- Safety Communication I/O Editor

Follow these steps to search for a column:

1. Right-click on any location of editor and select [Find Column].
   The sub menu appears.
2. Enter a column title to search in the sub menu.
   Matched candidates appear in a list every time the title is entered.
3. Fix the column title to search.

The screen is scrolled to the corresponding column title position, and the background color of title is displayed in yellow.

TIP

- Columns set to hide by a filtering function are not search targets.
- If you want to search for a user-defined column that has an alias name set, the column title to search is the alias name.

B4.3.2 Sorting rows by a specified column

You can sort the rows by a value of one column or by values of multiple columns.

Sorting by a single column

Perform this step to sort the rows by the values of a specified column:

- Click a column heading.
  Each time the column heading is clicked, the order of rows switches to ascending order, descending order, and unsorted status.

Sorting by multiple columns

For the following editors, you can sort the order of rows by multiple columns:

- Safety I/O Editor
- Safety Communication I/O Editor

Follow these steps to sort the rows by specifying multiple columns:

1. Click a heading of any one column.
2. Click a heading of another column while pressing the [Shift] key. You can combine up to ten columns.

TIP

- The sort order is displayed with numbers in the column heading.
- Each time you click the column heading for sorting while pressing [Shift] key, the order of rows switches between ascending and descending order.
- If you click the column heading for sorting without pressing [Shift] key, the rows are sorted by a single column.
- If the editor is in a comparison mode, only the right view (current data) is sorted.
- To reset the sort, click the [Sub menu] button and select [Reset to default display setting].
- Sorted status is not maintained. When you exit the editor and restart it, the display returns to the default status.

B4.3.3 Displaying filtered data

Rows can be filtered by using the Filter icon in the column heading or selecting cells. In the Filter setting dialog box, you can select the check boxes of the column values to be displayed or specify conditions for displaying.

Filtering by using the Filter icon in the column heading

Follow these steps to filter rows by using the Filter icon in the column heading:

1. Click the Filter icon in the column heading.
   The Filter setting dialog box appears.

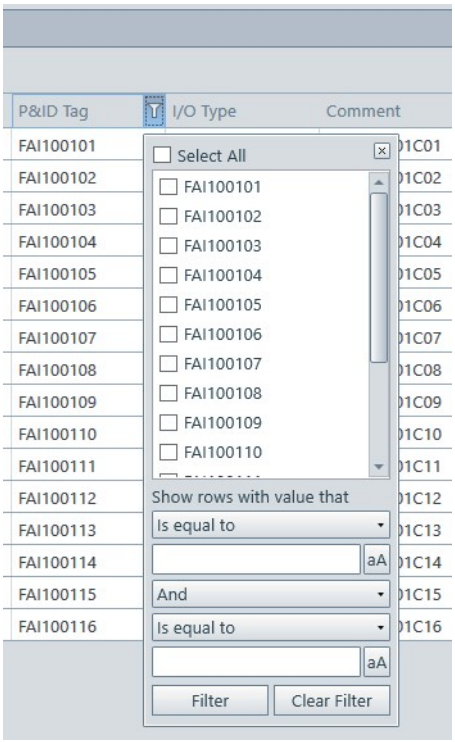


Figure B4.3.3-1 Filter setting dialog box

2. Select the filtering targets.
3. Select the types of filter.
4. Enter the values, and click [Filter].

TIP

When the display of rows is being filtered, the Filter icon is displayed in the heading line.

To remove the filter, click the Filter icon to display the Filter setting dialog box and click [Clear].

Filter setting dialog box

The Filter setting dialog box is displayed when you perform the filtering operation. You can select the check boxes of the values to be displayed or specify conditions for displaying.

TIP

If you specify both of check boxes and conditions, the rows that satisfy both conditions appear.

1. To select values by the check boxes, select the check boxes of the values that you want to display and clear the check boxes of the values that you do not want to display from the displayed list.

TIP If the number of selectable values exceeds 1000, this list is not displayed.

2. To set a filter by using conditions, perform these steps:
   a. From the drop-down list, select conditions.
      You can use the following conditions:
      - Is equal to
      - Is not equal to
      - Starts with
      - Ends with
      - Contains
      - Does not contain
      - Is contained in
      - Is not contained in
      - Is empty
      - Is not empty
      - Is less than
      - Is less than or equal to
      - Is greater than
      - Is greater than or equal to
      - Is null
      - Is not null

   b. If you need to specify a value, enter the value in the text box.
   c. If you want to distinguish between upper case and lower case letters for the entered value, click [aA] shown next to the text box.
      Case Sensitive and Not Case Sensitive are switched.

      When the color of [aA] is dark, it is in Case Sensitive status.
   d. Up to two conditions can be specified. When you specify the second condition, select the relationship of two conditions from the drop-down list.
      You can use the following relational expressions:
      - And
      - Or

   e. If you need the second condition, set it in the same way as the first condition.
3. Click [Filter].
   Display of rows is filtered.

Filtering rows by a value of selected cell

For the following editors, you can filter the rows by values:

- Safety I/O Editor
- Safety Communication I/O Editor

There are the following two types of filters:

- [Filter by Selection]

- [Filter Excluding Selection]

Perform this step to filter the rows by a value:

1. Select a cell. You can also specify multiple cells. Right-click on the selected cell and select a type of filter.
   Rows are filtered according to your designation.

TIP

- The value of the selected cell and the type of filter are reflected in the Filter setting dialog box.
- To remove the filter, right-click the cell and select [Remove Column Filter].

B4.3.4 Operating the columns

This section describes the column operations that are common to editors.

Changing the position of a column

Perform this step to change the position of a column:

- Drag the header of the column you want to change and drop it to a desired position.

TIP

- With this operation, the position of the column is retained. If you close the table format window and open it again, the column is displayed in the changed position.
- Column View scrolls automatically while dragging the column header to the left most/ right most of the Row Area.

Freezing columns to prevent them from scrolling during horizontal scroll

In the following editors, you can freeze columns to prevent them from scrolling during horizontal scroll.

- Safety I/O Editor
- Safety Communication I/O Editor
- Safety I/O Parameter Profile Editor

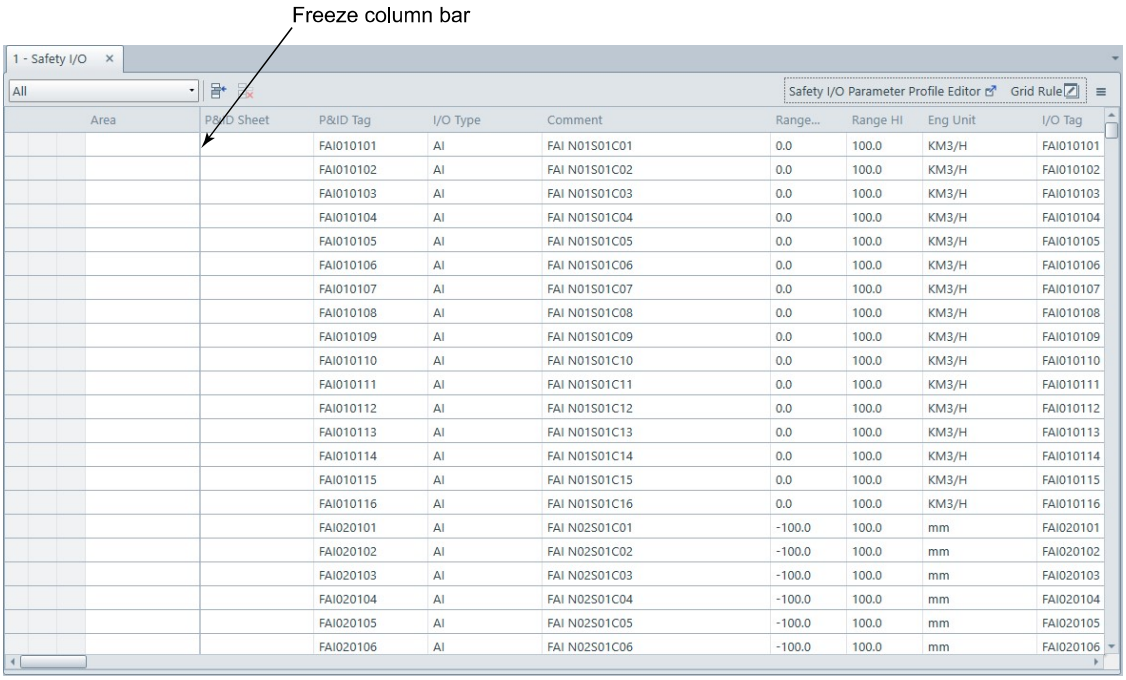
You can freeze columns by using one of the following two methods:

- Drag the freeze column bar to the right of the column you want to freeze
- Right-click the column header you want to freeze and select from the menu

Freezing columns by dragging the freeze column bar

Perform this step to freeze columns by dragging the freeze column bar to prevent it from scrolling during horizontal scroll.

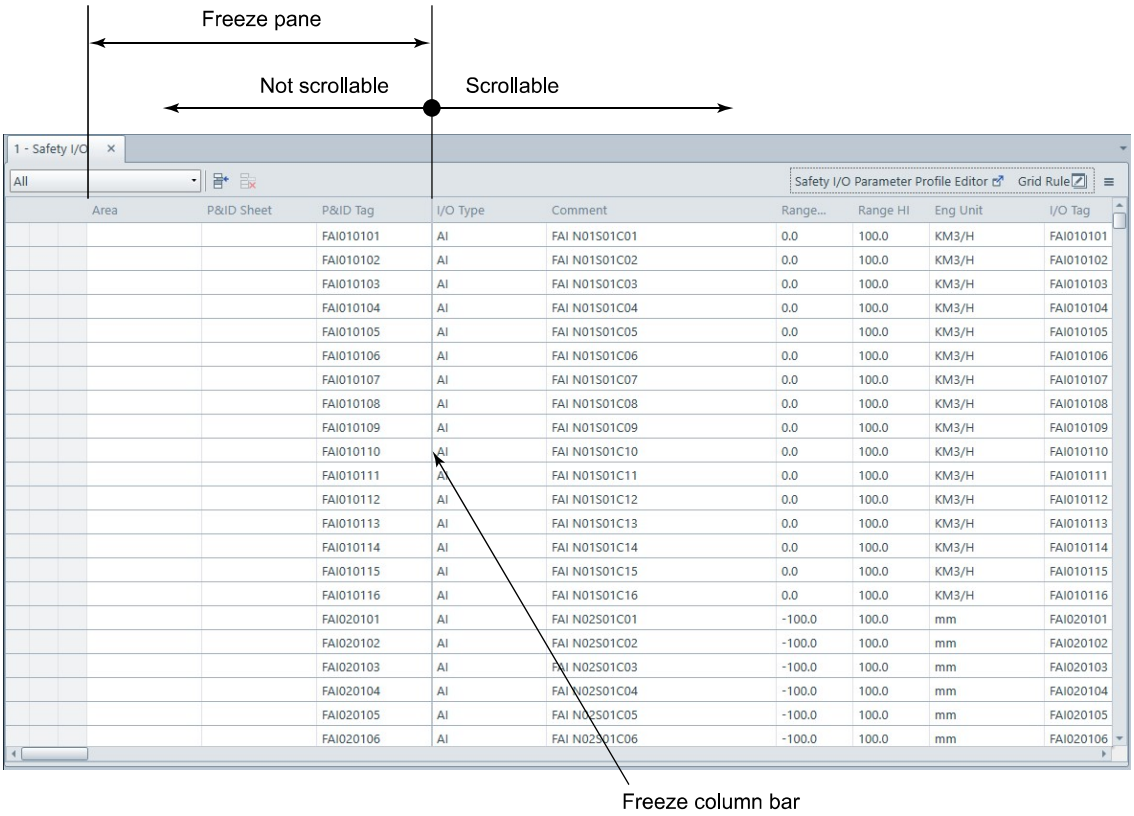
- Drag the freeze column bar on the left side of the screen and drop it on the right of the column you want to freeze.



Area	P&ID Sheet	P&ID Tag	I/O Type	Comment	Range...	Range HI	Eng Unit	I/O Tag
		FAI010101	AI	FAI N01S01C01	0.0	100.0	KM3/H	FAI010101
		FAI010102	AI	FAI N01S01C02	0.0	100.0	KM3/H	FAI010102
		FAI010103	AI	FAI N01S01C03	0.0	100.0	KM3/H	FAI010103
		FAI010104	AI	FAI N01S01C04	0.0	100.0	KM3/H	FAI010104
		FAI010105	AI	FAI N01S01C05	0.0	100.0	KM3/H	FAI010105
		FAI010106	AI	FAI N01S01C06	0.0	100.0	KM3/H	FAI010106
		FAI010107	AI	FAI N01S01C07	0.0	100.0	KM3/H	FAI010107
		FAI010108	AI	FAI N01S01C08	0.0	100.0	KM3/H	FAI010108
		FAI010109	AI	FAI N01S01C09	0.0	100.0	KM3/H	FAI010109
		FAI010110	AI	FAI N01S01C10	0.0	100.0	KM3/H	FAI010110
		FAI010111	AI	FAI N01S01C11	0.0	100.0	KM3/H	FAI010111
		FAI010112	AI	FAI N01S01C12	0.0	100.0	KM3/H	FAI010112
		FAI010113	AI	FAI N01S01C13	0.0	100.0	KM3/H	FAI010113
		FAI010114	AI	FAI N01S01C14	0.0	100.0	KM3/H	FAI010114
		FAI010115	AI	FAI N01S01C15	0.0	100.0	KM3/H	FAI010115
		FAI010116	AI	FAI N01S01C16	0.0	100.0	KM3/H	FAI010116
		FAI020101	AI	FAI N02S01C01	-100.0	100.0	mm	FAI020101
		FAI020102	AI	FAI N02S01C02	-100.0	100.0	mm	FAI020102
		FAI020103	AI	FAI N02S01C03	-100.0	100.0	mm	FAI020103
		FAI020104	AI	FAI N02S01C04	-100.0	100.0	mm	FAI020104
		FAI020105	AI	FAI N02S01C05	-100.0	100.0	mm	FAI020105
		FAI020106	AI	FAI N02S01C06	-100.0	100.0	mm	FAI020106

Figure B4.3.4-1 Initial state of the freeze column bar

The left side of the freeze column bar is called the freeze pane, and columns in the freeze pane are fixed without horizontal scroll. The right side of the freeze column bar scrolls horizontally.



Area	P&ID Sheet	P&ID Tag	I/O Type	Comment	Range...	Range HI	Eng Unit	I/O Tag
		FAI010101	AI	FAI N01S01C01	0.0	100.0	KM3/H	FAI010101
		FAI010102	AI	FAI N01S01C02	0.0	100.0	KM3/H	FAI010102
		FAI010103	AI	FAI N01S01C03	0.0	100.0	KM3/H	FAI010103
		FAI010104	AI	FAI N01S01C04	0.0	100.0	KM3/H	FAI010104
		FAI010105	AI	FAI N01S01C05	0.0	100.0	KM3/H	FAI010105
		FAI010106	AI	FAI N01S01C06	0.0	100.0	KM3/H	FAI010106
		FAI010107	AI	FAI N01S01C07	0.0	100.0	KM3/H	FAI010107
		FAI010108	AI	FAI N01S01C08	0.0	100.0	KM3/H	FAI010108
		FAI010109	AI	FAI N01S01C09	0.0	100.0	KM3/H	FAI010109
		FAI010110	AI	FAI N01S01C10	0.0	100.0	KM3/H	FAI010110
		FAI010111	AI	FAI N01S01C11	0.0	100.0	KM3/H	FAI010111
		FAI010112	AI	FAI N01S01C12	0.0	100.0	KM3/H	FAI010112
		FAI010113	AI	FAI N01S01C13	0.0	100.0	KM3/H	FAI010113
		FAI010114	AI	FAI N01S01C14	0.0	100.0	KM3/H	FAI010114
		FAI010115	AI	FAI N01S01C15	0.0	100.0	KM3/H	FAI010115
		FAI010116	AI	FAI N01S01C16	0.0	100.0	KM3/H	FAI010116
		FAI020101	AI	FAI N02S01C01	-100.0	100.0	mm	FAI020101
		FAI020102	AI	FAI N02S01C02	-100.0	100.0	mm	FAI020102
		FAI020103	AI	FAI N02S01C03	-100.0	100.0	mm	FAI020103
		FAI020104	AI	FAI N02S01C04	-100.0	100.0	mm	FAI020104
		FAI020105	AI	FAI N02S01C05	-100.0	100.0	mm	FAI020105
		FAI020106	AI	FAI N02S01C06	-100.0	100.0	mm	FAI020106

Figure B4.3.4-2 After dragging the freeze column bar

TIP

To unfreeze columns, drag the freeze column bar and drop it on the left end. The freeze column bar moves to the right side of a column that is always fixed, such as the Checked-out Status and Modification Status columns. You cannot move the freeze column bar to the left of the always-fixed column.

Freezing a column by selecting the right-click menu of the column header

Perform this step to freeze a column by selecting the right-click menu of the column header to prevent it from scrolling during horizontal scroll:

- Right-click the header of a column you want to freeze and select [Send to Freeze Pane]. The column moves to the leftmost of the freeze pane.

Unfreezing columns

You can unfreeze columns in the freeze pane. Perform this step to unfreeze columns:

- Right-click any column header in the freeze pane and select [Unfreeze Pane]. All columns in the freeze pane will be unfrozen and the freeze column bar will return to its default position.

TIP

Unfreeze operation does not restore columns to their previous positions.

B4.4 Overview of grid rule definitions

By defining grid rules, you can convert the data defined with Safety I/O Editor or Safety Communication I/O Editor in bulk and also perform a consistency check of the data in bulk.

You can use the Grid Rule Editor to define the batch conversion rule and the consistency check rule.

A maximum of 1000 grid rules can be defined.

Grid Rule Editor

Grid rules are defined in the Grid Rule Editor. In the Define Rule window expanded from the Grid Rule Editor, you can define individual grid rules for each editor. In the Common Grid Rules dialog expanded from the Grid Rule Editor, you can define common grid rules . The following figure shows the Grid Rule Editor used to define grid rules.

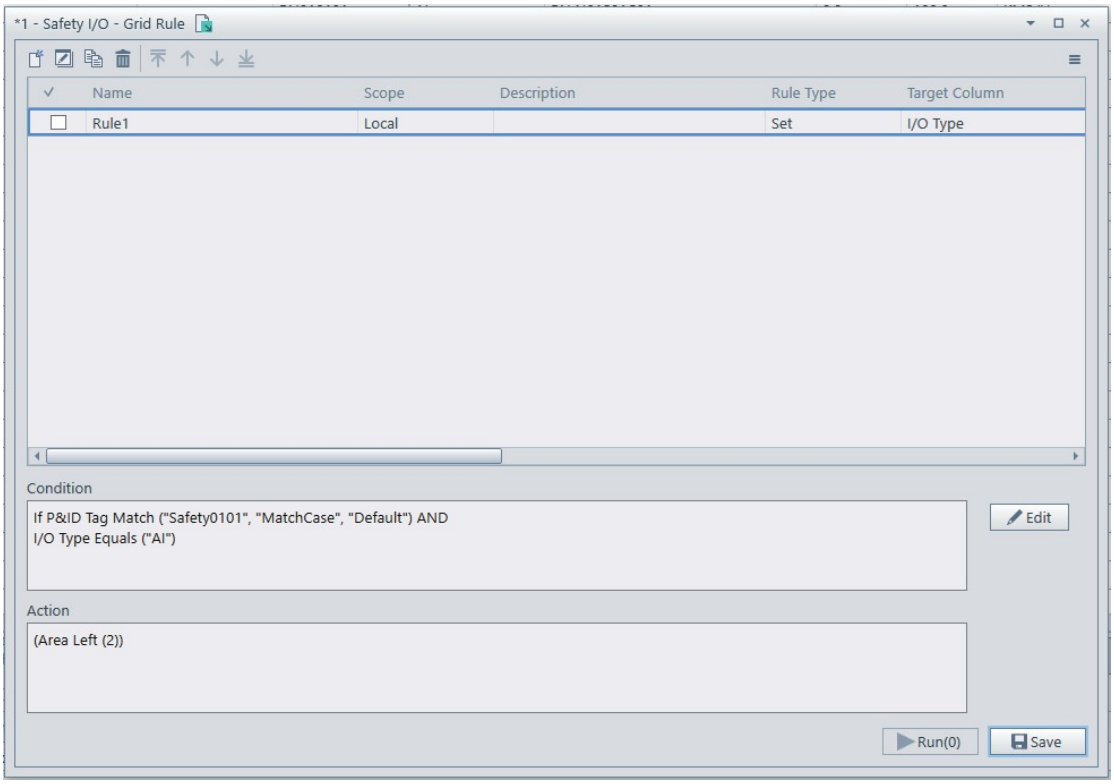


Figure B4.4-1 Grid Rule Editor

Grid Rule Editor display items

The following table shows the items displayed in the Grid Rule Editor.

Table B4.4-1 Grid Rule Editor display items

Display item name	Description
Name	Rule definition name

Continues on the next page

Table B4.4-1 Grid Rule Editor display items (Table continued)

Display item name	Description
Scope	The scope of the grid rule. Global or Local is displayed. • Global Common grid rules used in the Safety I/O Editor and common grid rules used in the Safety Communication I/O Editor. They are applicable to all the P&ID groups. Common grid rules are defined in the Common Grid Rule dialog box. • Local Grid rules other than Global. They are applicable only in the same P&ID group. These grid rules are defined in the Grid Rule Editor for each I/O list.
Description	Rule comment
Rule Type	Rule type
Target Column	Definition item name in which rule is applied
Condition	Application criteria definition for the rule
Action	Batch conversion or consistency check definition that is applied when the conditions are met
Format	Data format that is set in the format results
Created by	User created initially
Editor	Updated user name

Defining grid rules for each I/O list

Follow these steps to define grid rules for each I/O list.

1. On the toolbar of the Grid Rule Editor, click the [New] button.
   A dialog box appears to confirm the check-out.

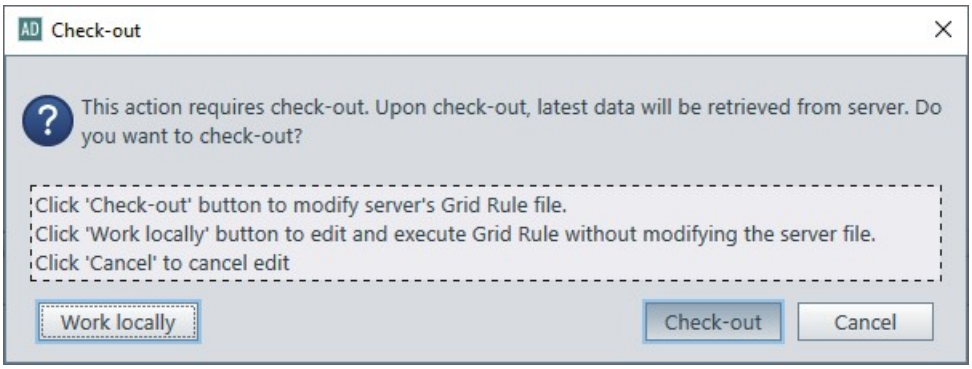


Figure B4.4-2 Check-out confirmation dialog box

2. To check out and define grid rules, click [Check-out]. If you want to define in local mode without checking out, click [Work locally].
   The Define Rule Window appears when you click [Check-out] or [Work locally].

TIP

- In local mode, you can define and execute the grid rules, but you cannot save them. If you want to save the grid rules defined in local mode, export the rules and save them locally.
- By selecting a row in the Grid Rule Editor and clicking [Edit], you can change the definition of the defined grid rule.

3. In the Define Rule Window, define grid rules.
   The rules that you defined in the Define Rule window appear in the list of the Grid Rule Editor.

SEE ALSO For more information about defining common grid rules, refer to:

"■ Defining common grid rules" on page B4-31

Define Rule window definition items

The grid rules execute the set actions according to the set conditions for the defined data and perform batch conversion or consistency check for the data.

You can define the conditions and actions in the Define Rule window.

The following table shows the definition items of the Define Rule window.

Table B4.4-2 Definition items of the Define Rule window

Definition item	Description
Name	Define rule definition name.
Description	Define rule definition comment.
Rule Type	Select set or check. • Check: Consistency check for the defined data. • Set: Data value change for the defined data.
Target Column	Specify definition item in which the rule is applied.
Format Result	While selecting Set for the Rule Type, it specifies the conversion format in the case of numeric data type. Specification is not required if the data type is string.
Condition	Defines the conditions for executing batch conversion or consistency check.
Action	Defines the actions that are executed as per the conditions.

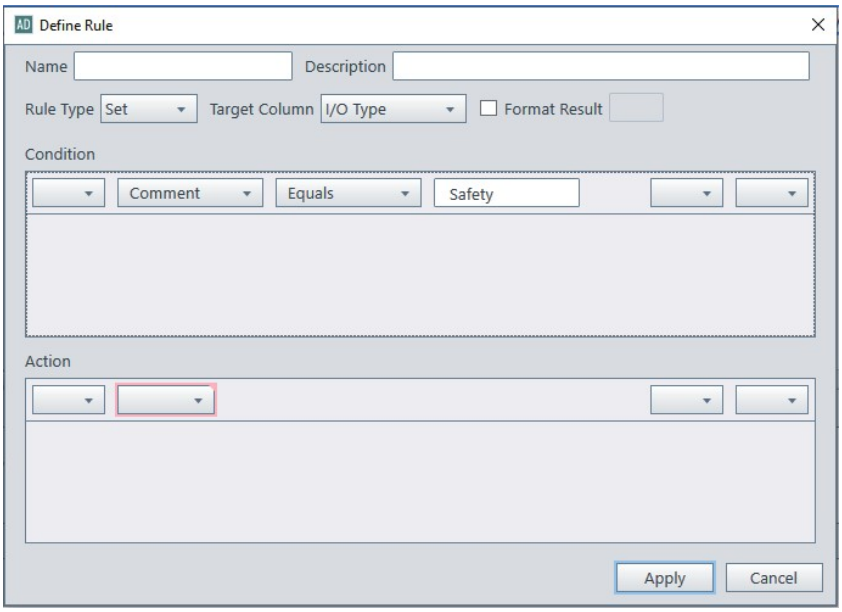


Figure B4.4-3 Define Rule window

Format Result

The following table shows the data conversion format to be specified when Format Result is selected.

Table B4.4-3 Data conversion format

Data conversion format	Description
Fn	The data is converted to the specified number of decimal digits. n: Specifies the number of digits in the range of 0 to 9 If the value n is less than the actual number of decimal digits, the value is rounded off. However, if the value n is more than the actual number of decimal digits, 0 is added.
Yn	Displays the data with the specified number of digits. n: Specifies the number of digits in the range of 1 to 9 If the value n is less than the actual number, the value is rounded off. However, if the value n is more than the actual number, 0 is added.
Xn	The data is converted to a hexadecimal value with the specified number of digits. n: Specifies the number of digits in the range of 1 to 9

The following table shows an example of data conversion.

Table B4.4-4 Example of data conversion

Data before conversion	Data conversion format	Conversion results
123.456	F0	123
123.54	F0	124
123.456	F1	123.5
123.456	F2	123.46
123.456	F4	123.4560
- 123.456	F4	- 123.4560
123.456	F9	123.456000000
123.56	Y1	124
123.456	Y3	123
123.456	Y4	123.5
- 123.0001	Y6	- 123.000
123.456	Y9	123.456000
123	X1	7B
123	X6	00007B

Condition

You can set the condition definition required to execute the rules.

You need to define the criteria in conditions to filter the target for batch editing or check. Each row of conditions corresponds to a single criteria. You can connect multiple rows by using AND/OR, and add priority for determining the criteria within parentheses to create a single condition.

The condition definition has the following items as shown in the table.

Table B4.4-5 Defining conditions

Item	Description
Start parentheses	Sets the priority rank for executing the conditions.
Column name	A definition item name that is displayed in the editor

Continues on the next page

Table B4.4-5 Defining conditions (Table continued)

Item	Description
Relational operator	• Equal to the specified value: The condition is satisfied if the definition item value that is set in the column name field matches the value that is set in the parameter field. • Not equal to the specified value: The condition is satisfied if the definition item value that is set in the column name field does not match the value that is set in the parameter field. • Specified cell is blank: The condition is satisfied if the definition item value that is set in the column name field is blank. • Specified cell is not blank: The condition is satisfied if the definition item value that is set in the column name field is not blank. • Contains the specified value: The condition is satisfied if the definition item value that is set in the column name field contains the value that is set in the parameter field. • Does not contain the specified value: The condition is satisfied if the definition item value that is set in the column name field does not contain the value that is set in the parameter field. • Higher than specified value: The condition is satisfied if the definition item value that is set in the column name field exceeds the value that is set in the parameter field. • Lower than specified value: The condition is satisfied if the definition item value that is set in the column name field is less than the value that is set in the parameter field. • Match: The condition is satisfied if the definition item value that is set in the column name field is as per the format of the regular expression that is set in the parameter field.
Parameter	A decimal or a hexadecimal value that is required for the relation operator, or data in string format • Decimal number: A number from -999999999 to 1000000000 can be set. The number of decimal places can be set up to 10 digits. • Hexadecimal number: A value from -0xFFFFFFFFF to xFFFFFFFFF can be set. • String format: Up to 1000 characters can be set.
Match Case Type Options	If you select Match as a relational operator, specify whether the search string is case sensitive or not. You can select either Match Case or Ignore Case.
Match Text Type Options	If you select Regular Expression for this option, you can include certain meta characters in your search string.
Closing parentheses	Sets the priority rank for executing the conditions.
AND/OR operator	A logical operator to combine multiple conditions • AND: Signifies that both the conditions need to be met. • OR: Signifies that either of the conditions need to be met.

The following figure shows an example of conditions that are specified to check whether the P&ID Tag is defined as `Safety0101`.

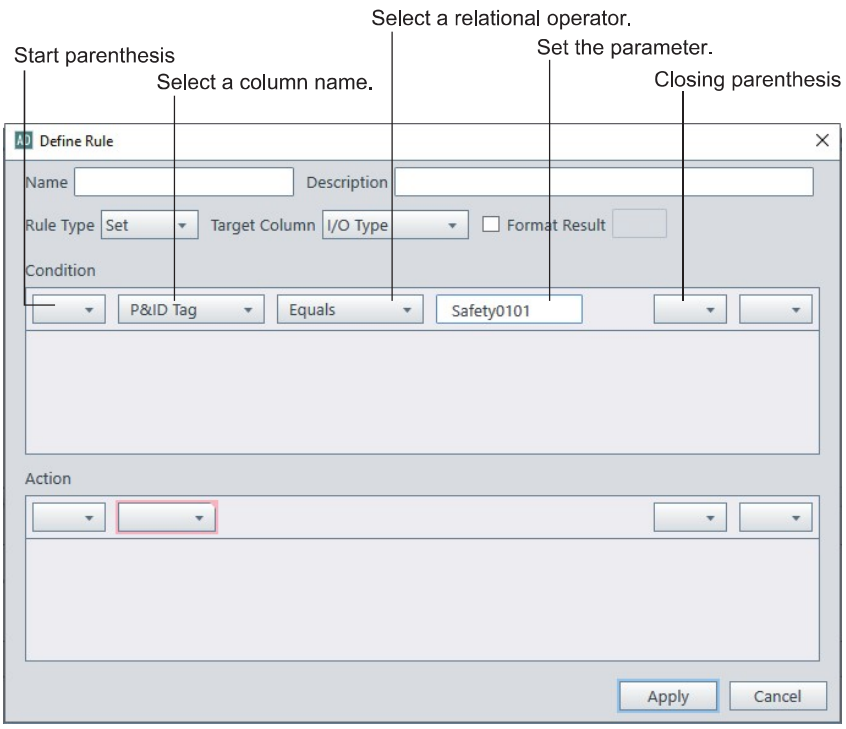


Figure B4.4-4 Condition definition example No.1

A maximum of 20 conditions can be defined under multiple conditions.
The following shows an example of multiple condition definitions.

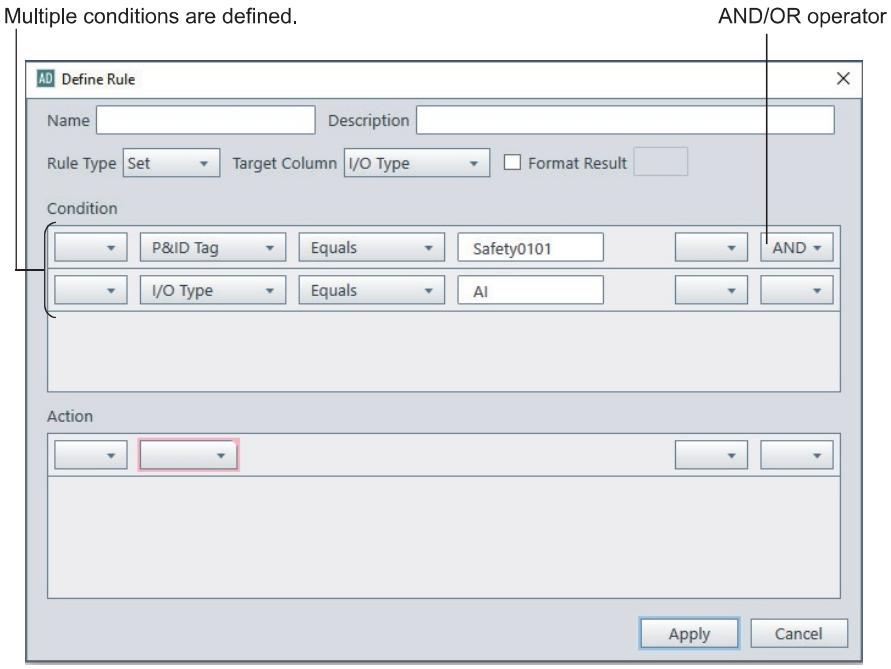


Figure B4.4-5 Condition definition example No.2

SEE ALSO For more information about use examples of regular expression, refer to:

"● Use examples of regular expression" on page B4-35

Action

You can set the action definitions that need to be executed as per the conditions. The action definition differs depending on whether Set or Check is set in the Rule Type.

For the action to be executed for set, you need to define the editing specifications required to perform bulk editing for the Target Column. Each row of action corresponds to a single editing specification. You can connect multiple rows and add priority for determining the criteria within parentheses to create a single run formula. The action definition for set is created by using the following items.

Table B4.4-6 Defining actions for set

Item	Description
Start parentheses	Sets the priority rank for executing the action.
Type of operation target	You can select either column name, string, or number. If [String] is selected, any string can be set as the action target. If [Number] is selected, any number can be set as the action target.
Column name	If Column Name is selected in operation target type, the definition item name that is displayed in the editor appears
Action operator	If Column Name is selected in the operation target type, the operators that can be used are displayed. • Left: Acquires the specified number of characters from the beginning of the string. The number of characters is specified in the parameter column. • Right: Acquires the specified number of characters from the end of the string. The number of characters is specified in the parameter column. • Mid: Acquires the specified number of characters from the specified start position. The start position and number of characters are specified in the parameter column. • Length: Acquires the string length. • Pad Left: Inserts a blank at the beginning of the string to make the string of the specified length. The string length is specified in the parameter column. • Pad Right: Inserts a blank at the end of the string to make the string of the specified length. The string length is specified in the parameter column. • Trim: Deletes any blank in the string. • Trim Left: Deletes the blank at the beginning of the string. • Trim Right: Deletes the blank at the end of the string. • To Upper: Converts the string to upper case characters. • To Lower: Converts the string to lower case characters. • Get: Replaces the Find string with the Replace string. The Find string and the Replace string are specified in the parameter column. • SQRT: Requests the square root of the definition item value that is set in the column name field.
Parameter	Sets the required parameters for using the action operators.
String options for Get operator	If you select Get as an action operator, specify whether the replacement string is case sensitive or not. You can select either Match Case or Ignore Case.
Regular Expression options for Get operator	If you select Regular Expression for this option, you can include certain meta characters in your replacement string.
Closing parentheses	Sets the priority rank for executing the action.
Operator	• Append: Combines multiple action results related to the string. • +: Adds multiple action results related to the value. • -: Subtracts multiple action results related to the value. • *: Multiplies multiple action results related to the value. • /: Divides multiple action results related to the value. It can be set if the definition item value is a decimal.

You can define up to 20 actions.

The following shows an example of action definitions.

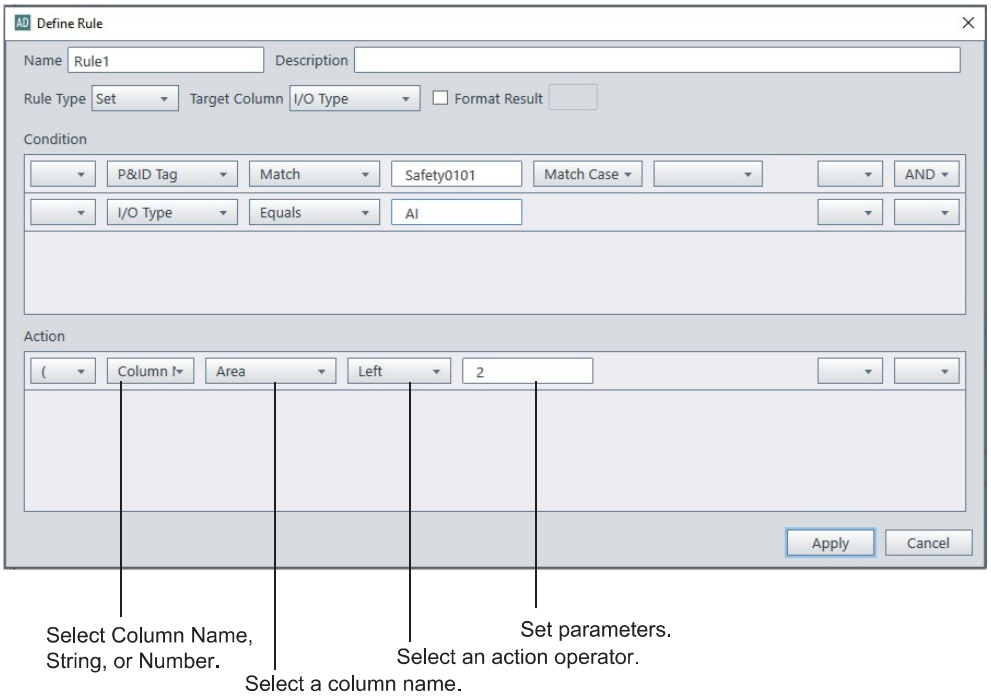


Figure B4.4-6 Example of action definition

For the action to be executed for check, you need to define the conditions required to check the Target Column. Each row of action corresponds to a single editing specification. You can connect multiple rows and add priority for determining the criteria within parentheses to create a single run formula. The action for check is comprised of the following items.

Table B4.4-7 Defining actions for check

Item	Description
Start parentheses	Sets the priority rank for executing the conditions.
Column name	A definition item name that is displayed in the editor
Relational operator	• Equal to the specified value: The condition is satisfied if the definition item value that is set in the column name field matches the value that is set in the parameter field. • Not equal to the specified value: The condition is satisfied if the definition item value that is set in the column name field does not match the value that is set in the parameter field. • Specified cell is blank: The condition is satisfied if the definition item value that is set in the column name field is blank. • Specified cell is not blank: The condition is satisfied if the definition item value that is set in the column name field is not blank. • Contains the specified value: The condition is satisfied if the definition item value that is set in the column name field contains the value that is set in the parameter field. • Does not contain the specified value: The condition is satisfied if the definition item value that is set in the column name field does not contain the value that is set in the parameter field. • Higher than specified value: The condition is satisfied if the definition item value that is set in the column name field exceeds the value that is set in the parameter field. • Lower than specified value: The condition is satisfied if the definition item value that is set in the column name field is less than the value that is set in the parameter field. • Match: The condition is satisfied if the definition item value that is set in the column name field is as per the format of the regular expression that is set in the parameter field.

Continues on the next page

Table B4.4-7 Defining actions for check (Table continued)

Item	Description
Parameter	A decimal or a hexadecimal value that is required for the relation operator, or data in string format • Decimal number: A number from -999999999 to 1000000000 can be set. The number of decimal places can be set up to 10 digits. • Hexadecimal number: A value from -0xFFFFFFFFF to xFFFFFFFFF can be set. • String format: Up to 1000 characters can be set.
Match Case Type Options	If you select “Match” as a relational operator, specify whether the search string is case sensitive or not. You can select either Match Case or Ignore Case.
Match Text Type Options	If you select Regular Expression for this option, you can include certain meta characters in your search string.
Closing parentheses	Sets the priority rank for executing the conditions.
AND/OR operator	A logical operator to combine multiple conditions • AND: Signifies that both the conditions need to be met. • OR: Signifies that either of the conditions need to be met.

TIP

The relational operators that can be used are the same as the operators that can be used for condition.

SEE ALSO

For more information about use examples of regular expression, refer to:

“● Use examples of regular expression” on page B4-35

Defining common grid rules

Follow these steps to define common grid rules in the Safety I/O Editor or in the Communication I/O Editor:

1. On the toolbar of the Grid Rule Editor, click the [Common Grid Rule] button.
   A dialog box appears to confirm the check-out.

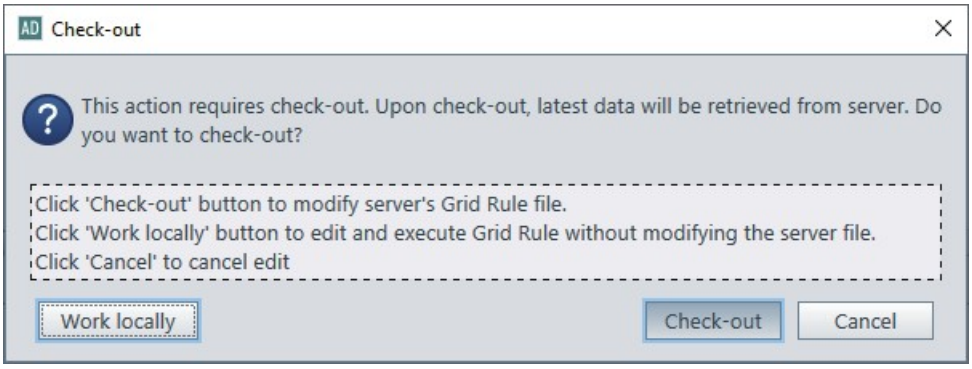


Figure B4.4-7 Check-out confirmation dialog box

2. To check out and define common grid rules, click [Check-out]. If you want to define in local mode without checking out, click [Work locally].
   The Common Grid Rule dialog box appears when you click [Check-out] or [Work locally].

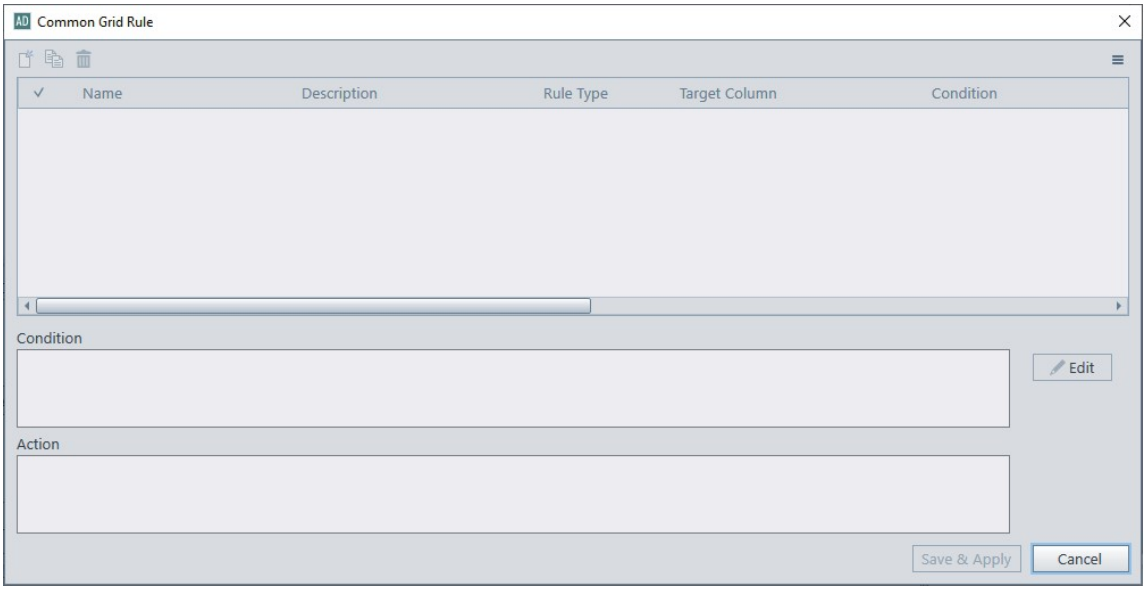


Figure B4.4-8 Common Grid Rule dialog box

TIP

- In local mode, you can define and execute the common grid rules, but you cannot save them. If you want to save the common grid rules defined in local mode, export the rules and save them locally.
- By selecting a row in the Common Grid Rule dialog box and clicking [Edit], you can change the definition of the defined common grid rule.

3. In the Common Grid Rule dialog box, click [New].
   The Define Rule Window appears.
4. In the Define Rule Window, define conditions and actions.
   In the Grid Rule Editor, a list of rules defined in the Define Rule Window is displayed.

TIP

The definitions for the common grid rules are the same as the definitions for the grid rules for each I/O list.

Specifying common grid rules

Specify whether the created common grid rule is used or not for each P&ID group.

Perform this step in the Grid Rule Editor of the P&ID group where you want to use the common grid rule.

1. On the toolbar of the Grid Rule Editor, click the [Common Grid Rule] button.
   The Common Grid Rule dialog box appears.

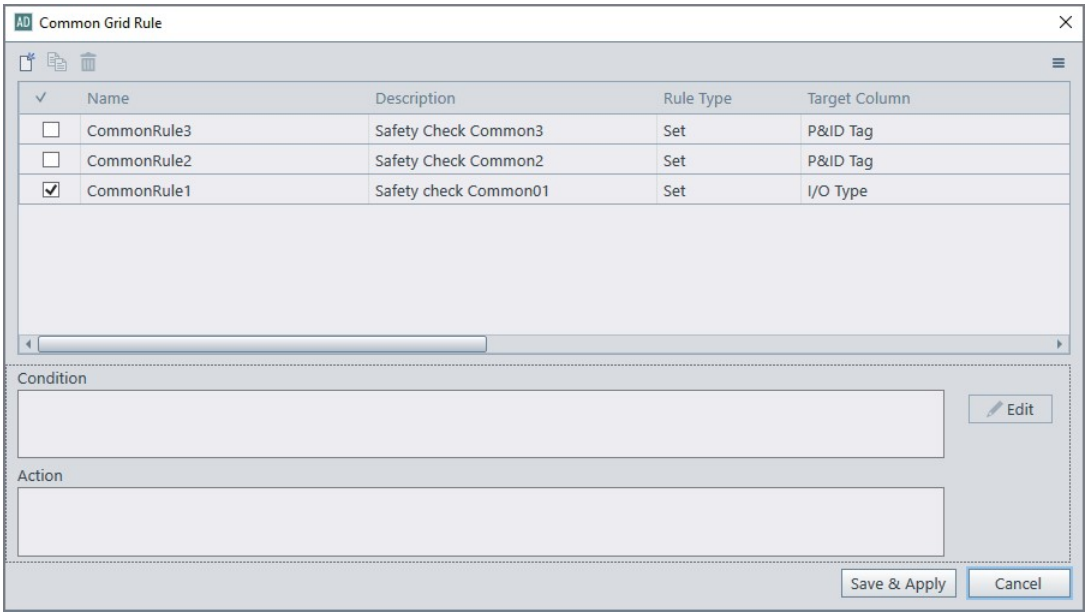


Figure B4.4-9 Common Grid Rule dialog box

2. Select the check boxes for the common grid rules you want to use. Clear the check boxes for the common grid rules you do not use.

3. Click the [Save & Apply] button.
   The Common Grid Rule dialog box closes.

   The common grid rules you use appear on the Grid Rule Editor. The common grid rules you do not use are deleted from the Grid Rule Editor.

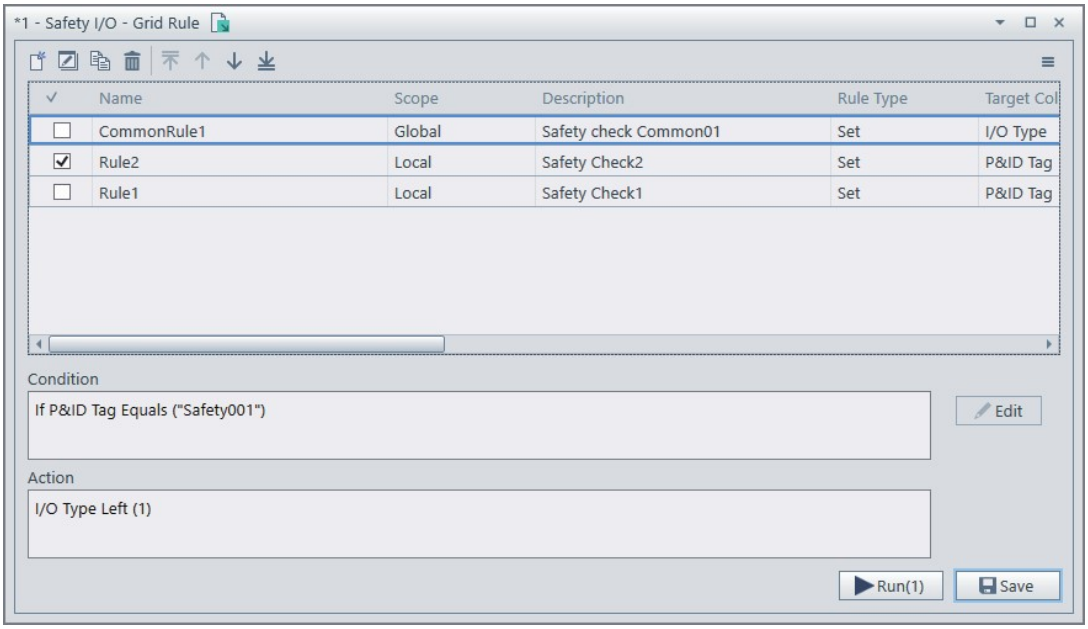


Figure B4.4-10 Grid Rule Editor

4. Click the [Save] button in the Grid Rule Editor.
   The changes are saved.

Clearing use of common grid rules in the Grid Rule Editor

Perform this step in the Grid Rule Editor of the P&ID group where you want to clear use of the common grid rules.

1. Select a common grid rule you want to clear use.
   The selected common grid rule is surrounded by a blue frame.
2. Click the Delete button on the toolbar.
   The selected common grid rule is deleted from the Grid Rule Editor.

TIP

It just clears use of the common grid rule. The common grid rule itself is not deleted.

3. Click the [Save] button.
   The changes are saved.

Deleting common grid rules in the Common Grid Rule dialog box

Perform this step in the Common Grid Rule dialog box to delete common grid rules.

1. On the toolbar of the Grid Rule Editor, click the [Common Grid Rule] button.
   The Common Grid Rule dialog box appears.
2. Select a common grid rule you want to delete.
   The selected common grid rule is surrounded by a blue frame.
3. Click the Delete button on the toolbar.
   The selected common grid rule is deleted.
4. Click the [Save & Apply] button.
   The Common Grid Rule dialog box closes.

   If the deleted common grid rule is displayed in the Grid Rule Editor, it will be deleted from the Grid Rule Editor.
5. Click the [Save] button in the Grid Rule Editor.
   The changes are saved.

Regular expressions that can be used in grid rules and their use examples

If you select Regular Expression for Match Text Type Options, you can include meta characters in your search string or replacement string.

Available major meta characters

The following table describes the major meta characters that are available when you select Regular Expression for Match Text Type Options.

Table B4.4-8 Available major meta characters

Meta character	Meaning
[x]	Character Classes Any one of the specified characters
[x-y]	Specify character range Any single character in the specified range
[^x]	Characters other than the specified character “x”
|	Logical OR of patterns
()	Group patterns

Continues on the next page

Table B4.4-8 Available major meta characters (Table continued)

Meta character	Meaning
^	Head of line
$	End of line
.	Any single character except line feed
*	Repeat the previous character zero or more times
+	Repeat the previous character one or more times
?	The previous character appears zero or one time
\	Escape character (escape sequence)

Use examples of regular expression

The following tables describe the use examples of regular expression when you select Regular Expression for Match Text Type Options.

Table B4.4-9 Use examples of regular expression for Match set values

Setting value	Reference value	Result
[FS]CS	FCS	Match
	SCS	Match
TAG[0-1]	TAG1	Match
	TAG3	Not match
TAG[^XY]	TAG0	Match
	TAGX	Not match
TAG1|TAG2	TAG1	Match
	TAG2	Match
TAG([0-1]|[X-Y])	TAG1	Match
	TAGX	Match
^[2-8]ALF111	3ALF111	Match
TAG001$	01TAG001	Match
	01TAG0011	Not match
HIS016.	HIS0164	Match
TAG.*	TAGA	Match
	TAGAA	Match
	TAG	Match
TAG.+	TAGA	Match
	TAGAA	Match
	TAG	Not match
010?TAG	01TAG1	Match
	010TAG1	Match
	0100TAG1	Not match
TAG01\.	TAG01.	Match

Table B4.4-10 Use examples of regular expression for Get set values

Setting value		Reference value	Result
Match value	Replace value		
[FS]CS	DCS	FCS	DCS
		SCS	DCS
TAG[0-1]	TAG2	TAG1	TAG2
		TAG3	TAG3
TAG[^XY]	TAGZ	TAG0	TAGZ
		TAGX	TAGX
TAG1|TAG2	TAG3	TAG1	TAG3
		TAG2	TAG3
TAG([0-1]|[X-Y])	TAG2	TAG1	TAG2
		TAGX	TAG2
^[2-8]ALF111	1ALF111	3ALF111	1ALF111
TAG001$	TAG002	01TAG001	01TAG002
		01TAG0011	01TAG0011
HIS016.	HIS0163	HIS0164	HIS0163
TAG.*	TAG01	TAGA	TAG01
		TAGAA	TAG01
		TAG	TAG01
TAG.+	TAG01	TAGA	TAG01
		TAGA A	TAG 01
		TAG	TAG
010?TAG	TAG01	01TAG1	01TAG1
		010TAG1	01TAG1
		0100TAG1	01000TAG1
TAG01\.	TAG01	TAG01.	TAG01

Starting the Grid Rule Editor

You can start the Grid Rule Editor by selecting the [Grid Rule] button of the target editor for the grid rules.

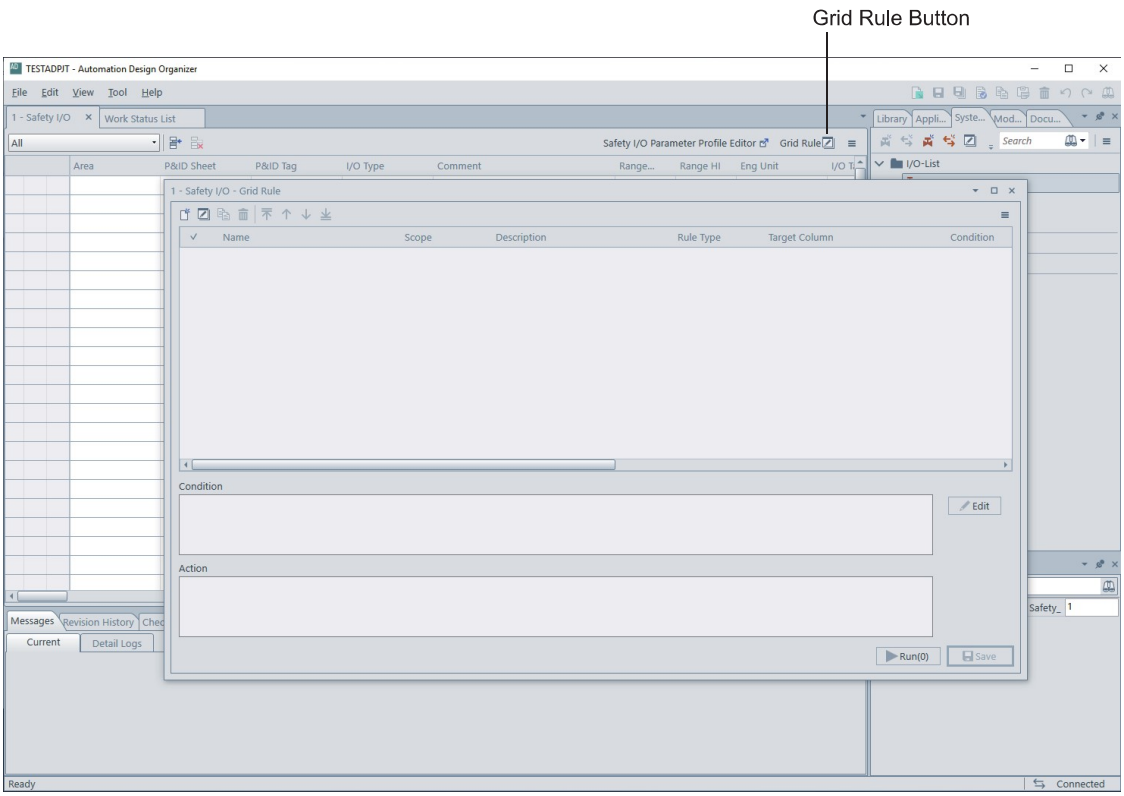


Figure B4.4-11 [Grid Rule] button

Operating the Grid Rule Editor

You can change the run sequence and the rule definition of the created grid rules, and copy or delete the rules.

Changing the rule execution sequence

When multiple rules are selected and run, the rules are executed in the sequence from top to bottom in the Grid Rule Editor.

To change the run sequence of the rule, you need to perform the following operation.

- Select the rules whose run sequence needs to be changed, and click the [Move to Top] / [Move Up] / [Move Down] / [Move to Bottom] buttons that are found on the Grid Rule Editor.

Changing the rule definition

- To change an already defined rule, you need to select one row of the rule that is displayed in the Grid Rule Editor by using the mouse, and double-click on this row.
  The Define Rule window appears, and the rules can be changed.

Deleting rules

- To delete a defined rule, you need to use the mouse to select one row from the Grid Rule Editor, and click the [Delete] button on the tool bar.
  The selected rule is deleted.

Duplicating rules

- To duplicate a defined rule, use the mouse to select one row from the Grid Rule Editor, and click the [Duplicate] button on the tool bar.
  The rule is duplicated.

Running grid rules

1. To run the rules defined in the Define Rule window, select the respective check boxes on the left side of the Grid Rule Editor, and click [Run].
   When a [Set] rule type grid rule is executed, the data of cells that match the conditions will be changed.

   When a [Check] rule type grid rule is executed, the cells that match the conditions are highlighted. The data in the cell will not be changed.

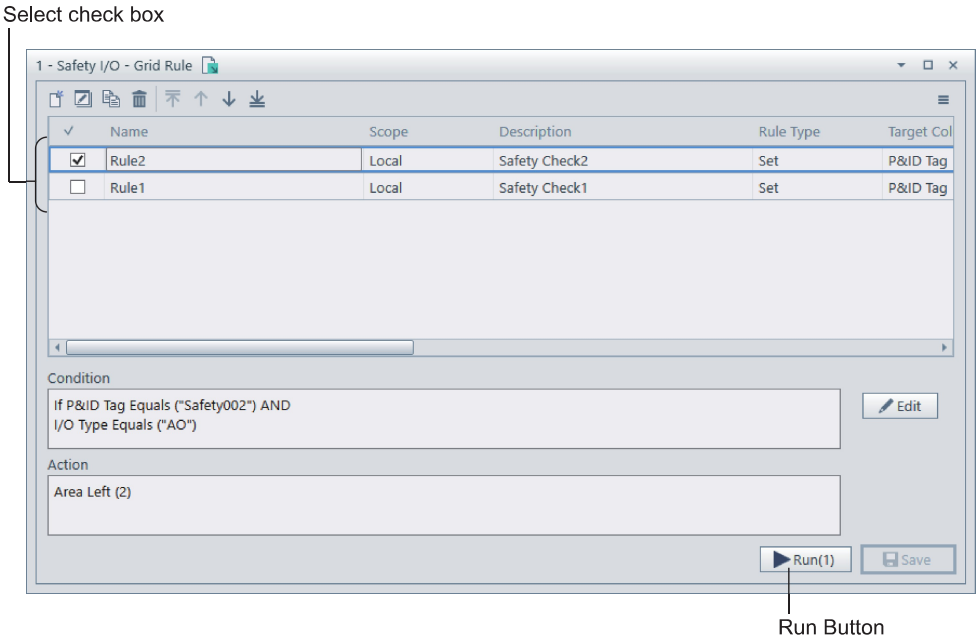


Figure B4.4-12 Run

TIP

- When a grid rule with rule type [Set] is executed, the relevant files are not checked out automatically.
- When a grid rule with rule type [Set] is executed, up to 10 columns can be changed at the same time.

Exporting grid rules

The grid rules that are defined by each user can be exported and saved to the computer. Follow these steps to export grid rules:

1. Select the grid rules that need to be exported in the Grid Rule Editor.
2. Select [Export] from the sub menu of the Grid Rule Editor.
   A selection dialog box appears to choose the save location.
3. Specify the folder to which the rules need to be exported, and click [OK].

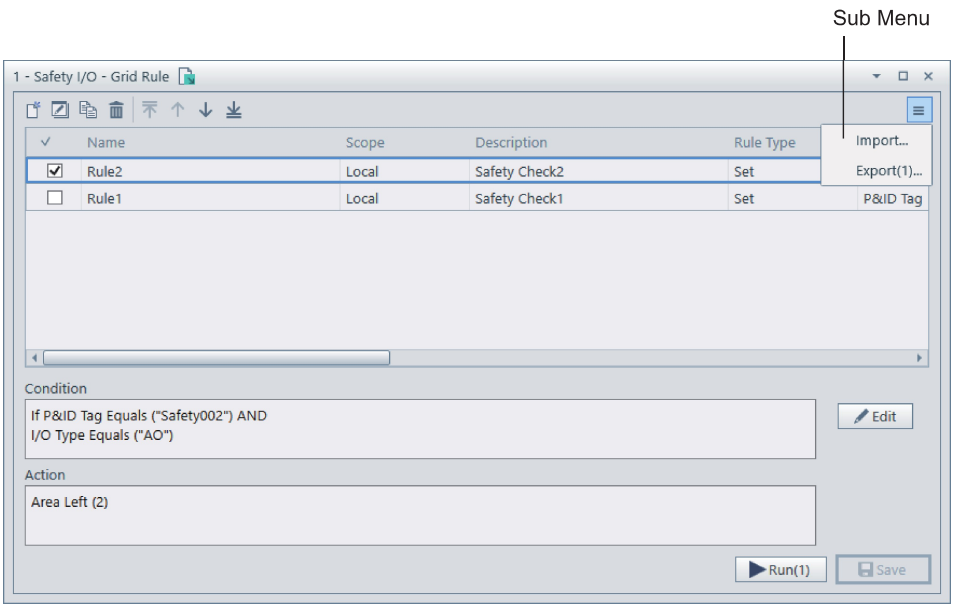


Figure B4.4-13 Tools menu

TIP

When the filter function is used, the export menu will turn gray, and export operation cannot be performed.

Importing grid rules

The grid rules that are exported and saved can be imported. Follow these steps to import grid rules:

1. Select [Import] from the sub menu of the Grid Rule Editor.
   A selection dialog box appears to choose the source.
2. Specify the XML file in which the grid rules to be imported are defined, and click the [OK] button.
   The imported grid rules is added in the last row of the Grid Rule Editor.

TIP

- You cannot import grid rules of a different editor.
- When the filter function is used, the import menu will turn gray, and export operation cannot be performed.

Saving the grid rules and performing check-in

The grid rules that are defined in the Grid Rule Editor can be stored in the AD project by saving and checking-in the grid rules.

Saving grid rules

- To save grid rules, click the [Save] button in the Grid Rule Editor.
  The edited grid rules are saved.

Performing check-in of the grid rules

- You can check in the edited grid rules by using the Check-in window.

C. Automation Design Server administration functions and history management

This section describes the management of AD Server and AD projects that use Automation Design Suite Administration Tool (hereinafter referred to as "ADS Administration Tool") as well as history management for AD Suite.

C1. AD Server administration functions

Administration functions of AD Server consist of management of AD Server and AD projects.

AD Server management includes functions such as backing up, restoring, and setting the location of the ADMDB.

AD project management includes functions such as creating AD projects, exporting and importing project data, and configuring access control settings.

C1.1 Tools for management of AD Server and AD projects

Use ADS Administration Tool for management of AD Server and AD projects. ADS Administration Tool runs on a computer with AD Server. To use ADS Administration Tool, the user must have the proper access rights.

Functions of ADS Administration Tool

ADS Administration Tool provides AD Server management functions and AD project management functions.

Functions for management of AD Server are as follows:

- Communication setting of the AD server and encryption setting of the ADMDB
- Backing up and restoring the ADMDB
- Viewing the history of backup and export operations
- Location setting of the ADMDB

Functions for management of AD projects are as follows:

- Creating and deleting AD projects
- Modifying properties of AD projects
- Controlling access to AD projects
- Exporting and importing AD project databases
- Prohibiting and permitting modification of AD project data
- Forcibly canceling the checked-out status of currently checked-out AD project files

Access rights for use of ADS Administration Tool

An Access Right in accordance with the IT security model is required in order to use each function of ADS Administration Tool. If the IT security model is the Standard model or the Strengthened model, log on to a computer with AD Server by using an account that belongs to either of the following groups:

- ADS_MANAGER group
- ADS_MANAGER_LCL group

In addition to the ADMDB backup and AD project export functions, ADS Administration Tool has a function to back up RS projects and SCS projects. To activate this function, you must log on to a computer with AD Server by using an account that belongs to all of the following groups. However, the CTM_MAINTENANCE group can be excluded if the AD Server to which ProSafe-RS is connecting is not used by CENTUM VP.

- ADS_MANAGER group or ADS_MANAGER_LCL group
- PSF_MAINTENANCE group
- CTM_MAINTENANCE group

Starting ADS Administration Tool

- To start ADS Administration Tool, from your desktop, select [Start] > [All Programs] > [YOKOGAWA AD Suite] > [ADS Administration Tool].
  ADS Administration Tool launches.

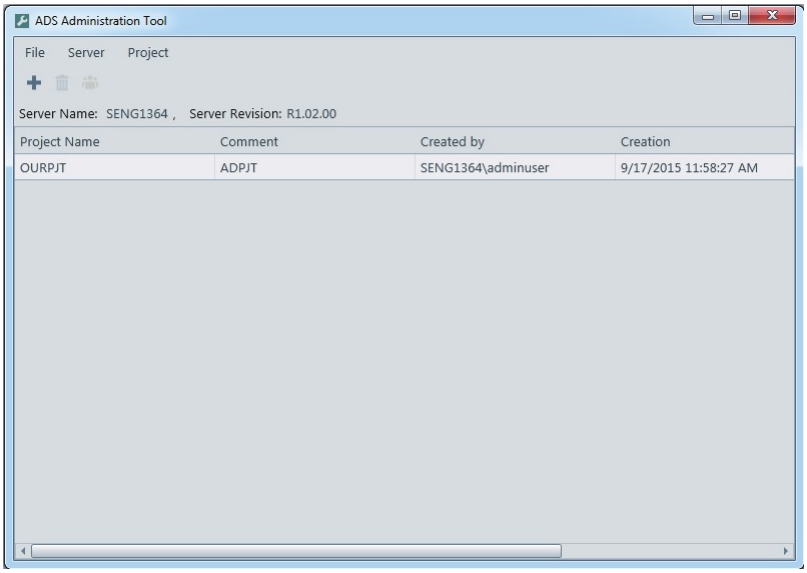


Figure C1.1-1 ADS Administration Tool

Activating the system project backup function

When backing up ADMDB and when exporting an AD project, by default the system is configured to automatically perform a backup of all system projects prior to Server Backup.

Follow these steps to activate the system project backup function:

1. Start the ADS Administration Tool.
   If any one of the following conditions is met, the Activation setting for System Project Backup Function dialog box may appear.
   - AD server license has been distributed.
   - CENTUM VP or ProSafe-RS has been upgraded on a computer where the AD server is installed.
   - CENTUM VP and ProSafe-RS have been installed on a same computer.

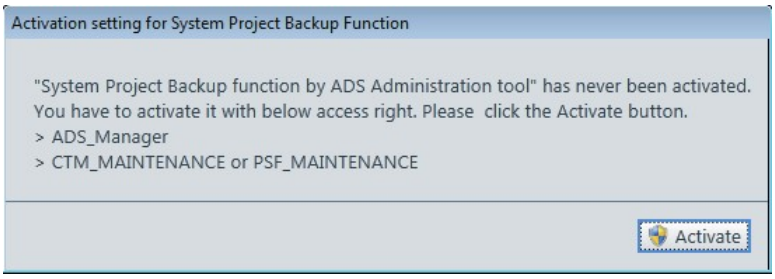


Figure C1.1-2 Activation setting for System Project Backup Function dialog box

2. Click the [Activate] button.

TIP

When you start the ADS Administration Tool again after activation has failed, the Activation setting for System Project Backup Function dialog box appears again.

IMPORTANT

- After activating the system project backup function, change the initial password of PSF_PROCESS. If you change the password before activating the system project back-up function, the [Backup System Projects prior to AD Project Export] check box in the ADS Administration Tool appears dimmed. In that case, change the initial password of PSF_PROCESS after activating the system project backup function.
- When changing the password, ensure that the same password is set in the entire system.

SEE ALSO For more information about changing the password for a user account, refer to:

6.11, “Other Utility Programs” in ProSafe-RS Security Guide (IM 32P01C70-01EN)

C1.1.1 Communication setting of the AD Server and Encryption setting of the ADMDB

The Communication setting of the AD server and the Encryption setting of the ADMDB are set in the Option Setting dialog box of ADS Administration Tool.

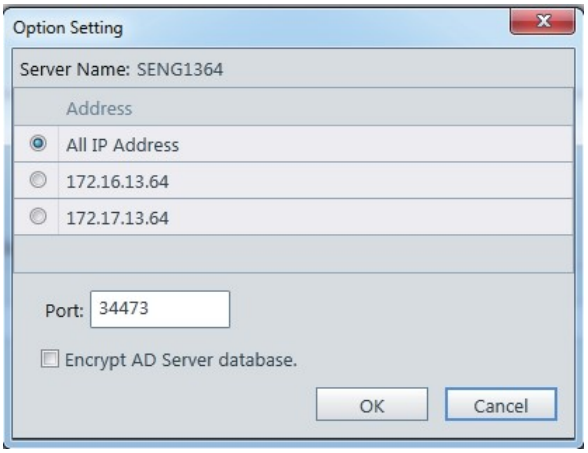


Figure C1.1.1-1 Option Setting dialog box

IMPORTANT

After changing the Option setting, restart the computer with AD Server.

C1.1.2 Changing the Communication setting of the AD Server and the Encryption setting of the ADMDB

Two AD Server options are available: one for setting up communication and the other one for setting up ADMDB encryption.

Setting communication

If the computer with AD Server has multiple network interface cards installed in it, you can set which network interface card is used and change the communication port used by AD Organizer to communicate with AD Server. You can change the communication setting by using the Option Setting dialog box of ADS Administration Tool.

TIP

After changing the communication setup, restart the computer with AD Server.

IMPORTANT

If the computer with AD Server is connected to the control bus, the control bus network interface also appears in the Option Setting dialog box. However, you must be aware that AD Organizer and AD Server cannot communicate with each other through the control bus.

In the standard setting, the IP address of the control bus network interface is as follows:

172.16.<domain number>.<station number>

Changing the Communication setting

Follow these steps to change the communication setting of AD Server.

1. From the menu of ADS Administration Tool, select [Server] > [Option Setting].
   The Option Setting dialog box appears.
2. From the IP address list, select the radio button of the network interface card to be used.
   Selecting [All IP Address] enables all Network Interface Cards (NIC) installed on the computer to communicate with AD Server.
3. Change the port number, if necessary.
4. In the Option Setting dialog box, click [OK].
   The AD Server Restart Confirmation dialog box appears.
5. Restart the computer with AD Server.

Encryption setting of the ADMDB

You can set whether or not to encrypt the ADMDB by using Encrypting File System. The default setting is no encryption.

Encryption of the ADMDB can be run during an engineering process. Encryption can also be run while files currently being checked out are remaining.

In cases when the encryption setting has been changed, encryption processing runs the next time the computer is started and AD Server doesn't start until this processing is completed.

TIP

- After changing the ADMDB encryption setting, restart the computer with AD Server. When the computer is restarted, the encrypting or decrypting process is performed.
- Encrypting or decrypting the ADMDB requires some time.

Setting up encryption of the ADMDB

Follow these steps to configure encryption of the ADMDB.

1. From the menu of ADS Administration Tool, select [Server] > [Option Setting].
   The Option Setting dialog box appears.
2. Select the [Encrypt AD Server database] check box.
3. In the Option Setting dialog box, click [OK].
   The Encryption Time Message dialog box appears.
4. Click the [OK] button.
5. Restart the computer with AD Server.

TIP

An encrypted ADMDB can be decrypted. To decrypt the database, clear the check box in step 2 and perform step 3 onward.

C1.1.3 ADMDB location setting

You can specify a folder where the ADMDB for AD Server is placed. A folder named ChronusENG is created under the specified folder.

By default, the ADMDB is created in the system drive on the computer for AD Server.

However, when the space available on the system drive is insufficient or when the size of the ADMDB expands along with the processes of engineering tasks and the available space becomes insufficient, the ADMDB cannot be placed on this drive.

Accordingly, you must place the ADMDB in a folder with enough available space which is other than the location set by default.

You must not change the location of the ADMDB by using the explorer function of Windows.

Operation of AD Server after changing the folder of the ADMDB

After changing the location, AD Server operates using the data of the ADMDB that exists in the folder after the change. If the ADMDB does not exist on the folder after the change, the ADMDB is newly created.

To continue using the data of the ADMDB from before the change of location, you must manually perform operations to move the data of the ADMDB from the folder before the change to the folder after the change.

Data subject to the ADMDB location setting function

The following data included in the ADMDB is subject to this function.

- Engineering data and list information of AD projects
- Information regarding the history of backup and export operations of the ADMDB

Option setting information of AD Server not included in the ADMDB is not subject to this function.

Execution timing of the ADMDB location setting

The timings at which changing of the folder for the ADMDB can be implemented are as follows:

- When ADS Administration Tool of AD Server is started for the first time
  Location setting is required when ADS Administration Tool is started for the first time after installation of AD Server.
- At any timing chosen by the user
  While AD Server is in operation, the ADMDB location setting can be run at any timing chosen by the user.

ADMDB Location Setting window

When ADS Administration Tool is started for the first time, the following dialog box is displayed.

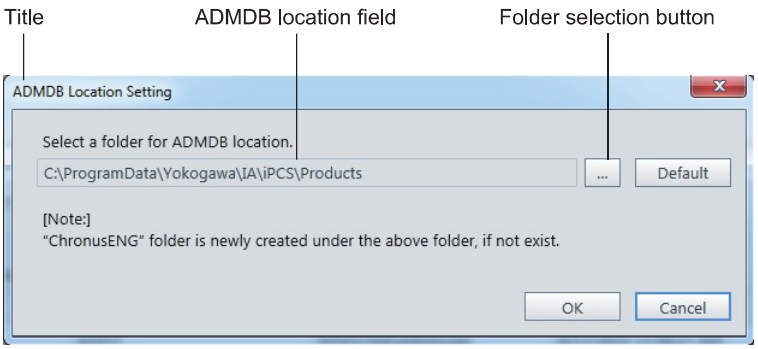


Figure C1.1.3-1 ADMDB Location Setting dialog box

Items displayed in the ADMDB Location Setting dialog box

Table C1.1.3-1 Items displayed in the ADMDB Location Setting dialog box

Displayed item	Description
ADMDB location field	The path of the folder in which the ADMDB is placed is displayed. Up to 100 characters can be configured for this item.
Folder selection button	Clicking this button displays a folder selection dialog with which the folder in which to place the ADMDB can be selected. When this item is not configured, the default settings are applied.
Default	Clicking this button displays the path of the default location in the ADMDB location field.

TIP

Pressing the ESC key cancels the settings and closes the screen without executing the settings.

Tasks before and after running the ADMDB location setting

The following window is displayed when running the ADMDB location setting at any timing chosen by the user.

Perform operations according to the precautions displayed in the window.

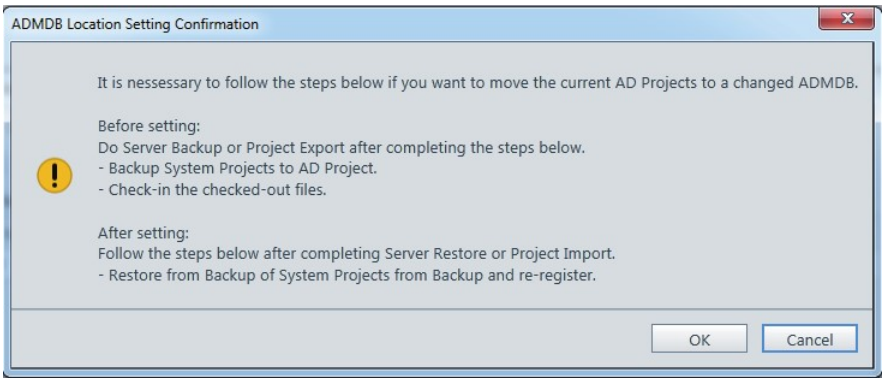


Figure C1.1.3-2 Precautions for ADMDB location setting

Server processing and status of the ADMDB at the time of the ADMDB location setting

This section describes the flow of the ADMDB location setting, server processing, and the statuses of the ADMDB before and after changing the location setting.

ADMDB location setting when ADS Administration Tool is started for the first time

The following table shows the flow of operations when changing the folder of the ADMDB the first time ADS Administration Tool is started, server processing, and the status of the new ADMDB.

Table C1.1.3-2 Flow of change of location when ADS Administration Tool is started for the first time

Order	Flow	User operations	Processing of AD Server	The ADMDB in the new location
1	ADMDB location setting	ADMDB location setting change request with ADS Administration Tool	Change the ADMDB location setting	A folder (ChronusENG folder) for the ADMDB is created under the folder specified by the user
2	IT security setting	Set access rights for the ADMDB folder by running the IT security tool	-	Access rights are set for the ADMDB folder
3	Starting AD Server and creating the ADMDB	Restarting the computer	Starting AD Server and creating the ADMDB in a new location	An empty ADMDB is created
4	Project registration (Creation of new projects)	AD project creation request with ADS Administration Tool	Executing creation of the AD project	The AD project is created

ADMDB location setting during operation

The following table shows the flow of operations when changing the folder of the ADMDB during operation with ADS Administration Tool, server processing, and the status of the new ADMDB.

Table C1.1.3-3 Flow of the ADMDB location setting during operation

Order	Flow	User operations	Processing of AD Server	The ADMDB in the new location
1	Backing up existing AD projects	Requesting a server backup with ADS Administration Tool	Acquiring a backup from the ADMDB before the change and creating a backup file	-
2	ADMDB location setting	ADMDB location setting change request with ADS Administration Tool	Change the ADMDB location setting	A folder (ChronusENG folder) for the ADMDB is created under the folder specified by the user
3	IT security setting	Set access rights for the ADMDB folder by running the IT security tool	-	Access rights are set for the ADMDB folder
4	Starting AD Server and creating the ADMDB	Restarting the computer	Creating the ADMDB in a new location	An empty ADMDB is created
5	Project registration (Re-registration of an existing project)	Requesting a server restoration with ADS Administration Tool	Executing a server restoration by using the backup file	The ADMDB is restored

Backing up existing AD projects

A server backup of the AD project is implemented.

The AD projects within the ADMDB of the former location are not automatically transferred to the ADMDB of the new location. For this reason, when it is necessary to transfer such AD projects, you must execute a server backup in advance.

You do not need to implement this operation if it is not necessary to transfer the AD projects.

TIP

When individually transferring AD projects, implement a project export instead of a server backup.

ADMDB location setting

The AD Server receiving a location setting request restarts after creating a folder for the ADMDB in the specified location.

The name of the folder for the ADMDB is ChronusENG.

However, if a folder for the ADMDB already exists in the new location, the folder is not newly created and the existing ADMDB is loaded after being restarted. At this time, if AD projects exist on the ADMDB, these AD projects are loaded.

TIP

Running a location setting restarts AD Server. Along with such, connections with ADS Administration Tool and each connected client are disconnected. For this reason, after restarting AD Server, ADS Administration Tool and each of the clients need to be reconnected.

IT security setting

You can run the IT security setting tool to set access rights for the ADMDB folder in the new location. The details of the access rights to be set are the same as the default ADMDB folder.

If the strengthened model has been selected, the ADMDB folder in the new location is registered with the software restriction policies.

A folder once registered with the software restriction policies cannot be deleted using the IT security tool. For this reason, when the user has changed the location again, the user must delete the old folder from the software restriction policies by themselves.

To delete the old folder, select and delete the applicable folder from Additional Rules under Software Restriction Policies of the local group policy editor shown in the following figure.

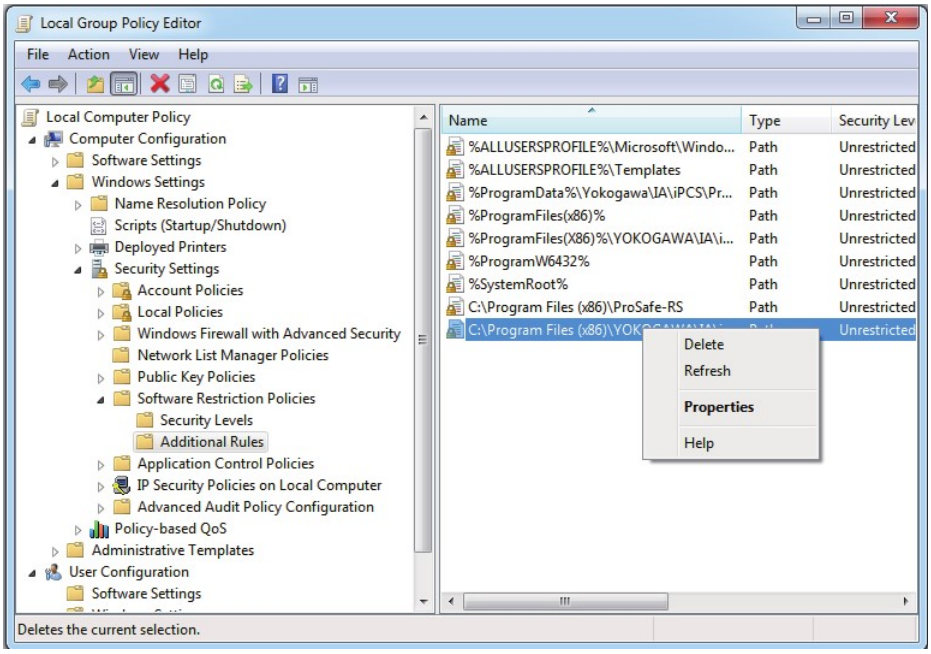


Figure C1.1.3-3 Example of canceling the registration of software restriction policies

Applicable folders are displayed as shown in the following figure.

"user specified folder name"/ChronusENG/Data/Projects

If the folder has been moved from the default location to another location, the previously mentioned "user specified folder name" subject to the deletion is the default location.

You must restart the computer after running the IT security tool.

Starting AD Server and creating the ADMDB

Restarting the computer starts AD Server. At this time, AD Server creates the ADMDB within the folder in the new location.

The user can create a new AD project using ADS Administration Tool or register an AD project. When newly creating an AD project, the AD project can be created by suing the AD project management function. When re-registering an existing AD project, restore the backup file created prior to the operation for changing the location.

Project registration

The user can create a new AD project using ADS Administration Tool or register an existing AD project.

- When newly creating an AD project
  You can create an AD project by using the AD project management function.
- When re-registering an existing AD project
  If you wish to continue using the same AD project from before the change of location, run a restoration of the backup file created at Backing up existing AD projects in the flow or run an import of the export file.

Precautions when transferring an existing AD project to the ADMDB in a new location

Precautions for transferring the engineering data of an existing AD project and continuing engineering with the new ADMDB are as follows:

Precautions prior to implementation of location setting

You must cancel the checked-out status of all files before obtaining a backup of the AD project to transfer.

The altered content of files that are checked-out when running server backup and project export are not transferred to the new ADMDB. You must check-in all edited details in advance.

Precautions after implementation of location setting and RS project registration

Similar to when running a normal server restoration or project import, you must re-register RS projects to the AD project that has been transferred.

Drives and types of folders in which the ADMDB can be placed

The drives and folders which can be specified in the ADMDB location setting are folders under the local drive.

IMPORTANT

You must not specify a folder under the following folders: When the following folders are specified, there is the possibility of subjects of setting with the IT security tool being duplicated and such setting not being implemented properly.

- Hidden folder
- Program Files folder (`C:\Program Files`, `C:\Program Files (x86)`)
- Program Data folder (`C:\ProgramData`)
- Installation folders of other coexisting YOKOGAWA products (example: `C:\CENTUMVP`)
- Network drive folders (not capable of IT security setting)

Database encryption at the time of the change of location

At the time of location setting, the encryption setting of the ADMDB that exists in the new location is inherited. The encryption setting of the ADMDB in the former location is not reflected to the destination of the change.

If the ADMDB does not exist in the new location, the ADMDB is created in a state where encryption is disabled.

Relation between the server backup function and the restoration function

The server backup function and the restoration function are implemented in relation to the location of the ADMDB changed with ADMDB location setting.

For example, changing the location after obtaining a backup and implementing a restoration after this restores the file in the most recently configured location. The setting at the time the backup was made is not taken into consideration.

The ADMDB location setting is not included in the information that is backed-up or restored.

Exclusive control of access to the ADMDB during processing of the location setting

All access to the ADMDB is restricted during the processing of the location setting. Accessing the ADMDB returns an error.

Further, location setting operations cannot be performed during processing of access to the ADMDB. Running a location setting during processing of access to the ADMDB displays an error dialog and cancels the location setting.

Handling of the data of the ADMDB before the change of location

Engineering data included in the ADMDB in the location prior to the change is maintained even when the location setting is changed. For this reason, the original ADMDB can be used again by returning the location setting to its original setting.

C1.1.4 Setting the location of the ADMDB

This section describes how to change or return to the default location the folder in which the ADMDB is placed at a timing of choice for a reason such as the server capacity becoming insufficient during operation of a project or when ADS Administration Tool is started for the first time.

Setting the location of the ADMDB when ADS Administration Tool is started for the first time

After installing AD Server, you can specify the folder in which to create the ADMDB when ADS Administration Tool is started for the first time.

1. Start ADS Administration Tool.
   The ADMDB Location Setting dialog box appears.

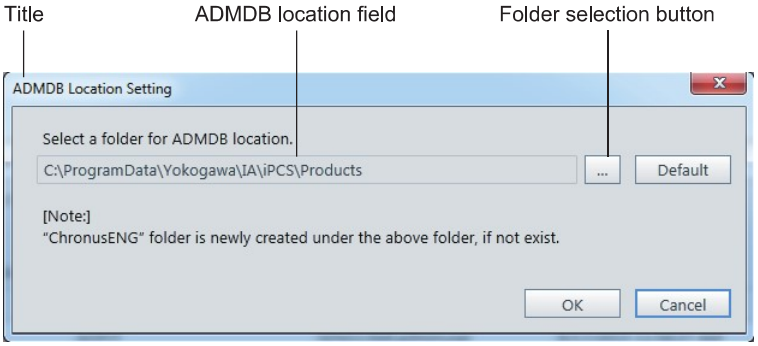


Figure C1.1.4-1 ADMDB Location Setting dialog box

2. Click the folder selection button to select the folder in which the ADMDB is placed.
   The selected folder path appears in the ADMDB location field.

TIP

- Click [Default] to configure the default setting as the folder in which the ADMDB is placed.
- The file path must be 100 characters or less.
- Specifying a folder in which the ADMDB does not exist newly creates an ADMDB.

3. Click the [OK] button.
   ADS Administration Tool closes.
4. Start the IT Security Tool and configure the IT security settings to the values that were set when ProSafe-RS was installed.
5. Restart the computer.

SEE ALSO For more information about IT security settings, refer to:

- 6.9, “Viewing the Information Configured by the IT Security Tool” in ProSafe-RS Security Guide (IM 32P01C70-01EN)
- B3.6, “Configuring IT Security Settings” in Installation Guide (IM 32P01C50-01EN)

Setting the location of the ADMDB at a timing of choice

Follow these steps to change the folder in which the ADMDB is placed at a timing of choice:

1. From the menu bar of ADS Administration Tool, select [Server] > [ADMDB Location Setting].
   A dialog box showing the details which should be implemented before and after changing the location of the folder is displayed.

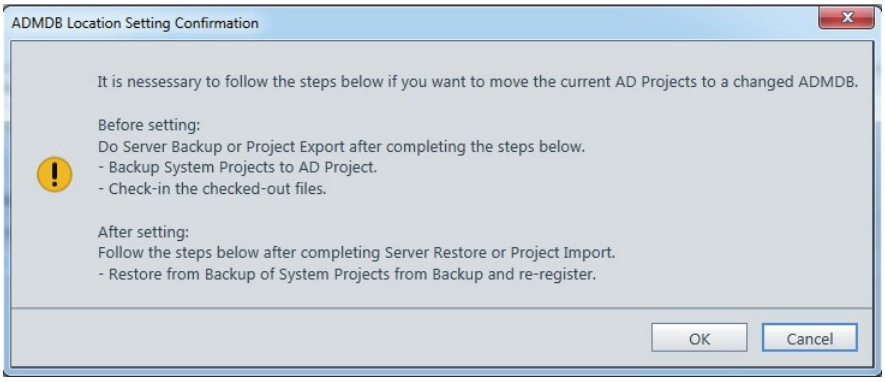


Figure C1.1.4-2 Details of processing before and after the ADMDB location setting

2. Confirm the details displayed in the dialog box.
   Once closed, the details of the dialog box cannot be confirmed during the tasks of changing the folder.
3. If tasks prior to the change of location have not been implemented, you can click the [Cancel] button and start again from Step 1 after implementing the tasks prior to the change of location. If tasks prior to the change of location have been implemented, you can click [OK].
   A dialog box for selecting the folder appears.
4. Click the folder selection button to select the folder in which the ADMDB is placed.
   The selected folder path is displayed in the ADMDB location field.

TIP

Click [Default] to return the folder in which the ADMDB is placed to the default setting.

The file path must be 100 characters or less.

5. Click the [OK] button.
   A dialog box for suggesting a restart and IT security setting appears.

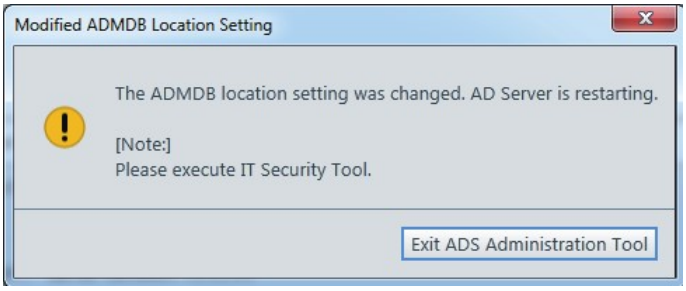


Figure C1.1.4-3 Messages after change of location

6. Click [Exit ADS Administration Tool].
   ADS Administration Tool closes.
7. Start the IT Security Tool and configure the IT security settings to the values that were set when ProSafe-RS was installed.
8. Restart the computer.
   An empty ADMDB is created in the new location.

TIP

If a ChronusENG folder is already created in the new location and an ADMDB exists in it, that ADMDB is read after the computer is restarted. If the ADMDB contains any AD project, that AD project is also read at the same time.

9. If any AD Server options were set before changing the location, set the AD Server options again.

10. Start the ADS Administration Tool and register the AD project. To register the project, perform one of the following operations:
    - Create a new AD project.
    - Restore the backed-up ADMDB.
    - Import an exported AD project.
11. Start AD Organizer and register the RS project with the AD project. To register the project, perform one of the following operations:
    - If you have created a new AD project, register the RS projects with the AD project.
    - If you have restored an ADMDB or imported an AD project, restore the backed up RS projects from the AD project.

TIP

- The AD Server and AD Organizer is disconnected when you change the ADMDB location. After changing the ADMDB location, reconnect to the AD Server.
- After moving an existing AD project to a new location, it is recommended that you delete the AD project from the old location.

SEE ALSO

For more information about how to back up and restore the ADMDB, refer to:

C1.1.7, “Backing up and restoring the ADMDB” on page C1-20

For more information about how to export and import the AD projects, refer to:

C1.2.3, “Export and import AD projects” on page C1-38

For more information about IT security settings, refer to:

- 6.9, “Viewing the Information Configured by the IT Security Tool” in ProSafe-RS Security Guide (IM 32P01C70-01EN)
- B3.6, “Configuring IT Security Settings” in Installation Guide (IM 32P01C50-01EN)

For more information about option settings of the ADMDB, refer to:

C1.1.2, “Changing the Communication setting of the AD Server and the Encryption setting of the ADMDB” on page C1-6

For more information about how to create and delete the AD projects, refer to:

C1.2.1, “Creating and deleting AD projects” on page C1-28

For more information about how to register RS projects in the AD project, refer to:

C1.2.3, “Registering RS projects in the AD project” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about how to restore RS projects from the AD project, refer to:

“■ Restoring RS projects” on page C1-18

C1.1.5 Backing up and restoring RS projects

You need to restore the RS projects from the AD project after restoring the ADMDB that has been backed up or importing the AD project.

● Backing up RS projects

Running a backup of RS projects copies all files under the RS project folder to the ADMDB. However, version management data and operation histories of RS projects and SCS project data is not subject to the backup of RS projects.

Backup data of RS projects can be made subject to backup of the ADMDB or export of AD projects. For this reason, you need to back up RS projects before backing up the ADMDB or exporting the AD projects.

● Restoring RS projects

You need to restore the RS project from the AD project after restoring the ADMDB or importing the AD project.

Restoring a backed up RS project with a different name creates a copy of the RS projects and configures a test environment.

Re-registering the data of an RS project restored with the same name by using System Structure Navigator reflects the restored content onto the ADMDB.

TIP

- When transferring an AD project to another environment, implement re-registration in order to associate the AD project to the RS projects again. More specifically, you can restore the RS projects from the AD project, specify this project data, and operate registration of the RS projects.
- Data of RS projects restored with a different name cannot be re-registered. They are handled as data of RS projects for new registration.

SEE ALSO

For more information about How to activate the system project backup function, refer to:

"■ Activating the system project backup function" on page C1-3

■ Backing up RS projects

Follow these steps to back up an RS project.

- How to use the system project backup function of the ADS Administration Tool
- How to use the backup function of the System Structure Navigator in AD Organizer

When backing up ADMDB or when exporting an AD project, backup can be performed automatically in advance by using the system project backup function of the ADS Administration Tool.

Follow these steps to backup an RS project by using the System Structure Navigator in AD Organizer.

1. Run System Structure Navigator in AD Organizer and select the RS projects to create a backup for.
2. In the sub menu of System Structure Navigator, select [Back up].
   A confirmation dialog box appears.
3. Click [Yes].
   An RS project can be made subject to backup of the ADMDB or export of an AD project so that backup of the RS project is automatically performed upon each execution.

   Backup starts.

SEE ALSO For more information about Procedures for automatically backing up an RS project when backing up ADMDB, refer to:

"■ Backing up the ADMDB" on page C1-22

For more information about Procedures for automatically backing up an RS project when exporting an AD project, refer to:

"■ Exporting an AD project database" on page C1-39

■ Restoring RS projects

Follow these steps to restore RS projects from the AD project after restoring the ADMDB or importing the AD project. If RS projects having the same name already exist in the restoration destination, an error dialog box is displayed and the restoration cannot be completed.

1. In AD Organizer, open System Structure Navigator.
2. In the System Structure Navigator, select an RS project that you want to restore.
3. In the sub menu of System Structure Navigator, select [Restore from Back up].
   The System Project Restore dialog box appears.

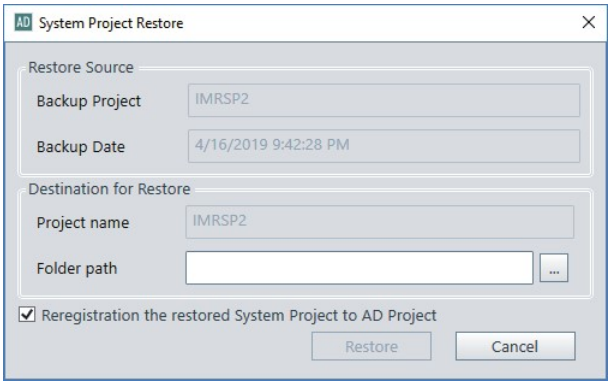


Figure C1.1.5-1 System Project Restore dialog box

4. Select the [Reregister the restored System Project to AD Project] check box if necessary.
   When you select this check box, the restored RS projects are reregistered with AD project.

TIP If you have changed the project name of RS project you want to restore, the check box cannot be selected.

5. To change the RS project to restore, you can input a new project name and folder path.
6. Click the [Restore] button.
   Restoration starts.
   If you have selected the [Reregister the restored System Project to AD Project] check box, RS project is registered with AD project when the restoration is completed.
7. If you have not selected the [Reregister the restored System Project to AD Project] check box, register the restored RS project with AD project.

SEE ALSO For more information about registering RS projects in the AD project, refer to:

C1.2.3, "Registering RS projects in the AD project" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

C1.1.6 Backing up and restoring Library projects

Library projects under RS project folders can be made subject to backup, restoration, export, and import of ADS Administration Tool by registering the corresponding RS projects to AD project.

Library projects which are not under RS project folders can be made subject to backup/restoration and export/import of ADS Administration Tool by registration using AD Organizer with operation similar to that of RS projects.

When the name of the Library project you are trying to register is not in accordance with the naming rules for RS projects, the Library project cannot be registered with AD Organizer. For this reason, you can create a folder in accordance with the naming rules for RS projects on a level above such Library project and then register this folder. We recommend setting the file name as USERLIB

C1.1.7 Backing up and restoring the ADMDB

You can back up or restore the ADMDB.

Operations related to the AD project cannot be performed using other software while the ADMDB is being backed up. Also, you cannot back up an AD project that is in use with other software.

■ Backing up the ADMDB

Back up the ADMDB in the Server Backup dialog box of ADS Administration Tool.

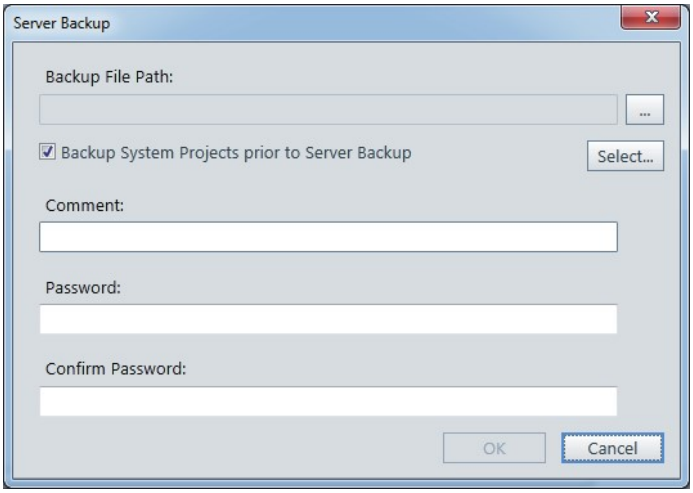


Figure C1.1.7-1 Server Backup dialog box

Activating the system project backup function by using the ADS Administration Tool activates the "[Backup System Projects prior to Server Backup]" check box. The check box is deactivated when activation of the system project backup function fails.

Clearing the "[Backup System Projects prior to Server Backup]" check box deactivates the system project backup function.

Backing up the ADMDB includes all data in the database.

TIP

- You cannot back up only a part of ADMDB data.
- If a data modification request is received from AD Organizer while the ADMDB is being backed up, the data modification request from AD Organizer results in an error or you must wait until the backup is complete.
- Running a backup when the AD project file is being checked-out by another user automatically cancels the checked-out status from the backed up project. For this reason, the checked-out status is not inherited by restoring the backup data.

SEE ALSO

For more information about How to activate the system project backup function, refer to:

"■ Activating the system project backup function" on page C1-3

● Backup password

When you back up the ADMDB, you are asked to enter a password. This password is required when you restore the ADMDB.

● Items set in the Server Backup dialog box

The following table shows the items set in the Server Backup dialog box and their explanations.

Table C1.1.7-1 Items set in the Server Backup dialog box

Setting items	Description
Backup File Path	Specify the folder to output the backup file to. The file path can contain up to 180 characters. The backup file is saved to this folder. When the size of the backup file exceeds 100 MB, the file is automatically split into and saved as multiple files.
Backup System Projects prior to Server Backup	Select the check box to backup system projects prior to backup of the ADMDB or clear the check box not to backup system projects. By default, it is selected. Selecting the check box activates the Select button.
Comment	Enter a comment. The text appears in the Server Restoration dialog box when restoring the database. The maximum number of characters is 128.
Password	Enter a 1 to 8-character length password that is required when restoring the database. You can use single-byte alphanumeric characters, under score (_), hyphen (-), and period. The password is case-sensitive.
Confirm password	Enter the password again to confirm.

Items set in the System Project Selection dialog box

System Project is a general term for RS Projects of ProSafe-RS and VP Projects of CENTUM VP.

IMPORTANT

If a system project has not been backed up prior to backing up the ADMDB, when restoring the ADMDB, a database inconsistency will occur between the ADMDB and system project.

System projects must be backed up prior to backing up the ADMDB.

As activating the system project backup function activates the "[Backup System Projects prior to Server Backup]" check box, system projects will be automatically backed up prior to backing up the ADMDB.

By selecting the "Backup System Projects prior to Server Backup" check box and clicking the Select button, the System Project Selection dialog box appears.

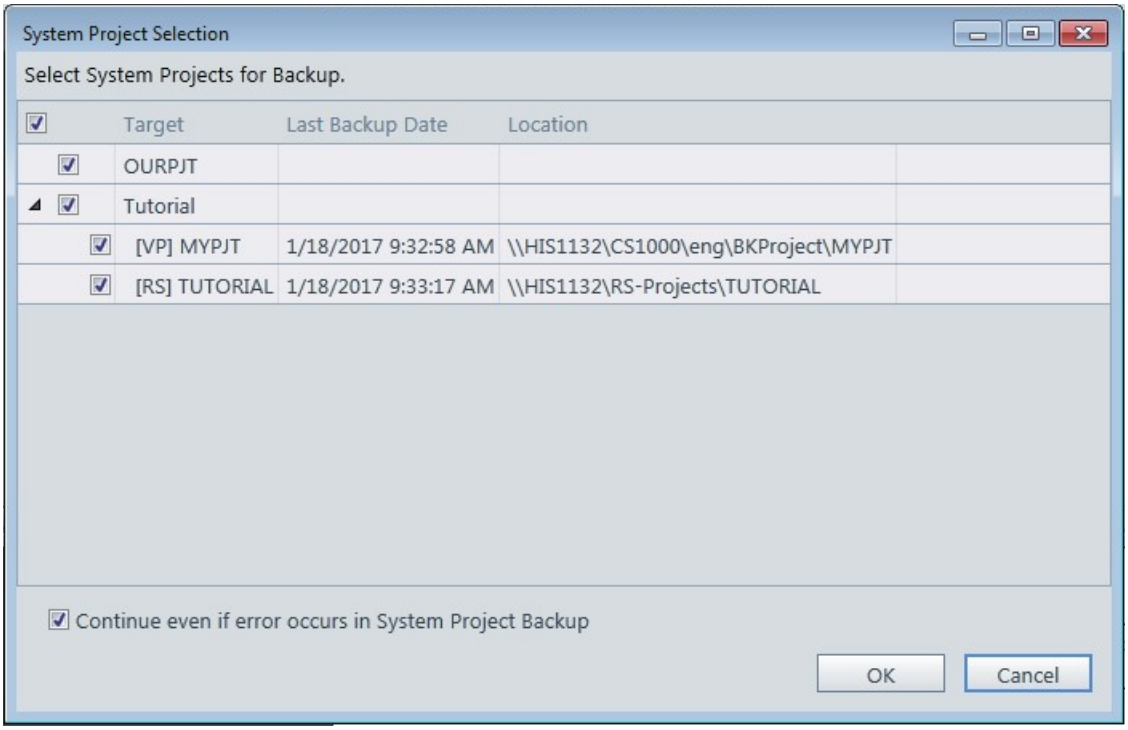


Figure C1.1.7-2 System Project Selection dialog box

The following table explains the items set in the System Project Selection dialog box.

TIP

The system project backup function is equivalent to the backup function of the System Structure Navigator in AD Organizer.

Table C1.1.7-2 Items set in the System Project Selection dialog box

Setting items	Description
Select System Projects for Backup.	In the System Project Selection dialog box, select the projects to backup to the server. By default, all check boxes are selected. A greater number of projects subject to backup will require more time to complete the backup. Check boxes for projects that do not need to be backed up can be cleared.
Continue even if error occurs in System Project Backup	Select whether to skip the backup of certain projects that cannot be accessed and proceed to backup of the next project or to stop the backup process when backing up system projects. There is no need to set this item if only a single system project is being backed up.

IMPORTANT

If a backup is performed by skipping errors when backing up multiple system projects, be sure to separately backup the system projects that have been skipped. Results of the backup are displayed as a message in the Backup Process window.

Backing up the ADMDB

Follow these steps to back up the ADMDB:

1. From the menu of ADS Administration Tool, select [Server] > [Backup File Path].
   The Backup Confirmation dialog box appears.
2. Click [OK].

The Server Backup dialog box appears.

3. Select the [Backup System Projects prior to Server Backup] check box.
   The [Select] button is activated.
4. Click [Select].
   The System Project Selection dialog box appears.
5. Select the system projects to backup.
6. Perform one of the following operations for the setting of the [Continue even if error occurs in System Project Backup] check box:
   - Select the check box if you wish to continue the process.
     When a certain projects of the system projects subject to backup cannot be accessed, skip the backup of such projects and proceed to backup of the next project.
   - Clear the check box if you wish to stop the process.
7. Click [OK].
8. In the Server Backup dialog box, specify [Backup File Path] and enter [Comment] and [Password].
9. In the Server Backup dialog box, click [OK].
   Backup starts and the Server Backup Progress window appears.

   If server backup is successful, a file with the following name will be generated in the output destination folder. The content displayed in the Server Backup Progress window will be saved in this file.

   `Operation.log`

TIP In the message area within the Server Backup Progress window, select [Copy] from the context menu to copy the message to the clipboard.

Restore the ADMDB

You can restore the backed-up ADMDB. Restore the ADMDB from the Server Restoration dialog box in ADS Administration Tool.

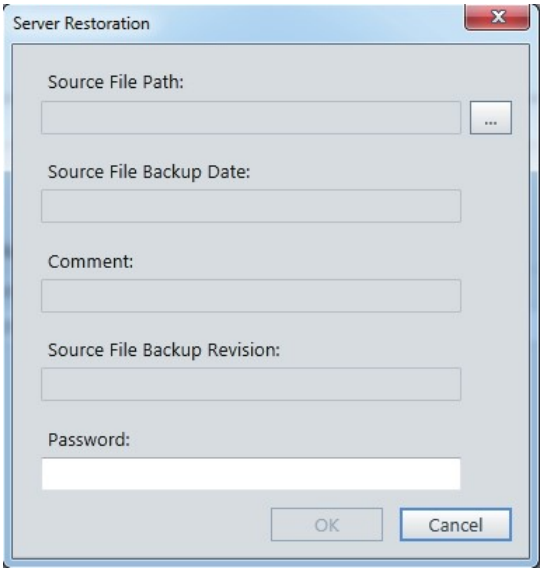


Figure C1.1.7-3 Server Restoration dialog box

Restoration replaces the ADMDB at the destination of the restoration with the restored ADMDB. The AD Server where the database is restored to must have the definitions of the Windows users and user groups used in the AD Server from which the database was backed

up. To restore the database, it is necessary to enter the password entered at the time of back-up.

IMPORTANT

After restoring the ADMDB, you must also restore the system projects and Library projects by using AD Organizer.

Not restoring the system projects and Library projects leads to inconsistencies between the AD project database and system project database.

TIP

- You cannot restore the ADMDB while it is being updated.
- Encryption of the restored ADMDB depends on the encryption setting on the computer where the ADMDB is restored regardless of the encryption setting on the computer where the backup ADMDB is stored.
- The location setting of the ADMDB is not subject to the backup. For this reason, when the locations of the ADMDB differ between backup and restoration, a restoration runs in relation to the location of the ADMDB at the time of restoration.

Restoring the backed-up ADMDB

Follow these steps to restore the backed up ADMDB:

1. From the menu of ADS Administration Tool, select [Server] > [Restore].
   The Server Restoration dialog box appears.
2. In the Server Restoration dialog box, click [OK].
   The Server Restoration dialog box appears.
3. In the Server Restoration dialog box, click the file selection button and select the folder you wish to restore.
   In the Server Restoration dialog box, the path of the file to be restored appears under [Source File Path].
4. Under [Password] in the Server Restoration dialog box, enter the password that was entered at the time of backup.
5. In the Server Restoration dialog box, click [OK].
6. If any AD Server setting information or AD project exists at the destination to restore the database to, a confirmation dialog box appears. Place a check in [Yes, I want to restore.] and click [OK].
   Restoration of the ADMDB starts, and the Server Restore Progress dialog box appears.

   If no AD Server setting information or AD project exists on the destination computer, restoration of the ADMDB starts and the Server Restore Progress dialog box appears.
7. When restoration of the ADMDB is complete, restore the RS projects by using AD Organizer.

TIP

If you have restored the ADMDB on a computer that is not the one where the backup was made, review the communication setup of AD Server.

When moving AD Server by restoring the ADMDB on a different computer or when changing the IP address of AD Server

Follow these steps to move AD Server by restoring the ADMDB on a different computer or to change the IP address of AD Server:

1. If you want to move AD Server to a different computer, restore the backed-up ADMDB on the destination computer. If you want to change the IP address of AD Server, change the IP address.
2. Check the communication setting of AD Server.
3. Start AD Organizer.
   The Select AD Project dialog box appears.
4. In the Select AD Project dialog box, specify AD Server and select the AD projects.
5. If you are restoring the ADMDB, restore the RS projects and Library projects by using AD Organizer.
6. Open System Structure Navigator in AD Organizer and start Revision History Utility.
7. After Revision History Utility is started, close Revision History Utility without doing anything.
   The internal data for retaining the AD Server address is updated with this operation.

C1.1.8 Viewing the history of backup and export operations

You can view the back up history of the ADMDB and export history of AD projects.

Viewing the history

You can view the history of backup and export operations through the Backup/Export History dialog box.

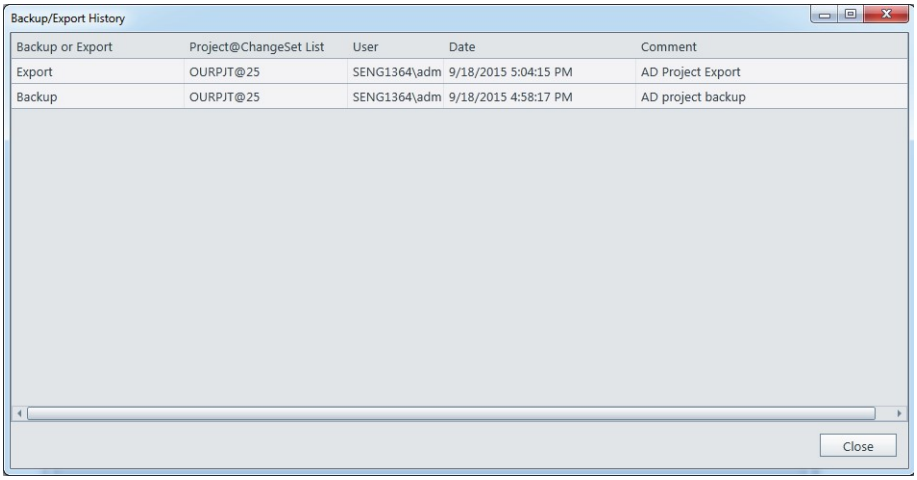


Figure C1.1.8-1 Backup/Export History dialog box

Items displayed in the Backup/Export History dialog box

The following table shows the items displayed in the Backup/Export History dialog box.

Table C1.1.8-1 Items displayed in the Backup/Export History dialog box

Item	Description
Backup or Export	"Backup" or "Export" is displayed.
Project@Change Set List	"AD project name@Change Set ID" is displayed. If two or more AD projects had been registered in the ADMDB when the ADMDB was backed up, the AD projects are listed with a comma in between.
User	The name of the user who executed the backup or export is displayed.
Date	The date and time of backup or export execution is displayed.
Comment	The comment that was set at the time of backup or export is displayed.

Viewing the history of backup and export operations

Follow this step to view the history of backup and export operations:

- From the [File] menu of ADS Administration Tool, select [Backup/Export History].

C1.2 Management of AD projects

The following AD project management tasks can be performed by using ADS Administration Tool:

- Creating and deleting AD projects
- Modifying properties of AD projects
- Controlling access to AD projects
- Export and import AD projects
- Prohibiting and permitting modification of AD project data
- Forcibly canceling the checked-out status of currently checked-out AD project files

C1.2.1 Creating and deleting AD projects

You can create or delete AD projects on or from AD Server.

Creating AD projects

You can create an AD project on AD Server. An AD project can be created with the Project Creation dialog box of ADS Administration Tool.

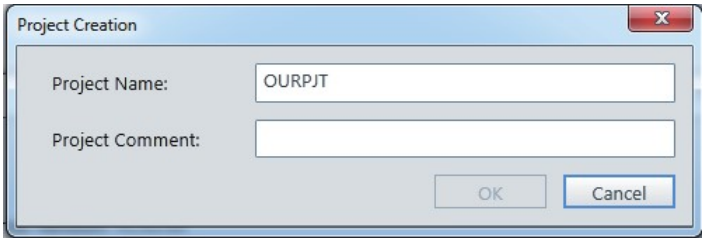


Figure C1.2.1-1 Project Creation dialog box

The following table shows the items set in the Project Creation dialog box and their explanations.

Table C1.2.1-1 Items set in the Project Creation dialog box

Setting items	Description
Project Name	Enter an AD project name using up to 50 single-byte alphanumeric characters and "_" (underscore). The first character must be an alphabetic character. The default project name is OURPJT.
Project Comment	Enter a comment of the AD project using up to 128 characters.

Creating an AD project

Follow these steps to create an AD project:

1. Click [Create Project] button in the ADS Administration Tool.
   The Project Creation dialog box appears.
2. In the Project Creation dialog box, you can enter the project name and project comment and then click [OK].
   The AD project is created. The created project appears in the list of ADS Administration Tool.

Deleting an AD project

You can delete any AD project that is created on AD Server. When deleting an AD project, you are required to confirm the deletion.

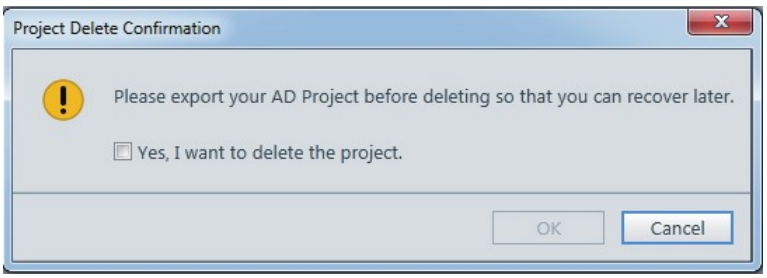


Figure C1.2.1-2 Project Delete Confirmation

IMPORTANT

When deleting an AD project, you must first unregister the RS projects that are registered in the AD project and then delete the AD project.

If you delete an AD project without unregistering the RS projects, you can no longer perform operations on the RS projects such as registering or deleting the RS projects.

If you have deleted an AD project without unregistering the RS projects, contact YOKOGAWA Service.

Deleting an AD project

Follow these steps to delete an AD project:

1. In AD Organizer, unregister the RS projects registered with the AD project that you want to delete.
2. In ADS Administration Tool, select the project you want to delete.
3. On the toolbar, click [Delete Project] button.
   The Project Delete Confirmation dialog box appears.
4. In the Project Delete Confirmation dialog box, place a check in the check box for [Yes, I want to delete the project.] and click [OK].

Modifying properties of AD projects

Modify the Project Name and Project Comment of an AD project in the Project Property dialog box of ADS Administration Tool.

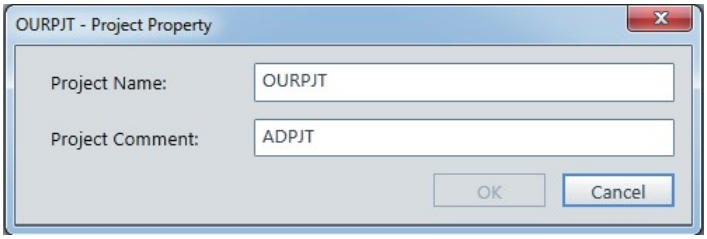


Figure C1.2.1-3 Project Property dialog box

Modifying the properties of AD projects

Follow these steps to modify the Project Name and Project Comment of AD projects:

1. In ADS Administration Tool, select the project whose properties you wish to modify.
2. From the menu bar of ADS Administration Tool, select [Project] > [Properties].
   The Project Property dialog box appears.
3. Enter the project name and project comment and then click [OK].

C1.2.2 Controlling access to AD projects

After creating an AD project, you can manage the users who access the AD project and define access control.

Configure access control of AD projects for all users who will be performing engineering and/or maintenance of ProSafe-RS.

IMPORTANT

Before you configure the access control, close all AD Organizers that connect to the AD project for which you are configuring.

If the IT security model is set to Standard model or Strengthened model, configure access control of AD projects for all users belonging to the following groups:

- PSF_ENGINEER
- PSF_ENGINEER_LCL
- PSF_MAINTENANCE
- PSF_MAINTENANCE_LCL

Setting user security for AD projects

You can use the Access Permission Definition dialog box to set user security. Follow these steps to display the Access Permission Definition dialog box:

- On the toolbar of ADS Administration Tool, click [Access Control] button.
  The Access Permission Definition dialog box appears.

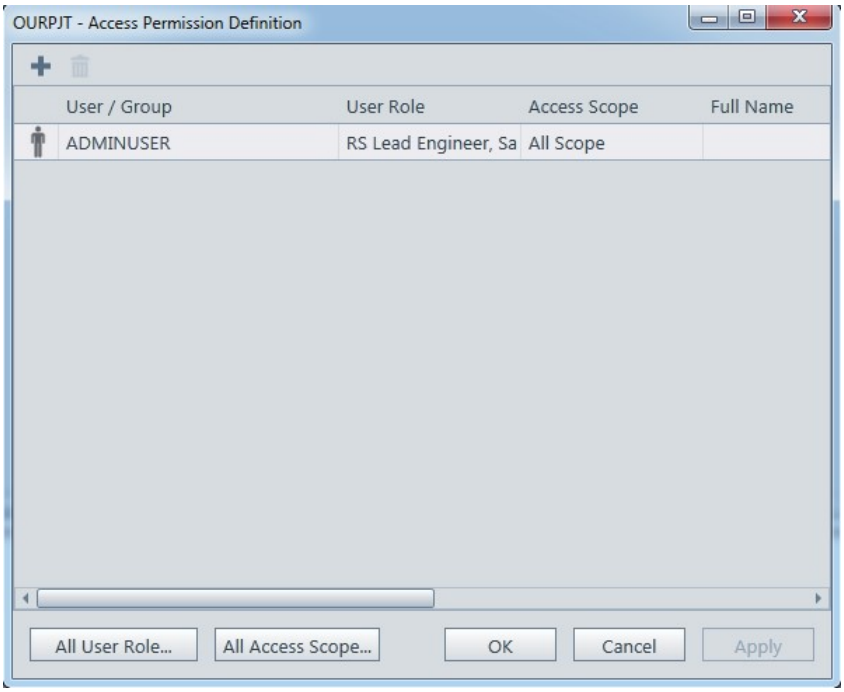


Figure C1.2.2-1 Access Permission Definition dialog box

User management and authentication

The user name and password of the currently logged-on Windows user are authenticated against the computer running AD Organizer by using a function provided with Windows.

Operation of ADS Administration Tool when the computer name and the domain name of AD Server are the same

If the name of the computer with AD Server is identical to the name of the domain to which the computer belongs, the user who tries to access AD Server from AD Organizer is regarded as a local user even if the user is a member of the domain.

The computer name of AD Server must be different from the name of the domain to which the user belongs.

Correspondence when settings of the Windows user are changed

When you change Windows user settings, such as the password or the group to which a user belongs, the change may not be reflected immediately. In such case, log off from the computer where AD Organizer is installed and log on again. Logging off and on is not required on the computer with AD Server. If you are a domain user, you must implement the log off and on operation twice.

Access control

Access of each user can be controlled for individual files and functions of an AD project. Access permission is granted to Windows users or groups. Access permission is a right which combines one or multiple user roles and one access scope.

Defining user roles

User roles are the definition of the access permissions that are appropriate for the user roles of ProSafe-RS.

The following shows types of access permissions.

- Access permissions on objects
  Access permissions that define reference, modification, creation, and deletion of data
- Access permissions on functions
  Access permissions that define acceptability of running functions

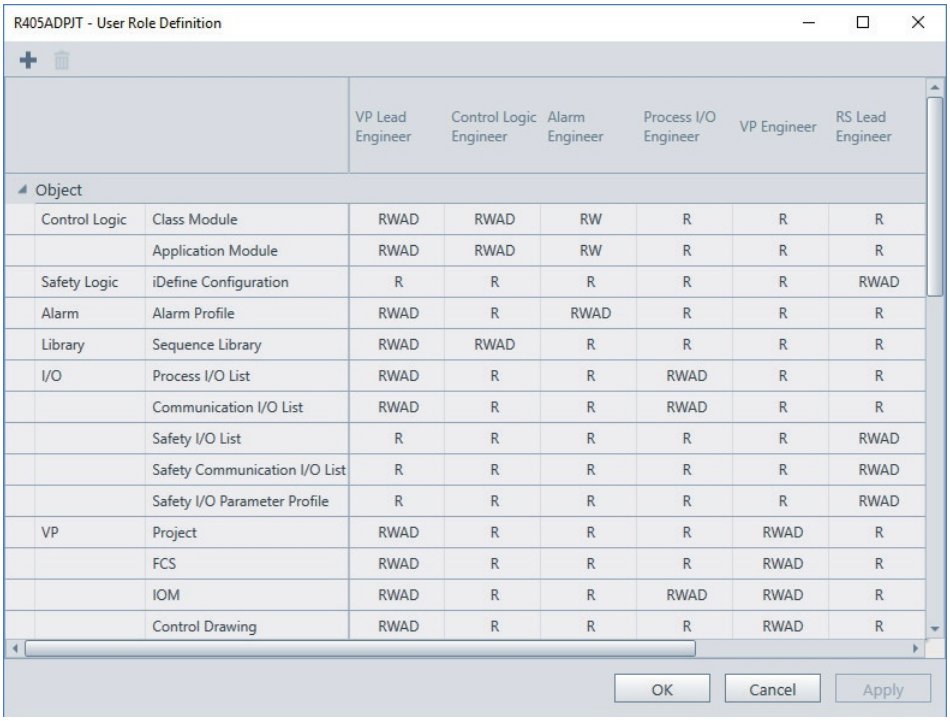
There are the following types of user roles:

- System definition user role
  Is a user role prepared to start with. You cannot change its settings.

  The system definition user roles of ProSafe-RS are as follows.
  - RS Lead Engineer
  - Safety Logic Engineer
  - Safety I/O Engineer
  - iDefine Engineer
  - RS Engineer
- Customizable user role
  Is a user role defined by user using the ADS Administration Tool.

  You can set access permissions on objects and functions.

The following figure shows examples of the User Role Definition dialog box.



		VP Lead Engineer	Control Logic Engineer	Alarm Engineer	Process I/O Engineer	VP Engineer	RS Lead Engineer
Object							
Control Logic	Class Module	RWAD	RWAD	RW	R	R	R
	Application Module	RWAD	RWAD	RW	R	R	R
Safety Logic	iDefine Configuration	R	R	R	R	R	RWAD
Alarm	Alarm Profile	RWAD	R	RWAD	R	R	R
Library	Sequence Library	RWAD	RWAD	R	R	R	R
I/O	Process I/O List	RWAD	R	R	RWAD	R	R
	Communication I/O List	RWAD	R	R	RWAD	R	R
	Safety I/O List	R	R	R	R	R	RWAD
	Safety Communication I/O List	R	R	R	R	R	RWAD
	Safety I/O Parameter Profile	R	R	R	R	R	RWAD
VP	Project	RWAD	R	R	R	RWAD	R
	FCS	RWAD	R	R	R	RWAD	R
	IOM	RWAD	R	R	RWAD	RWAD	R
	Control Drawing	RWAD	R	R	R	RWAD	R

Figure C1.2.2-2 Examples of the User Role Definition dialog box appear.

Access permissions on objects

The following table shows the access permissions on objects.

Table C1.2.2-1 List of access permissions on objects

Access permissions	Description
R	Able to reference the content of the applicable object
RW	Able to reference and change the content of the applicable object
RWA	Able to reference, change, and create the content of the applicable object
RWAD	Able to reference, change, create, and delete the content of the applicable object

The following table shows the types of data on which access permissions can be defined and the operations for defining them.

Table C1.2.2-2 Types of data on which access permissions can be defined

Data type		Applicable folder or applicable file and permitted operations	Editor used
I/O	Safety I/O List	Creating, editing, and deleting a safety I/O list Creating, editing, deleting, and applying grid rules	Safety I/O Editor
	Safety Communication I/O List	Creating, editing, and deleting a safety communication I/O list Creating, editing, deleting, and applying grid rules	Safety Communication I/O Editor
	Safety I/O Parameter Profile	Editing a safety I/O parameter profile	Safety I/O Parameter Profile Editor
Safety Logic	iDefine Configuration	Importing an iDefine-config file	System Structure Navigator

Continues on the next page

Table C1.2.2-2 Types of data on which access permissions can be defined (Table continued)

Data type		Applicable folder or applicable file and permitted operations	Editor used
RS	Project	The following operations are permitted in relation to the RS project folder of System Structure Navigator and the initial folders or initial files under the project folder. • Registering and unregistering an RS project • Backing up and restoring RS projects • Editing the comments of RS projects	System Structure Navigator
	SCS	The following operations are permitted in relation to the SCS folder of System Structure Navigator and the initial folders or initial files under the SCS folder. • Creating an SCS by importing an SCS • Deleting an SCS • Exporting a ProSafe-RS I/O file • Importing an iDefine-config file	System Structure Navigator
	IOM	The following operations are permitted in relation to the N-IO folder, F-IO folder, and subordinate folders or files of System Structure Navigator. • Adding a Node and IOM • Deleting a Node and IOM • Editing a Node and IOM	IOM Definition Editor

TIP

Operations with SCS Manager and operations with Generation Manager are not applicable to object access permissions.

Access permissions on functions

The following table shows the types of functions on which access permissions can be defined and the operations for defining them.

Table C1.2.2-3 Types of functions on which access permissions can be defined and permitted operations

Function type		Permitted operations
Document	Document	Creation, deletion, and reference of documents (*1)
ModPack	Creation	ModPack Creation
	Closing	ModPack Closing
	Reopen	ModPack Reopen
	Management	ModPack Management
	Implementation	ModPack Implementation
Revision History	Re-assign ModPack	Changing ModPack IDs in the existing revision history
	Modify Comment	Changing check-in comments in the existing revision history
	Set Label	Setting labels
	Delete Label	Deleting existing labels
	Change Label	Changing the comments of existing labels
	Utility	Running Revision History Utility

*1: When access is not permitted, documents can be referenced only.

Defining custom user roles

Rights can be added by using the Access Permission Definition dialog box. Follow these steps to define custom user roles.

1. In ADS Administration Tool, select the AD project for which you want to apply access control, and then click [Access Control] button.
   The Access Permission Definition dialog box appears.
2. Click [All User Role] button.
   The User Role Definition dialog box appears. By default, only the System definition user role appears.
3. Right-click the mouse in a blank space inside the user role list display area and select [Add User Role].
   The Add User Role Definition dialog box appears.
4. Enter a user role name consisting of up to 20 characters.
   A user role name can contain single-byte alphanumeric characters, single-byte space, and single-byte period.
5. Click the [OK] button.
   A column for a new user role is added to the User Role Definition dialog box. By default, all access rights are added.
6. Change the access rights on [objects] and [functions].
   Click the right edge of the cell to display the drop-down list.
7. In the User Role Definition dialog box, click [OK] button.

Access scope definition

Access scope is the access permissions to the files and folders at the levels under an AD project in AD Server.

Access permissions can be defined on the following folders and files shown in the System Structure Navigator.

- Safety I/O files and safety communication I/O files under the I/O List folder
- Safety I/O parameter profile file under the I/O-Profiles folder
- Folders and files under the RS project folder

The following figure shows an example of the screen for defining the access scope.

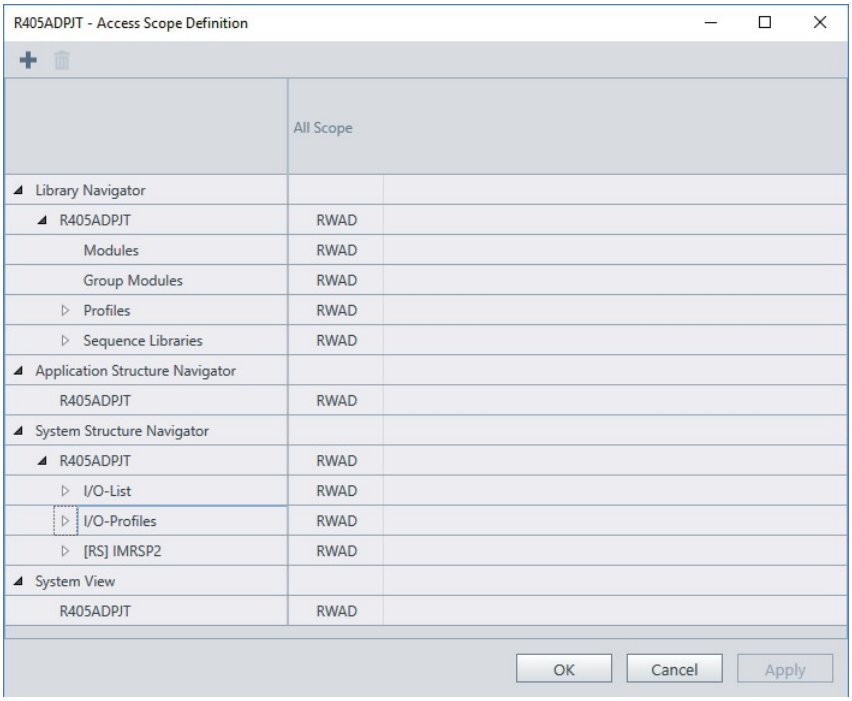


Figure C1.2.2-3 Example of screen for defining an access scope

The following shows types of access rights for an access scope.

Table C1.2.2-4 List of access rights for an access scope

Access right	Description
R	The content of applicable folders and applicable files can be referenced
RW	The content of applicable folders and applicable files can be referenced and altered However, the right to change the folder is the right to change the folder name and properties.
RWA	The content of applicable folders and applicable files can be referenced, altered, and created However, files cannot be created.
RWAD	The content of applicable folders and applicable files can be referenced, altered, created, and deleted

An access scope named All Scope is provided in advance. When this access scope is used, the access permission for folders and files on all tier levels of the AD project is RWAD.

Defining an access scope

Follow these steps to define an access scope:

1. Select the Project in the ADS Administration Tool, and then click [Access Control] button.
   The Access Permission Definition dialog box appears.
2. In the Access Permission Definition dialog box, click [All Access Scope].
   The Access Scope Definition dialog box appears.
3. Right-click the mouse in a blank space inside the access scope list display area and select [Add Access Scope].
   The Add Access Scope dialog box appears.
4. Enter an access scope name consisting of up to 20 characters.
   An access scope name can contain single-byte alphanumeric characters, single-byte space and single-byte period.

5. Click the [OK] button.
   A column for a new access scope is added to the Access Scope Definition dialog box.
6. Define access rights for every folder or file.
   The same rights as those constituting All Scope are defined by default. Access rights can be selected from the drop-down list.

   Selecting [Inheritance of Access Permission] from the drop-down list defines, for all folders and files under the folder, the same right as that applied to the selected folder.
7. In the Access Scope Definition dialog box, click [OK].

IMPORTANT

If you click [OK] or [Apply] in the Access Scope Definition dialog box while check-in is being performed by other user, your operation on access scope definition may fail with a warning message. If this happens, wait until the check-in is complete and then click [OK] or [Apply] in the Access Scope Definition dialog box.

Editing user roles and access scopes

Follow these steps to change the name of, delete, or duplicate a user role or access scope:

TIP Added user roles and access scopes can be edited. The user roles and access scopes prepared by default can not be edited.

- Right-click the name of the user role or the name of the access scope you wish to rename, delete, or duplicate and make a selection from amongst the displayed items.
  - To rename, select [Edit User Role Name] or [Edit Access Scope Name].
  - To delete, select [Delete User Role] or [Delete Access Scope].
  - To duplicate the item, select [Duplicate User Role] or [Duplicate Access Scope].

Access permissions when the AD server is upgraded

- User roles and access permissions when the AD server is upgraded to R4.03.10 or later
  Safety communication I/O list is added as a subject of user roles. Safety Communication I/O List is added as an object in the User Role Definition dialog box.

  Access permissions for user roles in relation to the safety communication I/O list are assigned as follows:
  - RWAD is assigned to RS Lead Engineer and Safety I/O Engineer.
  - R is assigned to system definition user roles other than RS Lead Engineer and Safety I/O Engineer.
  - R is assigned to custom user roles.

  In addition, the safety communication I/O definition is automatically added as a subject of the access scope. Specifically, the safety communication I/O definition is added below the SCS project.
- User roles and access permissions when the AD server is upgraded to R4.05 or later
  Safety I/O parameter profile is added as an object controlled by user roles. Safety I/O parameter profile is added as an object in the User Role Definition dialog box.

  Access permissions for user roles in relation to the safety I/O parameter profile are assigned as follows:
  - RWAD is assigned to RS Lead Engineer and Safety I/O Engineer.

- R is assigned to system definition user roles other than RS Lead Engineer and Safety I/O Engineer.
- R is assigned to custom user roles.

In addition, safety I/O parameter profile is automatically added as an object of the access scope. Specifically, I/O-Profiles is added below the AD project and the safety I/O parameter profile definition is added below the I/O-Profiles.

Setting access right for Windows users

Follow these steps to set Access Right for a Windows user or group.

1. In ADS Administration Tool, select the project for which you want to apply access control.
2. Display the Access Permission Definition dialog box.
3. Right-click the mouse in a blank space inside the list display area of the Access Permission Definition dialog box and select [Add User].
   A line to add a user is added in the Access Permission Definition dialog box.
4. Enter a Windows user name or group name consisting of up to 36 characters.
   - To register a local user or local group, enter a user name or group name.
   - To register a domain user or domain group, enter a name in the following format: `domain name\user name`, or `domain name\group name`
   - For a standard or strengthened IT security model, specify users that belong to the PSF_ENGINEER group.

   You can also preregister a user not yet registered to Windows. In this case, enter a name according to the Windows naming rules.
5. Select a desired user role from the drop-down list.
   You can select multiple user roles. VP Lead Engineer and RS Lead Engineer are selected by default.
6. Select a desired access scope from the drop-down list.
   You can select only one access scope. [All Scope] is selected by default.
7. In the Access Permission Definition dialog box, click [OK].

TIP

- To change a user name, select the cell containing the user name and change the name.
- To delete a user, select the user name and then click [Delete User] button.

C1.2.3 Export and import AD projects

You can export and import AD projects. By exporting an AD project and then importing it, you can create a copy of the AD project.

With the default export settings, system projects are automatically backed up before an AD project is exported. This setting is activated by activating the system project backup function.

An AD project in the process of backup cannot be operated using other software. Also, back-up cannot be performed for an AD project that is in use with other software.

SEE ALSO For more information about How to activate the system project backup function, refer to:

"■ Activating the system project backup function" on page C1-3

■ Export AD projects

The export of an AD project can be implemented through the Project Export dialog box of the ADS Administration Tool.

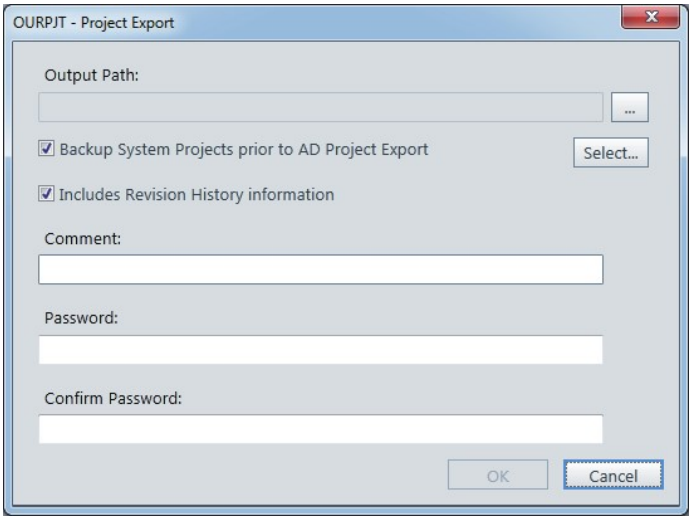


Figure C1.2.3-1 Project Export dialog box

Activating the system project backup function activates the [Backup System Projects prior to AD Project Export] check box. The check box is deactivated when activation of the system project backup function fails.

Clearing the [Backup System Projects prior to AD Project Export] check box deactivates the system project backup function.

When exporting an AD project, you can select whether to export only the latest data and whether to include revision history information together. When only the latest data is exported, only a check-in log of the latest files appears in the Revision History Window at the destination to which the database is imported.

TIP

- When exporting an AD project, you cannot export only a part of the history.
- If you export an AD project while other user is checking in files, the export fails with an error message. You must export after check-in is complete.
- If any files are checked out when you export an AD project, the export is executed with the checked-out status of the files discarded. Therefore, the checked-out status is not inherited when importing the exported AD project.

Export password

You need to enter a password to export the database. This password is used when importing the database.

Items set in the Project Export dialog box

The following table shows the items set in the Project Export dialog box and their explanations.

Table C1.2.3-1 Items set in the Project Export dialog box

Setting items	Description
Output Path	Specify the folder to which the file is exported. The file path can contain up to 180 characters.
Backup System Projects prior to AD Project Export	Select whether to backup system projects before exporting an AD project. By default, it is selected. Selecting the check box activates the Select button. System projects with access rights to PSF_PROCESS are subject to selection for backup.
Includes Revision History information	Specify whether or not to include the history information in the export file. Selecting the check box includes all revision history information in the export file. The check box is selected by default.
Comment	Enter a comment, if necessary. The text appears in the Project Import dialog box when importing the database. The maximum number of characters is 128.
Password	Enter a 1 to 8-character length password that is required when importing the database. You can use single-byte alphanumeric characters, under score (_), hyphen (-), and period. The password is case-sensitive.
Confirm Password	Enter the password again to confirm.

SEE ALSO For more information about Items set in the System Project Selection dialog box, refer to:

"● Items set in the System Project Selection dialog box" on page C1-21

Exporting an AD project database

Follow these steps to export an AD project:

1. In ADS Administration Tool, select the AD project you want to export.
2. From the menu bar of ADS Administration Tool, select [Project] > [Export].
   The Project Export Confirmation dialog box appears.
3. In the Project Export Confirmation dialog box, click [OK].
4. Select the [Backup System Projects prior to AD Project Export] check box.
   The [Select] button is activated.
5. Click [Select].
   The System Project Selection dialog box appears.
6. Select the system projects to backup.
7. Perform one of the following operations for the setting of the [Continue even if error occurs in System Project Backup] check box:
   - Select the check box if you wish to continue the process.
     When a certain projects of the system projects subject to backup cannot be accessed, skip the backup of such projects and proceed to backup of the next project.

- Clear the check box if you wish to stop the process.

8. Click [OK].
9. In the Project Export dialog box, specify [Output Path], and enter the information for [Comment] and [Password]. To include the revision history information in the export file, select the [Includes Revision History information] check box.
10. In the Project Export dialog box, click [OK].
    Export of the AD project starts and the Server Backup Progress window appears.

    If export of the AD project is successful, a file with the following name will be generated in the output destination folder. The content displayed in the Server Backup Progress window will be saved in this file.

    `Operation.log`

TIP

In the message area displayed within the Server Backup Progress window, select [Copy] from the context menu to copy the message to the clipboard.

Import AD projects

You can import an exported AD project. An AD project can be imported through the Project Import dialog box of ADS Administration Tool.

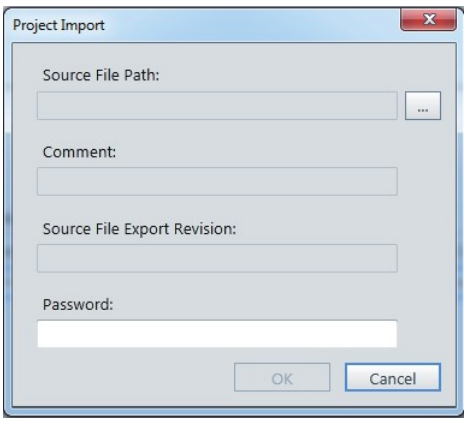


Figure C1.2.3-2 Project Import dialog box

The AD project is imported separately from any AD project that already exists on the computer where you import the AD project. If a project of the same name exists at the import destination, the dialog box for changing the project name appears at the time of import.

The AD Server to import the database to must have the definitions of the Windows users and user groups used in the AD Server from which the database was exported. When performing the import, enter the password entered at the time of export.

IMPORTANT

After importing the AD project, you must also restore the RS project by using AD Organizer. Not restoring the RS projects will cause inconsistencies between the AD project database and the RS project database.

TIP

Encryption of the imported AD project database depends on the encryption setting on the computer to which the database is imported, regardless of the encryption setting on the computer from which you exported the database.

Importing an AD project database

Follow these steps to import an exported AD project:

1. From the menu bar of ADS Administration Tool, select [Project] > [Import].
   The Project Import Confirmation dialog box appears.
2. In the Project Import Confirmation dialog box, click [OK].
   The Project Import dialog box appears.
3. In the Project Import dialog box, click the folder selection button and select the folder you wish to import.
   The path of the file to be imported appears under [Source File Path] in the Project Import dialog box.
4. Under [Password] in the Project Import dialog box, enter the password entered at the time of export.
5. In the Project Import dialog box, click [OK].
6. If an AD project of the same name exists at the import destination, the Project Name Change dialog box appears. In the Project Name Change dialog box, change the project name and click [OK].
   Import of the AD project starts and the Project Import Progress dialog box appears.

   If no AD project of the same name exists at the import destination, import of the AD project starts, and the Project Import Progress dialog box appears.
7. When the import is complete, restore the RS projects by using AD Organizer.
8. After selecting the applicable RS projects from System Structure Navigator of AD Organizer, select [Register System Project] from the sub menu.
   The RS projects are re-registered to the ADMDB.

C1.2.4 Prohibiting and permitting modification of AD project data

You can prohibit modification of AD project data. Data is "frozen" while its modification is prohibited. When a frozen AD project is activated, the prohibition of data modification is canceled. Whether a given project is frozen or active can be checked by using ADS Administration Tool.

Modifying frozen data

While frozen, the following operations are prohibited:

- Check-in and check-out of all data in the AD project.
- RS generation
- Operation of each builder started from SCS Manager

However, the following operations still can be performed while frozen.

- Referencing data
- Discarding the checked-out of data in the AD project
- Deleting an AD project

Purpose of prohibiting AD project data modifications

Freeze an AD project to prohibit, for a specific period, modification of the data of an active AD project whose software is to be modified.

For example, you may want to export active AD project data and modify it at a different location as part of plant reconstruction, etc., and then import the data to an active AD project at the plant site to reflect the changes. If you don't want the data of the active AD project at the plant site to be modified after the project data is exported until it is imported, freeze the AD project.

Prohibiting AD project data modifications

You can prohibit modification of AD project data. Data is "frozen" while its modification is prohibited. While frozen, check-in and check-out of all of the data of the corresponding AD project, RS generation, and SCS Manager operations are prohibited. However, you can still reference the data, cancel the checked-out status, or delete the project. Follow these steps to prohibit modification of AD project data:

1. In ADS Administration Tool, select the project whose data you wish to prohibit modification of.
2. From the menu bar of ADS Administration Tool, select [Project] > [Freeze/Activate]. The Freeze/Activate dialog box appears.
3. In the Freeze/Activate dialog box, click [OK].

TIP

When exporting an active AD project from a local plant to a different location and then importing and returning the project to the local plant after engineering in the different location, the imported project is reflected on the active project. If the project is frozen, modification of the imported project can be prohibited.

Canceling the prohibition of AD project data modifications

Follow these steps to cancel the prohibition for modification of the data of a frozen AD project.

1. In ADS Administration Tool, select the project for which you wish to cancel the prohibition of modification.

2. From the menu bar of ADS Administration Tool, select [Project] > [Freeze/Activate]. The Freeze/Activate dialog box appears.
3. In the Freeze/Activate dialog box, click [OK].

C1.2.5 Forcibly canceling the checked-out status of currently checked-out files

You can forcibly cancel the checked-out status of a file currently checked out. You may use this function to cancel the checked-out status of a file that remains checked out for some reason.

You can forcibly cancel the checked-out status of the files that are checked out by a certain user at a time.

The Discard Check-out dialog box of ADS Administration Tool is used to forcibly cancel the checked-out status. The Discard Check-out dialog box shows a list of files currently checked out under the applicable project.

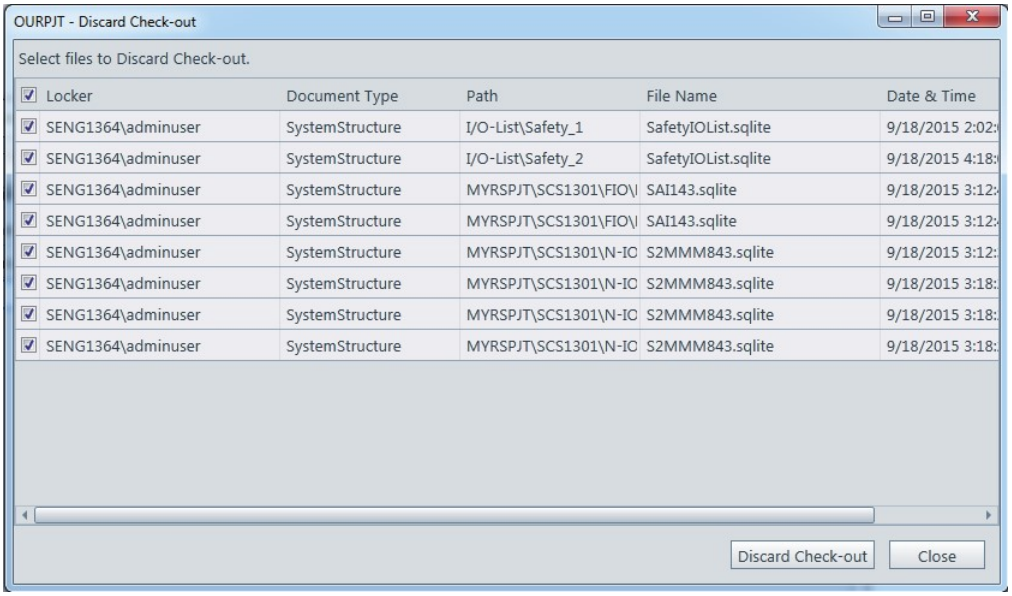


Figure C1.2.5-1 Discard Check-out dialog box

Forcibly canceling the checked-out status of a file currently checked out

Follow these steps to forcibly cancel the checked-out status of a file currently checked out:

1. In ADS Administration Tool, select the project for which you wish to cancel the checked-out status.
2. From the menu bar of ADS Administration Tool, select [Project] > [Discard Check-out]. The Discard Check-out dialog box appears.
3. In the Discard Check-out dialog box, click the file for which you wish to cancel the checked-out status.
4. In the Discard Check-out dialog box, click [Discard Check-out].

C2. History management

In an environment where the Engineering Server Function has been activated, the history management function is provided.

The subjects of history management are Safety I/O Editor, Safety Communication I/O Editor, and IOM Definition Editor of AD Organizer, SCS Manager, builders, tools such as the SCS Maintenance Support Tool, and Generation Manager.

The history management function is a function which records and manages the information of what kind of changes were along with when and by whom the changes were made and enables the checking of such history information.

Only SCS Manager is used with engineering in an environment in which only Engineering Server Function and Safety System Engineering and Maintenance Function package are activated. The revision history of all builders and editors are stored on AD Server and this revision history can be displayed in the history window of AD Organizer.

TIP

The history management function is a function which is different from the Access Control / Operation History Management functions. Even without the Access Control / Operation History Management packages, the following can be performed by using the history management function.

- Viewing the history in the Revision History window in AD Organizer.
- Displaying differences between two files saved as history in the Revision History window in AD Organizer. The display method consists of starting SCS Manager or builders in the read-only mode and displaying the differences in red.

C2.1 Overview of history management

The operation history management manages the following files in the ADMDB:

- Files of SCS projects that were updated by Generation Manager, as well as those edited by SCS Manager, builders, or other tools
- iDefine-config file imported by using AD Organizer

Furthermore, a group of subjects that were checked-out and changed by using the editors of AD Organizer can be checked-in as a Change Set and saved on the ADMDB. You can associate a Change Set with a ModPack.

You can view the history of editing by SCS Manager, builders, other tools, and the history of revision by Generation Manager through the Operation History Database Viewer and the Modification File Viewer. You can view the history of revisions that were made by using the editors of AD Organizer through the Revision history window.

The timings at which the history of changes are saved when using the history management function are as follows:

- Upon editing with SCS Manager
- Upon reflections and builds of Generation Manager
- Upon check-in of subjects of change by using Safety I/O Editor, Safety Communication I/O Editor, and IOM Definition Editor
- When checking-in the iDefine-config file

History management of SCS Manager, builders, tools, and Generation Manager consists of the following functions:

- Modification file saving function
  Files of SCS project newly created or successfully overwritten are saved on the ADMDB of AD Server.
- Operation logging function
  Information on operation with SCS Manager, builders, and tools are recorded on the ADMDB.
- Start and stop functions
  The user can specify whether to start or stop the revision history function.
- Updating function
  This function matches the files of the ADMDB to the files of SCS Manager when there are differences between the SCS project files of SCS Manager and the SCS project files of the ADMDB.
- Saving of Change Sets
  A group of files that were checked in at the same time are grouped as one set. This grouped set of files is referred to as a Change Set. Changed sets are stored in the Automation Design Master Database (ADMDB).

  When checking-in data that was edited by using the Safety I/O Editor, Safety Communication I/O Editor, and IOM Definition Editor or the iDefine-config file that was created by using iDefine, the check-in is run for the data or file that you selected. Check-in can be run at the same time for multiple subjects of change. Groups of files checked in at the same time are grouped as one Change Set and a Change Set ID is automatically assigned. You can associate a Change Set ID with a ModPack.
- Setting labels
- Displaying the revision history

C2.2 Modification file saving function

The modification file saving function is a function which saves the setting file of an updated SCS project on the ADMDB. This save operation is referred to as a check-in. There are no operations for explicitly saving the file on the ADMDB. The following are timings at which the file is saved:

- When the file is saved with SCS Manager, builders, or tools
- When the file is updated with the import function

At the same time as when the file is saved, this operation information and the name of the user running the operation are recorded on the ADMDB.

The following shows the user names which are recorded:

- Windows login user name when operations have been performed with SCS Manager or AD Organizer started from the Start menu
- HIS user name when operations have been performed with Revision History Utility of AD Organizer started from the tool button toolbox of the browser bar in HIS with Integration with CENTUM

The files subject to the modification file saving function are the setting file of the SCS project and the setting file of the library.

The projects subject to the modification file saving function are the RS projects registered to an AD project. RS projects are subject to this function regardless of whether the SCS project included in the RS project has specified I/O list engineering. When the registration of an RS project with an AD project is canceled, the history management function of such RS project ends.

With the modification file saving function, files are saved with all project attributes.

The project attributes include current project, default project and user-defined project.

All files subject to the modification file saving function are saved when a new SCS project is created, upon check-out with Version Control Tool, upon restoration of the Master database, and upon running the test project creation tool.

TIP

When the operation for opening an SCS project is performed with SCS Manager after an update of the software of ProSafe-RS, the SCS project files of SCS Manager are updated. After the operation for opening each individual SCS project, running the update function saves the files on the ADMDB.

C2.2.1 Operation history of SCS Manager, builders, and tools

With operations of SCS Manager, builders, and tools, the modification file is saved on the ADMDB.

Timings of save

The following table shows the timings at which the modification files are saved on the ADMDB as a result of the operations of each builder inclusive of SCS Manager.

Table C2.2.1-1 Timings at which modified files are saved

No	Type of builder or editor name	Timing at which the modified data is saved	Remarks
1	SCS Manager SCS Constant Builder I/O Parameter Builder Communication I/O Builder SCS Link Transmission Builder Modbus Address Builder DNP3 Communication Builder Tag Builder Alarm Priority Builder Alarm Processing Table Builder	Upon successful Save operation (*1)	The timing at which modified data is saved when an SCS project is newly created is the same as when OK is clicked with SCS project Property. When Save Project or Save Library Dependency of SCS Manager is clicked, Resource Properties, Configuration Property, Library Dependency, Connection Property, Binding, and External Binding are saved. When Path of Library of Library Dependencies is pointing to the LIBRARY folder of its own SCS, the file of the library is saved on the ADMDB.
2	Test Project Creating Tool	When SCS project creation is successful	Only in cases when the RS projects at the SCS project creation destination are subject to the revision history.
3	Version Control Tool	When check-out is successful	-
4	SCS Master DB Recover	When restoration is successful	-
5	SCS Manager (Build)	When a build is started	When Path of Library of Library Dependencies is pointing to the LIBRARY folder of its own SCS, the files of the library to which changes were applied are saved as subjects on the ADMDB.
6	SCS Manager (Revision Update)	When a revision update is successful	SCS projects of older versions are not registered with AD Server. Upon a successful revision update, similar to when an SCS project is newly created, all applicable files are saved on the ADMDB.

*1: Operation that differs from the Access control / Operation history management functions.

Operation information recorded together with the modification files

The following table shows the operation information that is recorded on the ADMDB together when the modification files are saved.

Table C2.2.1-2 Operation information recorded together with the saving of the modification files

No	Type of builder or editor name	Operation information		
		Program name	Operation name	Subject of operation
1	SCS Manager SCS Constant Builder I/O Parameter Builder Communication I/O Builder SCS Link Transmission Builder Modbus Address Builder DNP3 Communication Builder Tag Name Builder Alarm Priority Builder Alarm Processing Table Builder	Builder name	Create Project Save Project Save external binding list Save POU Save Dictionary Save I/O wiring Change SCS project Properties Save dependencies Import Save Builder	SCS project name (example: SCS0101) In the case of a library, the SCS project name
2	Test Project Creating Tool	Builder name	Create Project	SCS project name
3	Version Control Tool	Builder name	Check Out	SCS project name
4	SCS Master database recovery	Builder name	Restore Master Database	SCS project name
5	SCS Manager (Build)	Builder name	Build Project	SCS project name
6	SCS Manager (Revision Update)	Builder name	Create Project	SCS project name

C2.2.2 Operation history of Generation Manager

With operations of Generation Manager, the modification file is saved on the ADMDB.

Timings to save and files to be saved

The timing at which the modification file generated due to the reflection of Generation Manager is saved on the ADMDB and the files subject to the save are as follows:

- Timing at which the modified data is saved: When a reflection is successful
- Files to be saved: Files subject to reflection

Operation information recorded together with the modification files

The operation information that is recorded on the ADMDB together when the modification files are saved are as follows:

- Program name: Generation Manager
- Operation name: Reflection or Build
- Subject of operation: SCS project name

Operation information is recorded with a character sequence having the following configuration:

(Program name) + (,) + (single-byte space) + (operation name) + (,) + (single-byte space) + (subject of operation)

C2.2.3 Operation history of Revision History Utility

With operations of Revision History Utility, the modification file can be saved on the ADMDB.

Timings to save and files to be saved

The following table shows the timings at which the files are saved on the ADMDB due to operations of Revision History Utility and the files subject to the save.

Table C2.2.3-1 Timings at which files are saved and the files subject to the save

Function	Timing at which the modified data is saved	Information to be saved	Remarks
Start	When processing of a start is successful	Files in which there is a difference between the SCS projects of the ADMDB and SCS Manager	This processing of a start is also run when RS projects are registered with an AD project.
Stop	-	-	No files are saved.
Update	When processing of an update is successful	Files in which there is a difference between the SCS projects of the ADMDB and SCS Manager	-

Operation information of Revision History Utility

The following table shows the operation information that is recorded on the ADMDB together when the modification files are saved.

Table C2.2.3-2 Operation information recorded together with the saving of the modification files

Function	Operation information			Remarks
	Program name	Operation name	Subject of operation	
Start	Revision History Utility	Start Revision History	RS project name	Operation history is recorded even in cases when files are not saved with this operation.
Stop	Revision History Utility	Stop Revision History	RS project name	Operation history is recorded although files are not saved with this operation.
Update	Revision History Utility	Update Revision History	RS project name	Operation history is recorded although files are not saved with this operation.

Operation information is recorded with a character sequence having the following configuration:

(Program name) + (,) + (single-byte space) + (operation name) + (,) + (single-byte space) + (subject of operation)

C2.3 Operation logging function

With the modification file saving function, apart from the operation information that is recorded at the same time as the modified file, when the following operations are successful, such operation information is recorded on the ADMDB. The setting file of the SCS project is not changed.

- Build
- Offline download
- Online change download
- Master database off-line download
- IOM download

The following table shows the operation information that is saved on the ADMDB as a result of the operations using SCS Manager or SCS Maintenance Support Tool.

Table C2.3-1 Operation information recorded with the operation logging function

Function	Operation information		
	Program name	Operation name	Subject of operation
Build	SCS Manager	Build Project	SCS project name
Offline download	SCS Manager	Off-line Download	SCS project name
Online change download	SCS Manager	On-line Change Download	SCS project name
Master database off-line download	SCS Manager	Master Database Off-line Download	SCS project name
IOM download	SCS State Management Window	IOM Download	SCS project name

Operation information is recorded with a character sequence having the following configuration:

(Program name) + (,) + (single-byte space) + (operation name) + (,) + (single-byte space) + (subject of operation)

C2.4 Start/Stop function

You can specify whether to start or stop the history management function.

The history management function starts saving the history from when the RS project is registered to an AD project.

Start or stop can be specified in units of RS projects. You cannot specify whether to start or stop the function at the same time for multiple RS projects.

Only the Windows users who satisfy all of the following conditions can run the start/stop function:

- The user has the RWAD right for all categories under the corresponding RS project
- The user belongs to the following User Role with Access Right settings for the RS project of AD Server
  Revision History Utility of Revision History

The start/stop function can be specified with Revision History Utility.

Between the processes run after start or stop is specified, you cannot run operations that lead to new creation, modification, or deletion of files within the corresponding RS project.

Example:

Operations such as the creating of a new SCS project, modification of properties, and overwritten saving / downloading with a builder

The update function is run when revision history is started.

C2.5 Updating function

The updating function resolves differences in cases when there are differences between the setting file of the SCS project of SCS Manager and the setting file of the SCS project recorded on the ADMDB. Such difference between these files are generated upon failure of saving modified files on the ADMDB. In other words, this function saves on the ADMDB the setting file for which a save has failed and equalizes the ADMDB.

The updating function can be run from Revision History Utility.

The updating function can be run in units of RS project. You cannot run updates at the same time for multiple RS projects.

The update process can only be run for RS projects that are running revision history function.

Only the Windows users who satisfy all of the following conditions can run the updating function:

- The user has the RWAD right for all categories under the corresponding RS project
- The user belongs to the following User Role with Access Control settings for AD Server Revision History Utility of Revision History

At the same time as when the files with a difference are saved on the ADMDB, the name of the user running the operation is recorded on the ADMDB. The user name to be recorded are as follows:

- Windows login user name when operations have been performed with Revision History Utility of AD Organizer started from the Start menu
- HIS user name when operations have been performed with Revision History Utility of AD Organizer started from the tool button toolbox of the browser bar of HIS in an environment of Integration with CENTUM

During an update process, you cannot run operations that lead to new creation, modification, or deletion of files within the corresponding RS project.
Example:

Processes such as the creating of a new SCS project, modification of properties, and overwritten saving and downloading with a builder

C2.6 Operations of the revision history function

This section describes how to operate the Revision History Utility window when using the history management function along with precautions in regard to operations of SCS Manager and Generation Manager

C2.6.1 Window of Revision History Utility

Revision History Utility can be used to start, stop, and updates history management.

The following figure shows the Revision History Utility dialog box.

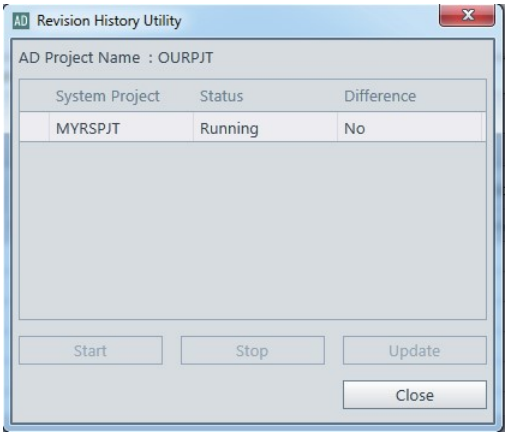


Figure C2.6.1-1 Revision History Utility dialog box.

The following figure shows items displayed on the Revision History Utility dialog box.

Table C2.6.1-1 Items displayed on the Revision History Utility

Displayed item	Description	Remarks
System project	The names of RS projects that are registered with an AD project and accessible from a computer on which the Revision History Utility screen has been started are displayed.	-
Status	The status of history management is displayed. Running: History management is running. Stopped: History management is stopped.	-
Difference	Whether or not there are differences between the files of AD Server and SCS Manager that are generated due to modification file saving errors is displayed. Yes: When there may be a file that could not be saved to the ADMDB No: When there are no files that could not be saved to the ADMDB	If this status is Yes, successfully running Start or Update changes the status to No.
Start	History management is run. This button is active when all of the following conditions are satisfied: The button is grayed-out in all other cases. • The line of the applicable System project has been selected (However, you cannot select multiple lines) • The Status of the selected System project is Stopped	-
Stop	History management is stopped. This button is active when all of the following conditions are satisfied: The button is grayed-out in all other cases. • The line of the applicable System project has been selected (However, you cannot select multiple lines) • The Status of the selected System project is Running	-

Continues on the next page

Table C2.6.1-1 Items displayed on the Revision History Utility (Table continued)

Displayed item	Description	Remarks
Update	An update is run. This button is active when all of the following conditions are satisfied: The button is grayed-out in all other cases. • The line of the applicable System project has been selected (However, you cannot select multiple lines) • The Status of the selected System project is Running	-

C2.6.2 Operations of the Revision History Utility window

1. In AD Organizer, start System Structure Navigator.
2. In the sub menu, select [ProSafe-RS] > [Revision History Utility].
   The Revision History Utility dialog box appears.
3. Perform the following operations according to your purpose.
   - To start history management, select the stopped RS project and click [Start].
   - To stop history management, select the running RS project and click [Stop].
   - To update history management, select the running RS project and click [Update].

   When history management is updated, the differences are resolved and the display of differences changes to No.

C2.6.3 Precautions regarding operation of SCS Manager and Generation Manager

Performing an operation for newly creating, modifying, or deleting a file during processing after clicking Start, Stop, or Update in Revision History Utility returns an error.

For example, performing the operation of such as creating a new SCS project, overwriting and saving with a builder, or modifying properties during processing returns an error.

C2.7 History management using the editors of AD Organizer

The history management function that uses Safety I/O Editor, Safety Communication I/O Editor, and IOM Editor started from AD Organizer consists of the following functions:

Saving of Change Sets

In I/O list engineering that uses AD Organizer, files checked in at the same time are grouped as one set. This grouped set of files is referred to as a Change Set.

With RS original engineering, at the time of download or overwritten saving, builder files subject to such are saved to the RS project. The applicable builder files are also saved to the ADMDB as a Change Set.

A unique number is assigned to each Change Set. This number is referred to as a "Change Set ID". Change Set IDs are automatically assigned by AD Server. You can associate a Change Set with a ModPack.

Setting labels

The user can set a desired string as a label for the latest of the chronologically saved files on AD Server. You can search for files having the same label in the Check-in window.

Displaying the revision history

Saved Change Sets and labels can be displayed in the Revision History Window of AD Organizer.

C2.8 Setting labels

Labels can be attached to a single or multiple files. Labels can be attached at any time to any files subject to the check-in or check-out functions. Set labels in the tree view of System Structure Navigator of AD Organizer.

Labels can be set in either ways: set labels for all folders and files displayed in the tree view at once, or set labels for specific folders and files individually. Set labels can be searched for by using the filtering function or by sorting labels according to each item in the Revision History window.

Setting labels all at once

Follow these steps to set labels all at once:

1. From AD Organizer, display System Structure Navigator.
   You can set labels for folders or files shown in the tree view of System Structure Navigator.
2. In the sub menu of AD Organizer, select [Add Label to all].
   The Label dialog box appears.
3. In the Label dialog box, enter a label name and label comment.
   A label name can contain up to 100 double-byte or single-byte characters, while a label comment can contain up to 1,000 double-byte or single-byte characters.
4. In the Label dialog box, click [OK].
   A label is set for each of the folders and files shown in the tree view of System Structure Navigator.

Setting labels individually

Follow these steps to set labels individually:

1. In the tree view of System Structure Navigator, select the folder or file you wish to set a label to.
2. In the sub menu of AD Organizer, select [Add Label].
   The Label dialog box appears.
3. Enter a label name and label comment.
   A label name can contain up to 100 double-byte or single-byte characters, while a label comment can contain up to 1,000 double-byte or single-byte characters.
4. Click the [OK] button.
   A label is set to the folder or file selected in the tree view of System Structure navigator.

C2.9 Displaying the revision history and labels

You can view the revision history and labels in the Revision History window. You can perform the following tasks in the Revision History window:

- Display a list and the details of Change Sets
- Display a list and the details of labels, modify labels, and delete labels
- Display engineering data associated with Change Sets
- Associate ModPacks with Change Sets
- Compare the details of engineering data

C2.9.1 Displaying the Revision History window

The Revision History window consists of the Revision History tab sheet and Labels tab sheet. In the Revision History tab sheet, you can call up the dialog box for displaying a list and the details of revision history. In the Label tab sheet, you can call up the dialog box for displaying a list view and the detail of labels. You can also change and delete labels. When the Revision History window appears, the Revision History tab sheet also appears by default.

How to display the Revision History window

Follow these steps to display the Revision History window:

1. Start AD Organizer.
2. In the navigator of AD Organizer, select a folder or file and then select [View Revision History] from the right-click menu.

TIP

If you select a folder that is editable with builders in System Structure Navigator, the Revision History dialog box appears. In the Revision History dialog box, you can specify the names of folders and files that are editable with builders. The Revision History window shows the revision history of the folders and files that you specified in this dialog box.

Note that the folder names and file names you specify in the Revision History dialog box are case-sensitive.

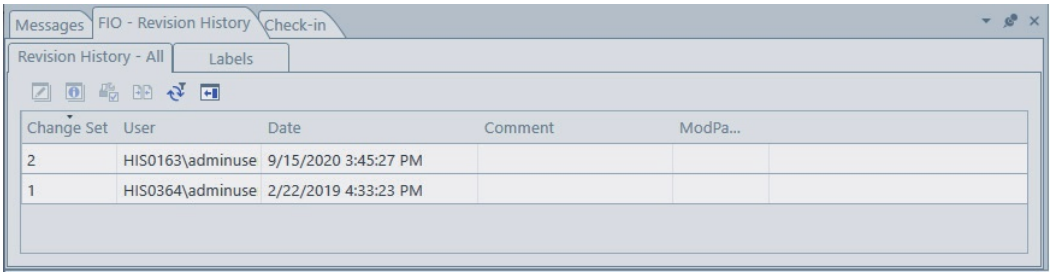


Figure C2.9.1-1 Revision History window (Revision History tab sheet)

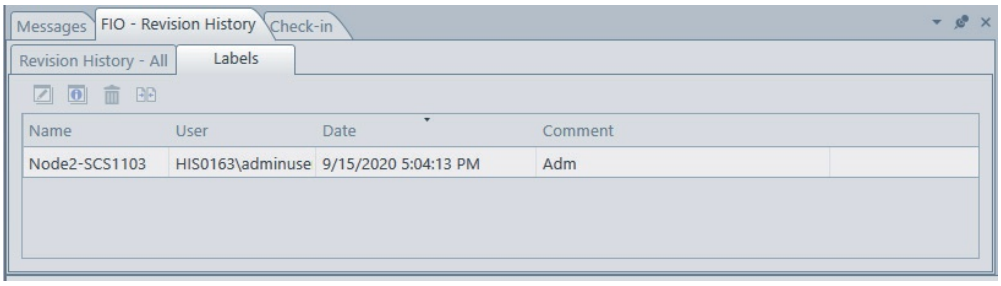


Figure C2.9.1-2 Revision History window (Labels tab sheet)

Filtering Change Sets displayed on the Revision History tab

By default, latest 100 Change Sets are displayed on the Revision History tab. You can filter Change Sets to be displayed on the Revision History tab in the following two ways.

- Filter by ranges of Change Sets
- Filter by dates of Change Sets

Filtering by specifying a range of Change Sets

Follow these steps to specify the range of Change Sets to be displayed on the Revision History tab:

1. On the toolbar, click [Specify Range].
   The Specify Range dialog box appears.

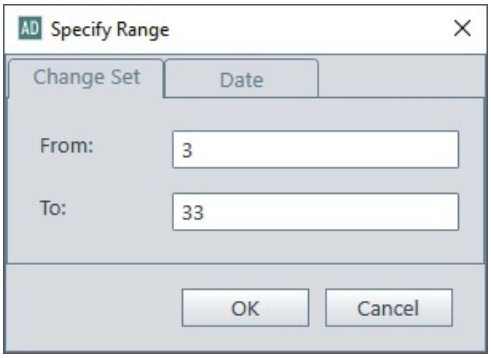


Figure C2.9.1-3 Specify Range dialog box (Change Set tab)

2. Select the [Change Set] tab.

TIP

By default, the Change Set tab is selected.

3. Enter the range of the Change Sets to be displayed, and click [OK].

● Filtering by dates of Change Sets

Follow these steps to specify the date of Change Sets to be displayed on the Revision History tab:

1. On the toolbar, click [Specify Range].
   The Specify Range dialog box appears.
2. Click the [Date] tab.

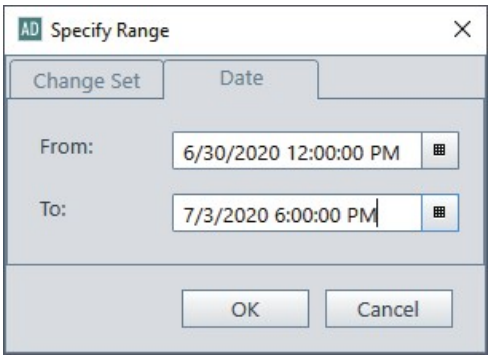


Figure C2.9.1-4 Specify Range dialog box (Date tab)

3. Enter the date range of the Change Sets to be displayed, and click [OK].

■ Items displayed on the Revision History tab sheet

The following table shows the items displayed on the Revision History tab sheet of the Revision History window.

Table C2.9.1-1 Items displayed on the Revision History tab sheet of the Revision History window

Item	Description	Remarks
Change Set	The Change Set ID is displayed.	
User	The name of the user who checked in is displayed.	
Date	The date and time of check-in is displayed.	

Continues on the next page

Table C2.9.1-1 Items displayed on the Revision History tab sheet of the Revision History window (Table continued)

Item	Description	Remarks
Comment	The check-in comment is displayed.	
ModPack ID	The ModPack ID of the ModPack associated with the Change Set is displayed.	Association with ModPack is performed at the time of check-in. You can also perform an association of ModPack to a Change Set in the Revision History window.

Items displayed on the Label tab sheet

The following table shows the items displayed on the Label tab sheet of the Revision History window.

Table C2.9.1-2 Items displayed on the Label tab sheet of the Revision History window

Item	Description
Name	The label name is displayed.
User	The name of the user who set the label is displayed.
Date	The date and time at which the label was set is displayed.
Comment	The label comment is displayed.

C2.9.2 Displaying the detailed information of a change set

You can display the detail information of a Change Set in the Change Set Detail dialog box brought up from the Revision History window.

In the Change Set Detail dialog box, you can display the information of individual files constituting the Change Set and modify the check-in comment.

How to display the detailed information of a change set

Follow these steps to display the detailed information of a Change Set:

1. On the [Revision History] tab sheet of the Revision History window, select the Change Set you want to display the details of.
2. In the Revision History window, click the [Details] button.
   The Change Set Detail dialog box appears.

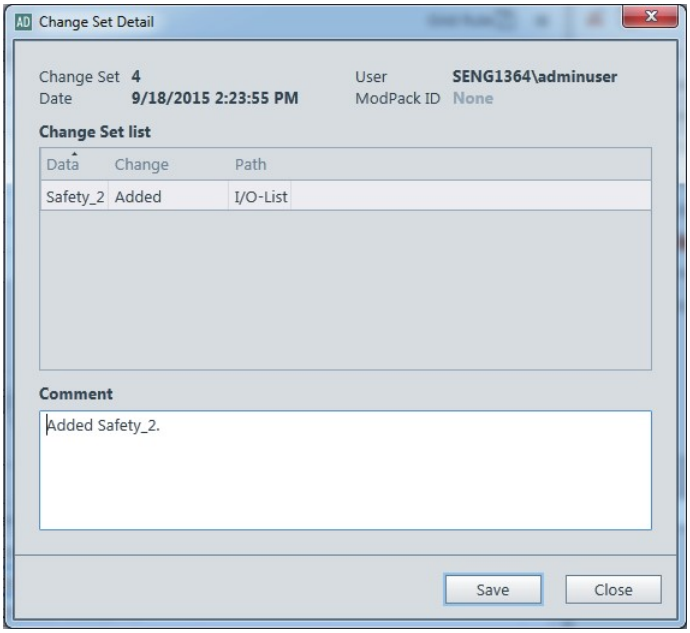


Figure C2.9.2-1 Change Set Detail dialog box

Items displayed in the Change Set Detail dialog box

The following table shows the items displayed in the Change Set Detail dialog box.

Table C2.9.2-1 Items displayed in the Change Set Detail dialog box

Item	Description	Remarks
Change Set	The Change Set ID is displayed.	-
User	The name of the user who checked in is displayed.	-
Date	The date and time of check-in is displayed.	-
ModPack ID	The ModPack ID of the ModPack associated with this Change Set is displayed.	Clicking the ModPack ID opens the ModPack corresponding to the ModPack ID.
Data	The names of individual files constituting the Change Set are displayed.	Selecting a file and selecting [Launch Editor] from the right-click menu starts the editor for editing the file. You can also select [View Revision History] from the right-click menu to display the revision history of the file.

Continues on the next page

Table C2.9.2-1 Items displayed in the Change Set Detail dialog box (Table continued)

Item	Description	Remarks
Change	The type of change is displayed. Added, Modified or Deleted is displayed.	-
Path	The file path is displayed.	-
Comment	The check-in comment is displayed.	You can change the check-in comment. After editing the check-in comment, you can click [Save] to save the edited check-in comment.

C2.9.3 Displaying a list view and detail view of files

You can display the list view of files in the file list pane of the Revision History window. When the Revision History window appears, files under the folder selected in the navigator are listed. You can also filter the list of displayed files.

Displaying the file list pane

Perform this step to display the file list pane in the Revision History window:

- On the toolbar in the Revision History window, click [File List Pane].
  The file history pane appears in the Revision History window.

TIP

- Repeat this operation to show and hide the file list pane.
- The files in the list are displayed in order of check-in date and file path.

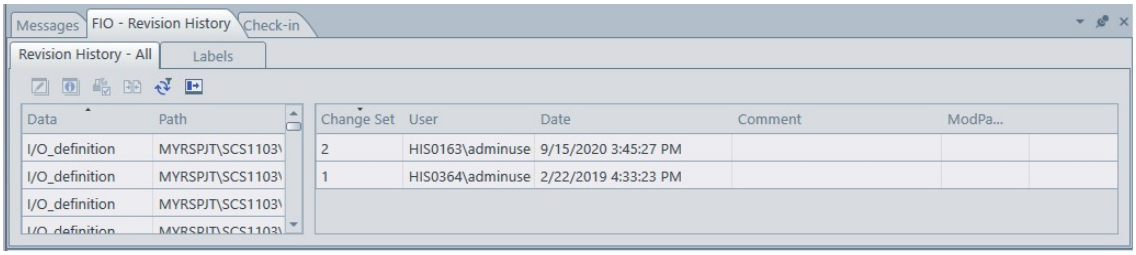


Figure C2.9.3-1 Revision History window showing the file list pane

Filtering Change Sets by selecting a file

You can select a file in the file list pane to display only the Change Sets that include the file. Follow these steps to select a file and filter Change Sets.

- Select a file in the file list pane.
  Only Change Sets that include the selected file are displayed in the Revision History window. If the selected file is not included in any Change Set, no Change Set is displayed.

Clearing a filter that applies to Change Sets

Follow these steps to clear a filter that applies to Change Sets.

- Select the file in the file list pane while holding down the [Ctrl] key.

C2.9.4 Displaying the detailed information of a label

You can display the detailed information of a label in the Label Detail dialog box brought up from the Revision History window.

In the Label Detail dialog box, you can display a list of the files and folders to which the selected label is set and also change the label comment.

How to display the detailed information of a label

Follow these steps to display the detailed information of a label:

1. On the [Labels] tab sheet of the Revision History window, select the label you want to display the details of.
2. In the Revision History window, click the [Details] button.
   The Label Detail dialog box appears.

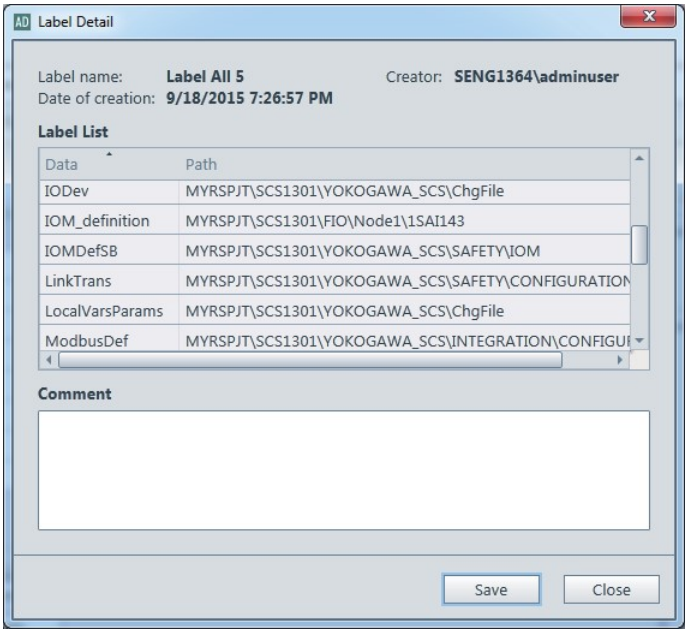


Figure C2.9.4-1 Label Detail dialog box

Items displayed in the Label Detail dialog box

The following table shows the items displayed in the Label Detail dialog box.

Table C2.9.4-1 Items displayed in the Label Detail dialog box

Item	Description	Remarks
Label name	The label name is displayed.	
Creator	The name of the user who set the label is displayed.	
Date of creation	The date and time at which the label was set is displayed.	
Data	The names of the folders and files to which the selected label is set are displayed.	Selecting a file and selecting [Launch Editor] from the right-click menu starts the editor for editing the file. You can also select [View Revision History] from the right-click menu to display the revision history of the file.
Path	The folder or file path is displayed.	

Continues on the next page

Table C2.9.4-1 Items displayed in the Label Detail dialog box (Table continued)

Item	Description	Remarks
Comment	The label comment is displayed.	You can change the label comment. After editing the label comment, click [Save] to save the edited label comment.

C2.9.5 Associating ModPacks with Change Sets

You can associate a ModPack with any of the Change Sets displayed on the [Revision History] tab sheet of the Revision History window.

TIP

The Change Management Package is required in order to use ModPacks.

Follow these steps to associate a ModPack with a Change Set:

1. From amongst the [Revision History] tab sheets in the Revision History window, select the Change Set you wish to associate with a ModPack.
2. In the Revision History window, click the [Assign ModPack] button.
   The Associate ModPack dialog box appears.

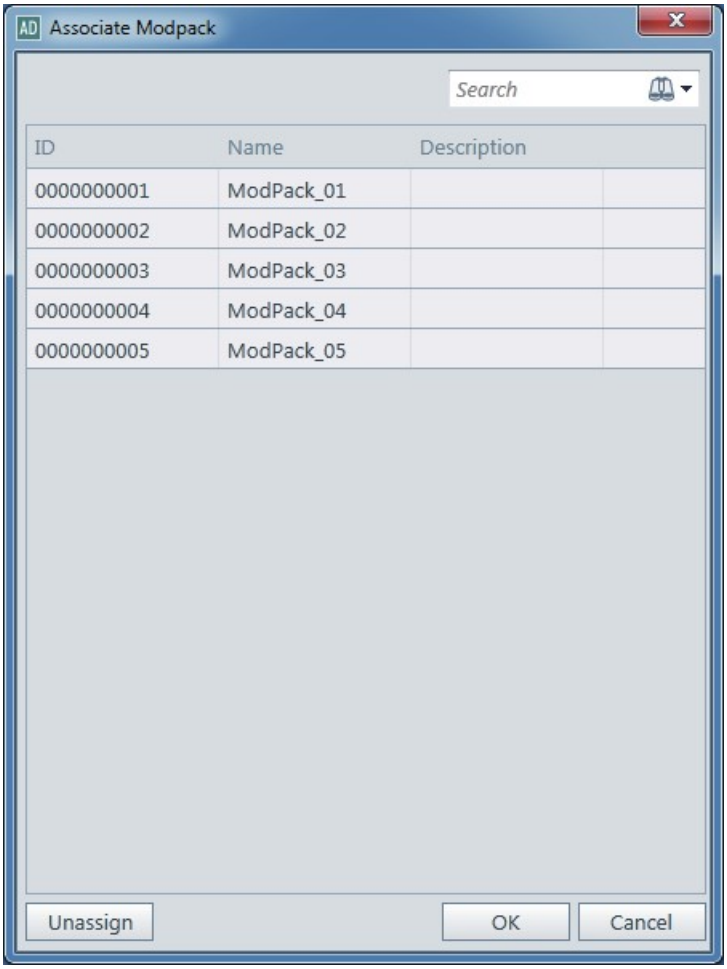


Figure C2.9.5-1 Associate ModPack dialog box

3. In the ModPack list view area, select the ModPack to associate and then click [OK].
   The ModPack ID of the associated ModPack appears on the Revision History tab of the Revision History window.

TIP

- You can only select one ModPack in the Associate ModPack dialog box.
- To cancel association with the ModPack, click [Unassign] button in the Associate ModPack dialog box.

D. ModPack change management

This section describes ModPack-based change management.

Change Management Package is required for ModPack Change management.

D1. Overview of ModPack change management

Your project may be subject to work involving changes during engineering work or at the final stage of engineering.

Using Change Management Package will allow you to use a ModPack to manage various changes applied during engineering work or at the final stage of engineering.

Change management comprises the request for change being registered, the extent of impact due to the change being determined, being able to confirm that changes are only applied in relation to the extent of impact, and finally retaining a history of the changes.

Change management using a ModPack

A package that contains a set of information that is related to a change is called a ModPack.

By managing changes with a ModPack, you can also keep records of the planning, implementation, and testing of the changes. A ModPack contains various information such as an ID for identifying the change, status of the change, users who implement the change, assets to be modified, assets actually modified, and test procedures. You can also attach, to a ModPack, files containing information such as test results.

When a project receives a request for change, you create a ModPack before implementing the change. In the ModPack, you register the information such as the users who implement the change, assets to be modified, and test procedures. The registered engineers implement the change based on this ModPack.

The items registered in a ModPack can be referenced and edited using ModPack Editor.

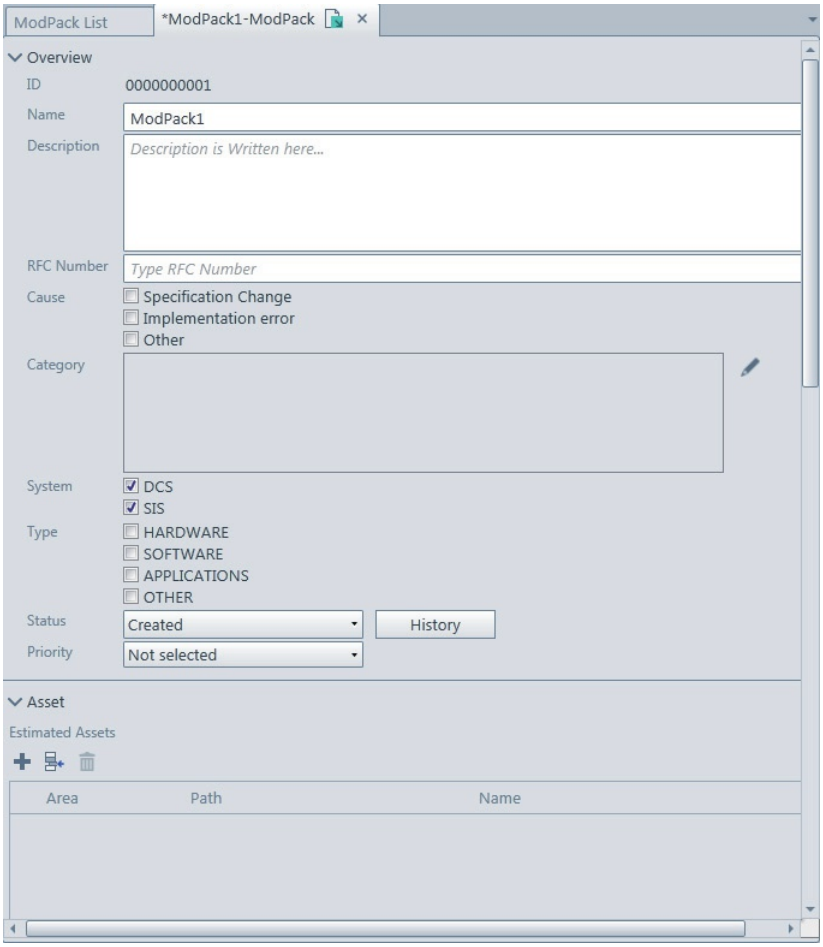


Figure D1-1 Example of ModPack Editor display

TIP

You can also associate a Change Set on iDefine data with a ModPack.

You can associate a Change Set on the iDefine-config file with a ModPack in the Operation History Management window or the Check-in window. You can also associate a Change Set on the selected FB with an instance name with a ModPack in the Operation History Management window.

ModPack access rights

The rights are further broken down for each ModPack operation. The operation rights according to each operation can be assigned.

D1.1 Workflow for handling a change

The following figure shows the workflow for handling a change in engineering using AD Suite.

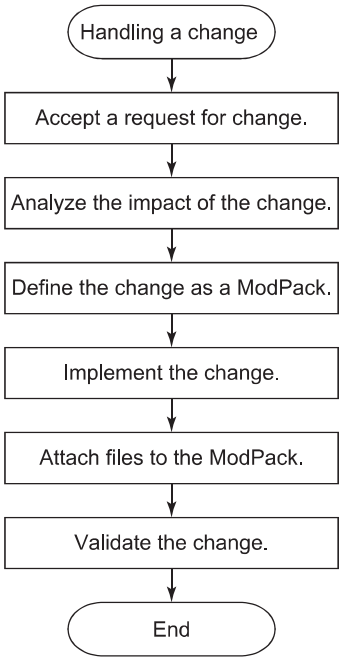


Figure D1.1-1 Workflow for handling a change

Accepting a request for change

Examine the change that is requested. If the request is reasonable, accept the request. The accepted change can be managed with the RFC (Request For Change) number of a ModPack. Enter the RFC number if necessary.

Analyzing the extent of impact by the change

The engineers are to examine the impact due to the change of settings such as tags and ranges in order to investigate the extent of impact. If the request is reasonable, accept the request. The accepted change can be managed with the RFC number of a ModPack.

Defining the change as a ModPack

Create a ModPack and define information about the change, such as the assets to be modified, users who implement the change, and test procedures for the ModPack. Hereafter, proceed with the change process based on this ModPack.

Implementing the change

The user manually performs the change. The implementation of the change can be associated with a ModPack at the time of check-in.

If the subject of the change is a file being changed from a builder of SCS Manager, check-in is automatically performed, without using the Check-in window, at the timing when the changes are saved on the builder. In such case, the ModPack can be associated afterwards with the subject of the change which is displayed in the History window.

After implementing the change, test the modified application.

Attaching files to the ModPack

Files that contain test results or other information can be attached to a ModPack. With these attachments, you can keep records of the test results related to this change.

Validating the change

After the implementation and testing of the change is finished, the user in charge of change management validates the change. If the change is regarded as valid, get an approval from the person who requested the change.

D1.2 Windows that are used in change management

The following three windows or editor are used in change management:

- ModPack Navigator
- ModPack List window
- ModPack Editor

D1.2.1 ModPack Navigator

ModPack Navigator lists ModPacks. ModPack Navigator displays ModPacks based on the role of the logged on user.

Opening ModPack Navigator

- From the AD Organizer, select [View] > [ModPack Navigator].
  ModPack Navigator is displayed.

Window layout of ModPack Navigator

In ModPack Navigator, ModPacks are listed for each status.

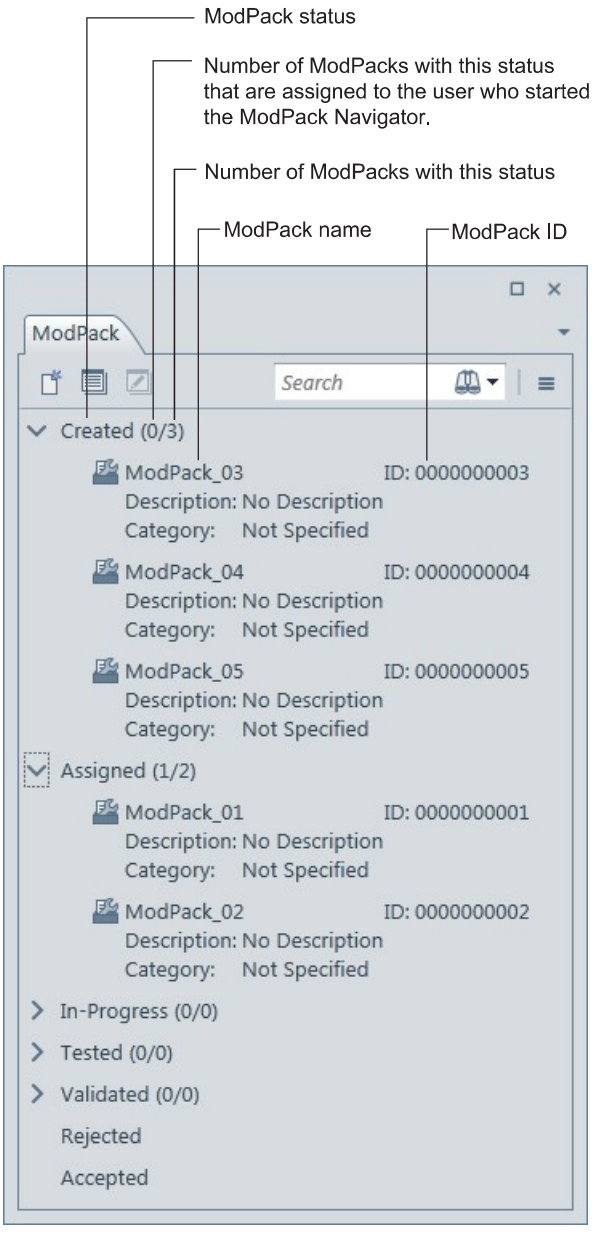


Figure D1.2.1-1 Window layout of ModPack Navigator

ModPack status

The following figure shows the ModPack status. ModPack Navigator categorizes ModPacks into these statuses and lists them.

Table D1.2.1-1 ModPack status

Status	Description
Created	The initial status of newly created ModPacks. ModPacks are automatically placed in this status when created.
Assigned	Indicates that the users who implement the change are already assigned to the ModPack. Multiple users can be assigned to a ModPack. The user who manages ModPacks sets this status manually.
In-Progress	Indicates that the change is being implemented. The user who implements the change of this ModPack sets this status manually.
Tested	Indicates that the testing of the modified assets is finished. The user who implements the change of this ModPack sets this status manually.
Validated	Indicates that the change was validated by the user who manages ModPacks. The user who manages ModPacks checks the validity of the change and, if there is no problem, sets this status manually.
Rejected (*1)	Indicates that the change was not implemented for certain reason. The user who manages ModPacks sets this status manually.
Accepted (*1)	Indicates that the change was accepted by the person who requested the change. After the change is accepted, the user who manages ModPacks sets this status manually.

*1: The ModPack statuses Accepted and Rejected are used in pair. ModPacks whose status is set to Accepted or Rejected no longer appear in ModPack Navigator. However, they still appear in the ModPack List window.

D1.2.2 ModPack List window

The ModPack List window displays the ModPacks that are listed in ModPack Navigator in a table format. You can open the ModPack List window from ModPack Navigator.

TIP

You cannot display two or more ModPack List windows at a time. If you try to open another ModPack List window while a ModPack List window is displayed, the currently displayed ModPack List window closes and a new ModPack List window opens.

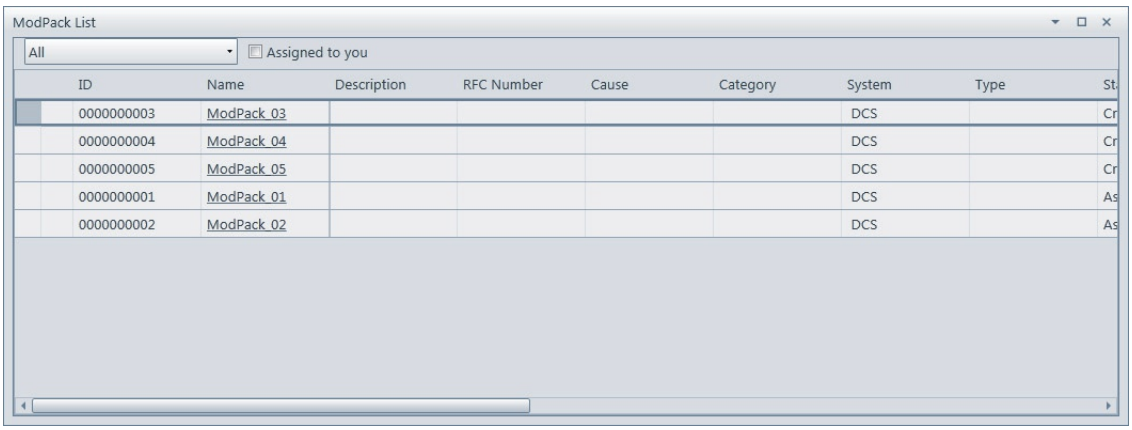


Figure D1.2.2-1 Example of ModPack List window display

Opening a ModPack List window

- To open a ModPack List window, double-click a ModPack status in ModPack Navigator. A ModPack List window opens, showing only the ModPacks with the status that you double-clicked.

D1.2.3 ModPack Editor

Use ModPack Editor when editing a ModPack. You can start ModPack Editor from ModPack Navigator or a ModPack List window.

Starting ModPack Editor

- Perform either of the following operations to start ModPack Editor:
  - In ModPack Navigator, double-click the ModPack.
  - In the ModPack List window, click a ModPack name.

Window layout of ModPack Editor

ModPack Editor consists of the following areas:

- Overview area
- Asset area
- Assignment area
- Implementation area
- Test area
- Attachment file area

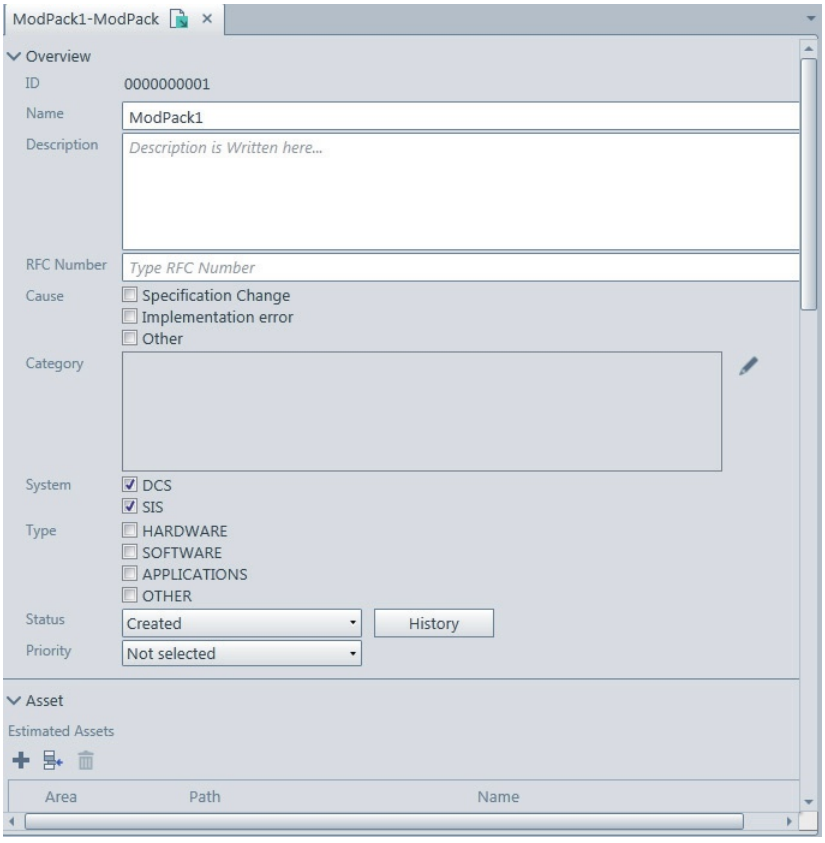


Figure D1.2.3-1 Example of ModPack Editor display

Overview area

The Overview area displays the basic information of the ModPack, such as the ID, RFC number, and status.

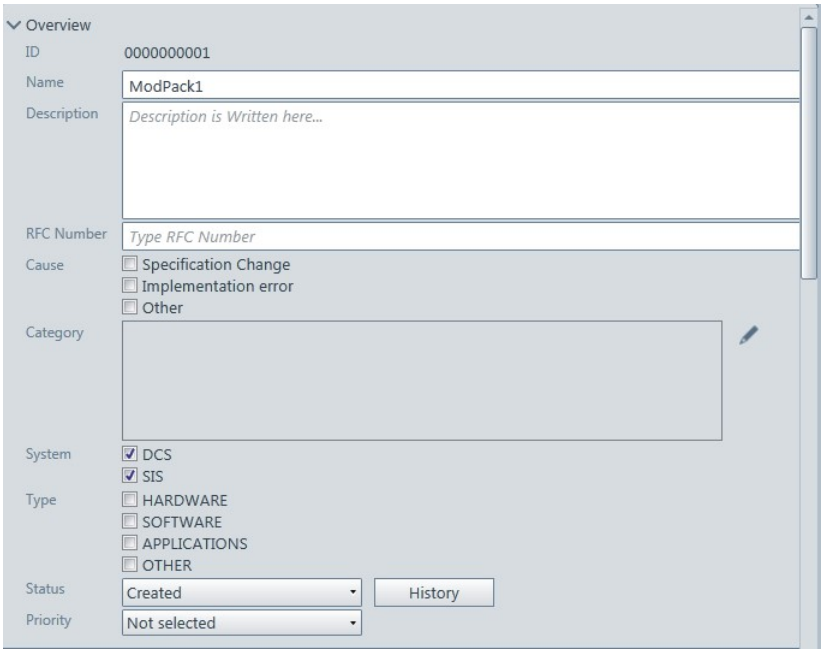


Figure D1.2.3-2 Overview area

The following table describes the items that are displayed in the Overview area.

Table D1.2.3-1 Items displayed in the Overview area

Item	Description
ID	The number that identifies the ModPack. An ID is automatically assigned by the system when the ModPack is created. Users cannot edit IDs.
Name	The name of the ModPack. Only the users with the ModPack Creation or ModPack Reopen right can enter this item. Duplicate names are allowed. Entry of Name is mandatory. The name that is entered here also appears in the Check-in window. Up to 50 characters can be entered for the name.
Description	A summary of the ModPack. The description entered here also appears in the Check-in window. Up to 1000 characters can be entered for the description.
RFC Number	The number for managing change requests. Only the users with the ModPack Creation or ModPack Reopen right can enter this item. Up to 50 characters can be entered for the RFC number.
Cause	Select the cause of change with check boxes. Multiple items can be selected. The following three choices are provided for Cause: • Specification Change • Implementation error • Others

Continues on the next page

Table D1.2.3-1 Items displayed in the Overview area (Table continued)

Item	Description
Category	The type and category of the change. Select the category in the Category dialog box. Multiple items can be selected. Only the users with the ModPack Creation or ModPack Reopen right can edit this item. The following choices are provided in the Category dialog box: • Instrument range • Parameters (set point, control, and so on) • Tag property (description, alarm priority, other attributes) • Control design information, graphics, subsystem communication I/F, and software I/O (PLC package) • Cable schedules, Junction box, and so on • P&ID • Safety logic • Tag addition/deletion • Document modification • Hardware version update/replacement • Software version update/replacement • System migration
System	The system that is to be changed. Use the check boxes to select the following subjects. • DCS • SIS
Type	The type of the change. Use the check boxes to select one or more of the following modifications. • Hardware • Software • Application • Others
Status	The status of the ModPack. Select a status from the drop-down list. Clicking the [History] button displays the status change history.
Priority	The priority of the change. Select the following priority level from the drop-down list. • Critical • High • Medium • Low

Asset area

The Asset area consists of an Estimated Assets list that displays the subjects of the change in the stage of estimates and an Actual Assets list that displays the subjects that have actually been changed. In the Estimated Assets list, users can register and view the assets that are candidates for modification. In the Actual Assets list, users can register and view the assets that were actually modified.

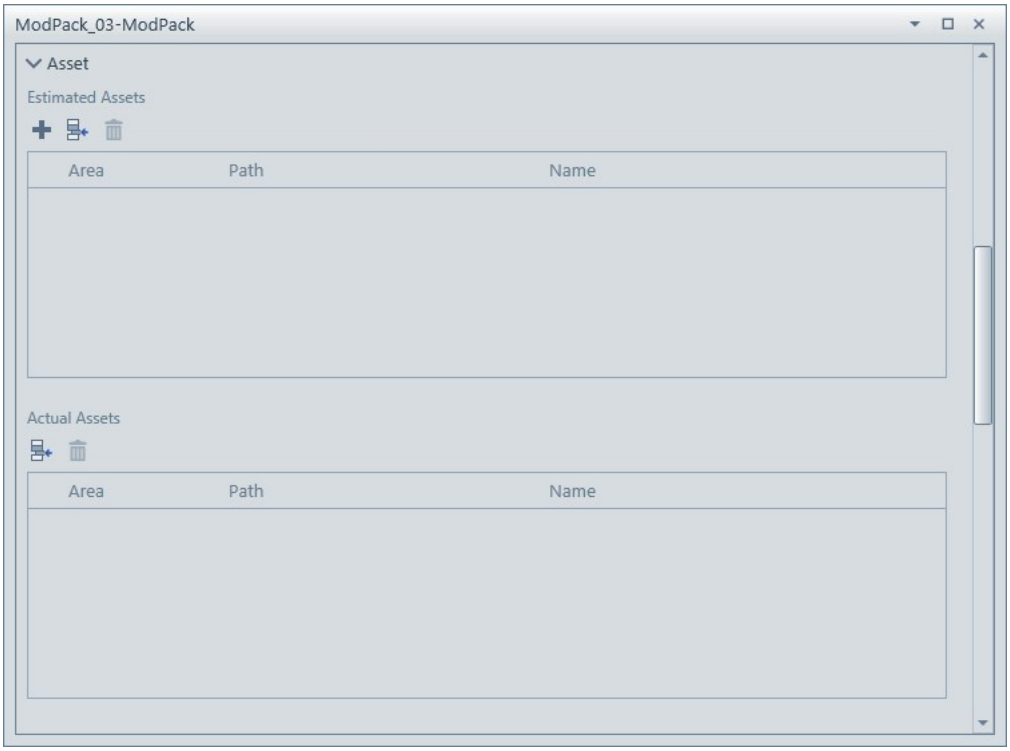


Figure D1.2.3-3 Asset area

Estimated Assets

The Estimated Assets list is where the user registers the assets to be modified. The following table describes the items that are displayed in the Estimated Assets list. Up to 1000 objects can be selected for modification.

Table D1.2.3-2 Items displayed in the Estimated Assets list

Item	Description
Area	The area of the assets to be modified. The user can select from the following four areas in the list: • Library • Application Structure • System configuration • Document The user can also type in an area with the keyboard. Up to 20 characters can be entered for the area.
Path	The path to the object to be modified. If the user selects an area, the paths to the objects, which are displayed in the relevant navigators, appear in the list. If the user typed in the area, the user must type in the paths as well. Up to 100 characters can be entered for the path.
Name	The name of the object to be modified. The names of the selected objects are automatically entered. If the user typed in the area, the user must type in the names as well. Up to 100 characters can be entered for the name.

Actual Assets

The Actual Assets list is where users can view the objects that were actually modified. When the user checks in a modification-completed object, specifying association with the ModPack, the object appears in the Actual Assets list. Manual entry of data is also possible in the Actual Assets list.

TIP

- Objects that are not registered as Estimated Assets can also be displayed in the Actual Assets list if they are associated with the ModPack when they are checked in.
- Paths in the Actual Assets list are displayed in a format that is different from the paths in the Estimated Assets list. The paths in the Actual Assets list are the same as those appear in the Check-in window.

Assignment area

The Assignment area is where the users or groups who modify the estimated assets are assigned. Names of the users or groups that are assigned to the ModPack are listed. Up to 100 users and user groups in total can be assigned to one ModPack.

When a users or a user who belongs to a group that was assigned here starts ModPack Navigator, only the ModPacks that are assigned to the user are displayed. However, if a user with the ModPack Management right starts ModPack Navigator, all ModPacks are displayed.

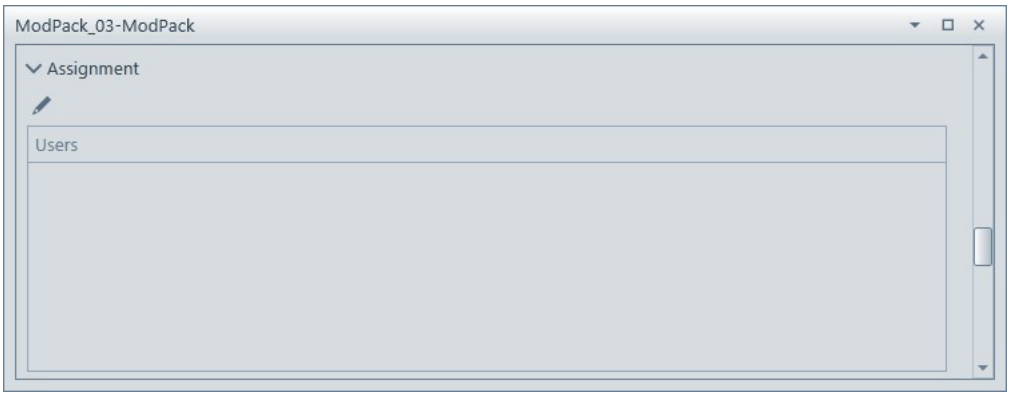


Figure D1.2.3-4 Assignment area

SEE ALSO For more information about how to assign the users who implement the change, refer to:

D2.4, “Assigning the users who implement the change” on page D2-6

Implementation area

The Implementation area is where descriptions related to implementation of the change, such as procedures for implementing the change, are entered. Up to 65536 characters can be entered.

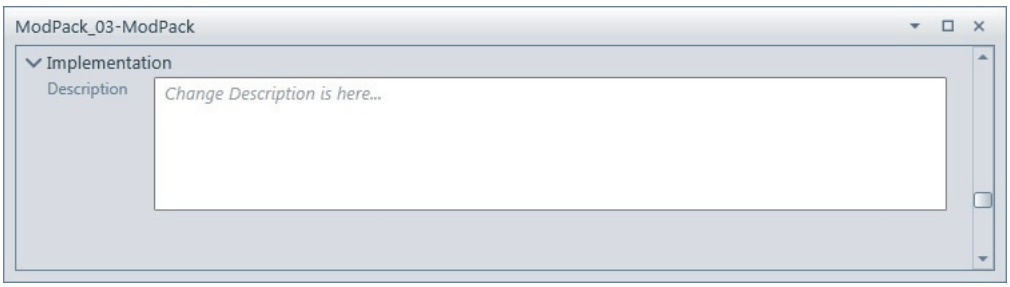


Figure D1.2.3-5 Implementation area

Test area

The Test area is where descriptions such as test procedures are entered. Up to 65536 characters can be entered.

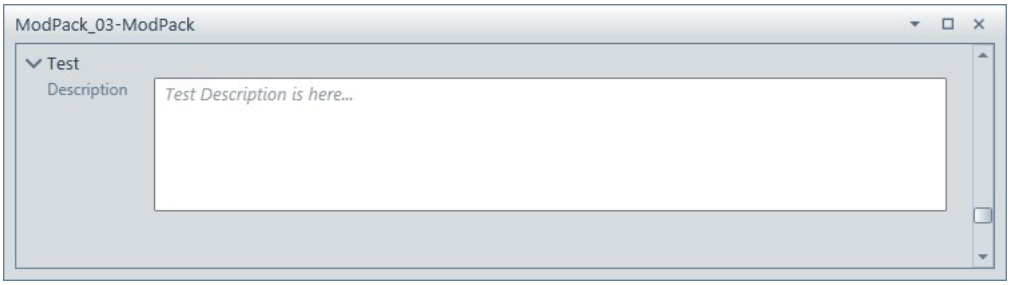


Figure D1.2.3-6 Test area

Attachment file area

The Attachment file area is where the user can attach files containing, for example, test results to the ModPack.

- File format of attachments
  Any file format is allowed.
- Maximum number of attachments
  100 files per ModPack
- Maximum size of an attachment
  100 MB
- Total size of all attachments
  100 MB per ModPack

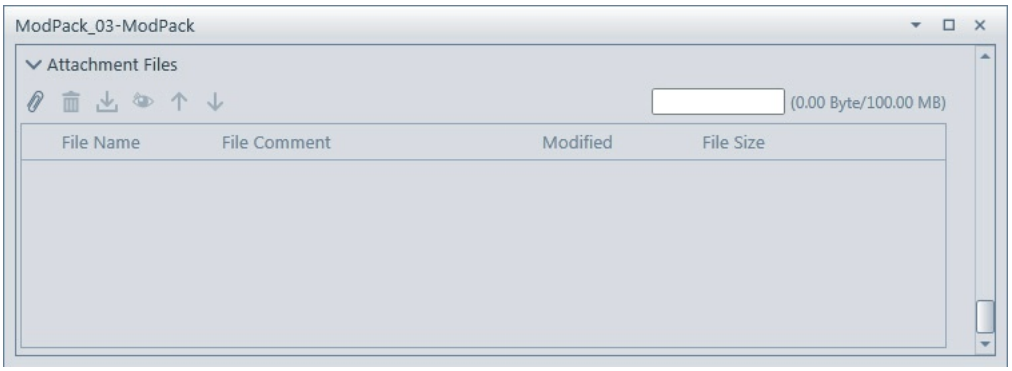


Figure D1.2.3-7 Attachment file area

SEE ALSO For more information about how to attach files in the Attachment file area, refer to:

D2.7, “Attaching files” on page D2-11

D1.3 Access control on ModPack operation

To be able to perform various operations in ModPack Editor, users must have the right to do the operation. It is possible to assign the rights appropriately to the users who work with ModPack Editor. In ModPack Editor, users are allowed to perform operations according to the right that is assigned to the users.

TIP

If ModPack Editor is run by a user who has no rights, ModPack Editor opens in read-only mode.

Relationship between ModPack Editor operations and access rights

ModPack Editor operations are functionally categorized. To perform a certain operation, the user must have the right to perform the operation.

ModPack operation categories

ModPack operations are categorized as follows:

- Create ModPacks
- Change ModPack status to Accepted or Rejected
- Change ModPack status from Accepted or Rejected to another status
- View all ModPacks in ModPack Navigator
- Enter Name, RFC Number, Category, and user assignments in ModPack Editor
- Register actual assets in ModPack Editor
- Enter items other than Name, RFC Number, Category, and user assignments in ModPack Editor
- Associate changes implemented in the past with a ModPack in the Revision History window.

ModPack access rights

ModPack access rights are as follows:

- ModPack Creation
- ModPack Closing
- ModPack Reopen
- ModPack Management
- ModPack Implementation
- Revision History Re-assign ModPack

ModPack access rights and permitted operations

The following table shows the ModPack access rights and the corresponding permitted operations.

Table D1.3-1 Correspondence between ModPack access rights and permitted operations

Access right	Category of operation (*1)							
	Create ModPacks	Change ModPack status to Accepted or Rejected	Change ModPack status from Accepted or Rejected to another status	Enter Name, RFC Number, Category, and user assignments in ModPack Editor	Register actual assets in ModPack Editor	Enter items other than Name, RFC Number, Category, and user assignments in ModPack Editor	Associate changes implemented in the past with ModPacks in the Revision History window	Remarks
ModPack Creation	Yes	-	-	Yes	Yes	Yes	-	
ModPack Closing	-	Yes	-	-	Yes	Yes	-	
ModPack Reopen	-	-	Yes	Yes	Yes	Yes	-	
ModPack Management	-	-	-	-	-	-	-	(*2)
ModPack Implementation	-	-	-	-	Yes	Yes	-	(*2)
Revision History Re-assign ModPack	-	-	-	-	Yes	-	Yes	

*1: Yes: The operation can be performed by a user with this right or this right is required to perform the operation.
- : The operation cannot be performed by a user with this right.

*2: Users who have the ModPack Implementation right but do not have the ModPack Management right can view only the ModPacks that are assigned to them. To enable a user to view all ModPacks, you must grant the user the ModPack Management right as well.

Assigning access rights

Access rights to ModPacks can be assigned to users or user groups. Access rights to ModPacks are assigned by using ADS Administration Tool.

SEE ALSO For more information about how to assign access rights, refer to:

C1.2.2, “Controlling access to AD projects” on page C1-30

D2. Operating ModPack change management

Before starting implementation of a change, the user in charge of change management creates a new ModPack. For the ModPack created, the user configures the basic information and assets to be modified and assigns the users who implement the change. The users who implement the change then proceed with the change process based on the ModPack.

D2.1 Creating ModPacks

ModPack creation is a task that should be done by the user in charge of change management. To be able to create ModPacks, the user must have the ModPack Create right. The status of a newly created ModPack is automatically set to Created.

Creating a ModPack

Follow these steps to create a ModPack:

1. Open ModPack Navigator.
2. In ModPack Navigator, click the [New ModPack] button.
   A new ModPack is created in the Created folder.
3. Enter the name of the ModPack.

D2.2 Configuring the basic information

Each ModPack has the following basic information items. The user configures these basic information items of the ModPack that is created.

- Description
- RFC Number
- Cause
- Category
- System
- Type
- Status
- Priority

Configuring basic information items

You need to open the ModPack before you can configure the basic information. Follow these steps to configure the basic information:

1. In ModPack Navigator, double-click the ModPack to open it.
   ModPack Editor starts.

TIP

If the ModPack List window is open, you can also start ModPack Editor by clicking the ModPack name in the ModPack List window.

2. Click the [Check-out] button in AD Organizer to check out the ModPack that you opened.
3. In ModPack Editor, enter the basic information items.

TIP

- You can specify Category in the Category dialog box that is opened by clicking the [Add Category] button.
- Change the status as necessary.

4. Click the [Save] button in AD Organizer.
   The ModPack is saved.
5. Check in the ModPack in the Check-in window.

D2.3 Registering the assets to be modified

The user registers the assets to be modified in the Asset area of ModPack Editor.

Registering the assets to be modified

Assets to be registered can be selected in the Estimated Asset dialog box. However, for assets that cannot be selected in the Estimated Asset dialog box, such as hardware objects, the user must enter them manually in the Estimated Assets list of the Asset area.

Selecting the assets to be modified in the Estimated Asset dialog box

Follow these steps to register the assets to be modified in the Estimated Asset dialog box:

1. Open the ModPack in which you register assets to be modified.
   ModPack Editor starts.
2. Click the [Check-out] button in AD Organizer to check out the ModPack that you opened.
3. In the Asset area, click the [Add Estimated Asset] button in the Estimated Assets list.
   The Estimated Asset dialog box appears.

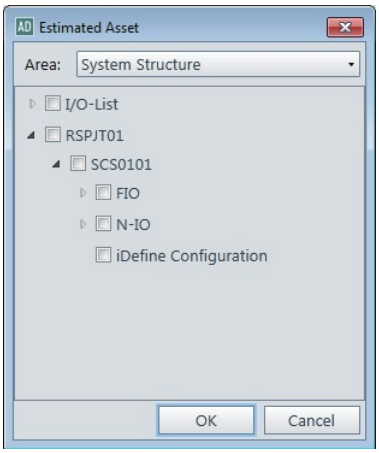


Figure D2.3-1 Estimated Asset dialog box

4. From the [Area:] list box in the Estimated Asset dialog box, select the area for modification.
   Items are hierarchically displayed based on the area that you have selected. You can select from among the following areas:
   - Library
   - Application Structure
   - System configuration
   - Document
5. Select the check boxes of the items that you want to register for modification.
6. Click [OK] in the Estimated Asset dialog box.
   The selected items are displayed in the Estimated Assets list in the Asset area of ModPack Editor.
7. Click the [Save] button in AD Organizer.
   The ModPack is saved.
8. Check in the ModPack in the Check-in window.

Entering the assets to be modified manually

Follow these steps to register the assets to be modified by manual entry:

1. Open the ModPack in which you register assets to be modified.
   ModPack Editor starts.
2. Click the [Check-out] button in AD Organizer to check out the ModPack that you opened.
3. In the Asset area, click the [Add Assets Manually] button in the Estimated Assets list.
   A new row is added to the Estimated Assets list in the Asset area.
4. In each cell in the row that you have added, enter information about the modified asset.
5. Click the [Save] button in AD Organizer.
   The ModPack is saved.
6. Check in the ModPack in the Check-in window.

SEE ALSO For more information about check-in operation, refer to:

"■ Checking in manually" on page B4-9

D2.4 Assigning the users who implement the change

The users who will implement the change are assigned in the Assignment area of ModPack Editor. Once a user is assigned, the ModPack status is set to Assigned.

Follow these steps to assign the users who implement the change:

1. Open the ModPack to which you assign users.
   ModPack Editor starts.
2. Click the [Check-out] button in AD Organizer to check out the ModPack that you opened.
3. In the Assignment area, click the [Assign Engineer] button.
   The Assign Member(s) dialog box appears.

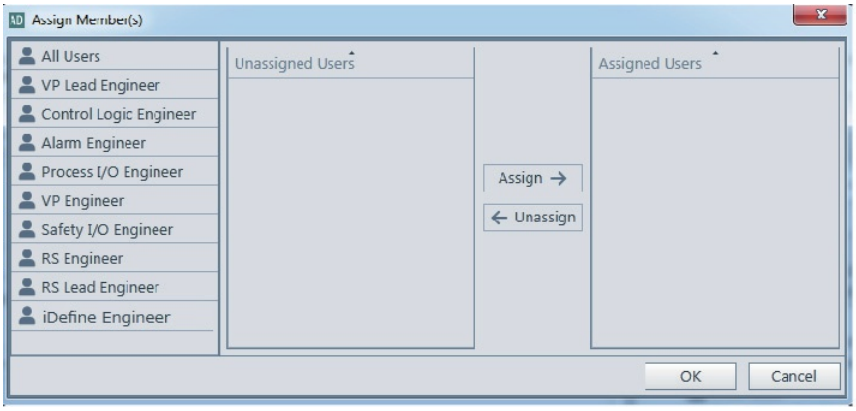


Figure D2.4-1 Assign Member(s) dialog box

4. In the Assign Member(s) dialog box, select a user role.
   The users who have been assigned with the role are listed.
5. Select users in the Unassigned Users section and click the [Assign] button.
   The selected users are added to the Assigned Users section.
6. If you need to delete users that are already assigned, select the users in the Assigned Users section and click the [Unassign] button.
   The users that you have deleted move to the Unassigned Users section.
7. Click the [OK] button in the Assign Member(s) dialog box.
   The users that you have assigned appear in the Assignment area of ModPack Editor.
8. Click the [Save] button in AD Organizer.
   The ModPack is saved.
9. Check in the ModPack in the Check-in window.

SEE ALSO For more information about check-in operation, refer to:

"■ Checking in manually" on page B4-9

D2.5 Implementing the change

The user who implements the change starts the implementation by changing the ModPack status to In-Progress.

The users who implement the change modify the estimated assets by using their respective editors. When all required modification is finished, the actually modified assets should be associated with the ModPack. Modifications can be divided into the following three types:

- Procedure for modification of objects that are handled by AD Organizer
- Procedure for modification by SCS Manager builders
- Other modifications (Example: change in hardware)

Procedure for modification of objects that are handled by AD Organizer

In the modification process for objects that are handled by AD Organizer, you specify a ModPack to be associated when you check in the object after modification. You do not need to specify a ModPack that is not to be associated

Follow these steps to modify an object that is handled by AD Organizer:

1. Start the editor for editing the object and modify the object.
2. In the Check-in window, select the check boxes of the files that have been modified and click the [ModPack Relation] button.
   The list of ModPacks that are assigned to the logged on user appears in the Check-in window.

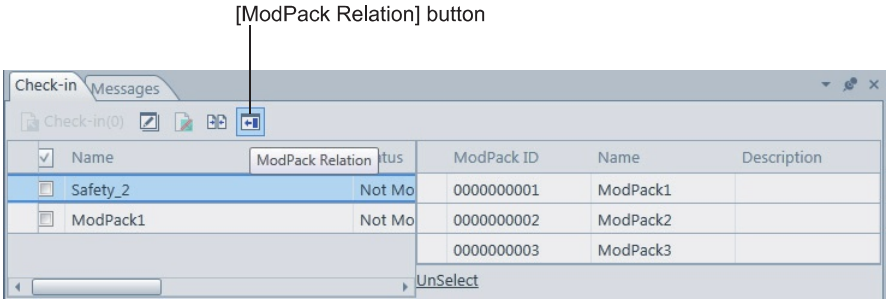


Figure D2.5-1 Check-in window

3. From the ModPack list, select the ModPack to be associated.
4. Click the [Check-in] button on the toolbar.
   The Check-in dialog box appears and the associated ModPack appears in the center of the dialog box.
5. In the Check-in dialog box, click [Check-in] button.
   Once associated with a ModPack, the modification is displayed in the Asset area of ModPack Editor as an actual asset.

Procedure for modification by SCS Manager builders

Follow these steps to associate a change that uses SCS Manager builders with a ModPack:

1. From SCS Manager, start the builder for the asset and modify the asset.
2. After you finish the modification, save or download the asset.
   The modified asset is stored in the Automation Design Master Database (ADMDB).
3. Open the Revision History window.

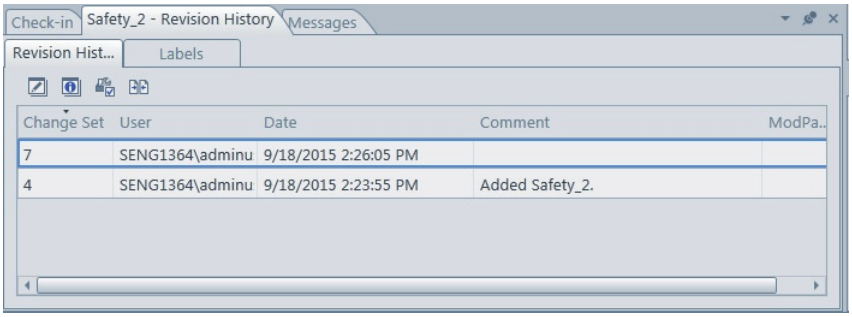


Figure D2.5-2 Revision History window

4. In the Revision History window, click the [ModPack Relation] button.
   The Associate ModPack dialog box appears.

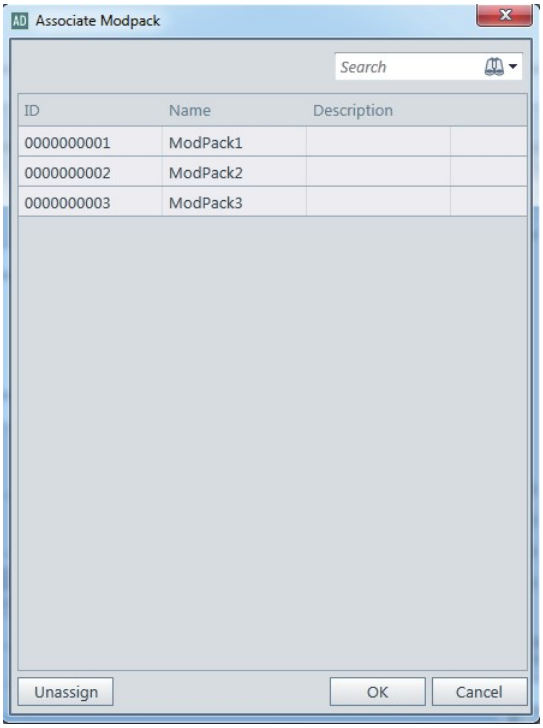


Figure D2.5-3 Associate ModPack dialog box

5. Select the ModPack to be associated and click [OK].
   Once associated with a ModPack, the modification is displayed in the Asset area as an actual asset.

TIP

- You can only select one ModPack in the Associate ModPack dialog box.
- To cancel association with the ModPack, click [Unassign] in the Associate ModPack dialog box.

Procedure for other modifications

Other modification here refers to modification of assets that were entered manually in the Estimated Assets list at the stage of estimating the change. For example, change in hardware falls in this category.

Because other modifications are out of the scope of management by AD Organizer, association with ModPacks must be manually implemented by a user. Follow these steps to associate other changes with a ModPack:

1. Open the ModPack to be associated with the modification.
   ModPack Editor starts.

2. Click the [Check-out] button in AD Organizer to check out the ModPack that you opened.
3. In the Asset area, click the [Add Actual Asset] button in the Actual Assets list.
   A new row is added to the Actual Assets list in the Asset area.
4. In each cell in the row that you have added, enter information about the modified asset.
5. Click the [Save] button in AD Organizer.
   The ModPack is saved.
6. Check in the ModPack in the Check-in window.

SEE ALSO For more information about check-in operation, refer to:

"■ Checking in manually" on page B4-9

D2.6 Testing the modified application

The users test the modified application according to the procedures written in the Test area of ModPack Editor to verify, for example, that the modified software works correctly. After the testing is finished, the user changes the ModPack status to Tested.

You can test the operation of ProSafe-RS application by using the test function.

SEE ALSO For more information about the test function, refer to:

1., “Overview of the test function” in Test Function Guide (IM 32P04B30-01EN)

D2.7 Attaching files

Files that contain test results or other information can be attached to a ModPack. Attached files are listed in the Attachment file area of ModPack Editor.

■ Attaching files

Follow these steps to attach files to a ModPack:

1. Open the ModPack to which you attach files.
   ModPack Editor starts.
2. Click the [Check-out] button in AD Organizer to check out the ModPack that you opened.
3. In the Attachment file area of ModPack Editor, click the [Add] button.
   The Choose a file dialog box appears.
4. In the Choose a file dialog box, specify the file to be attached and click [OK].
   The file that you have specified appears in the Attachment file area of ModPack Editor.
5. Click the [Save] button in AD Organizer.
   The ModPack is saved.
6. Check in the ModPack in the Check-in window.

SEE ALSO For more information about check-in operation, refer to:

"■ Checking in manually" on page B4-9

■ Handling attached files

Users can delete, save in a local computer, or sort or view files that are attached to a ModPack.

- In ModPack Editor, select the Attachment file you wish to operate and click the [Delete] button, [Save] button, [Move up] button, [Move down] button, or [View] button.

D2.8 Validating the change

After the implementation and testing of the change is finished, the user in charge of change management validates the change. After validating the change, the user changes the ModPack status to Validated. Finally, get an approval from the person who requested the change and change the ModPack status to Accepted.

■ Changing the ModPack status

Follow these steps to change the ModPack status:

1. Open the ModPack that you change the status.
   ModPack Editor starts.
2. Click the [Check-out] button in AD Organizer to check out the ModPack that you opened.
3. In the Overview area of ModPack Editor, select the status from the [Status] list.
4. Click the [Save] button in AD Organizer.
   The ModPack is saved.
5. Check in the ModPack in the Check-in window.

SEE ALSO For more information about check-in operation, refer to:

"■ Checking in manually" on page B4-9

E. Access Control/Operation History Management functions

This section describes the Access Control / Operation History Management functions.

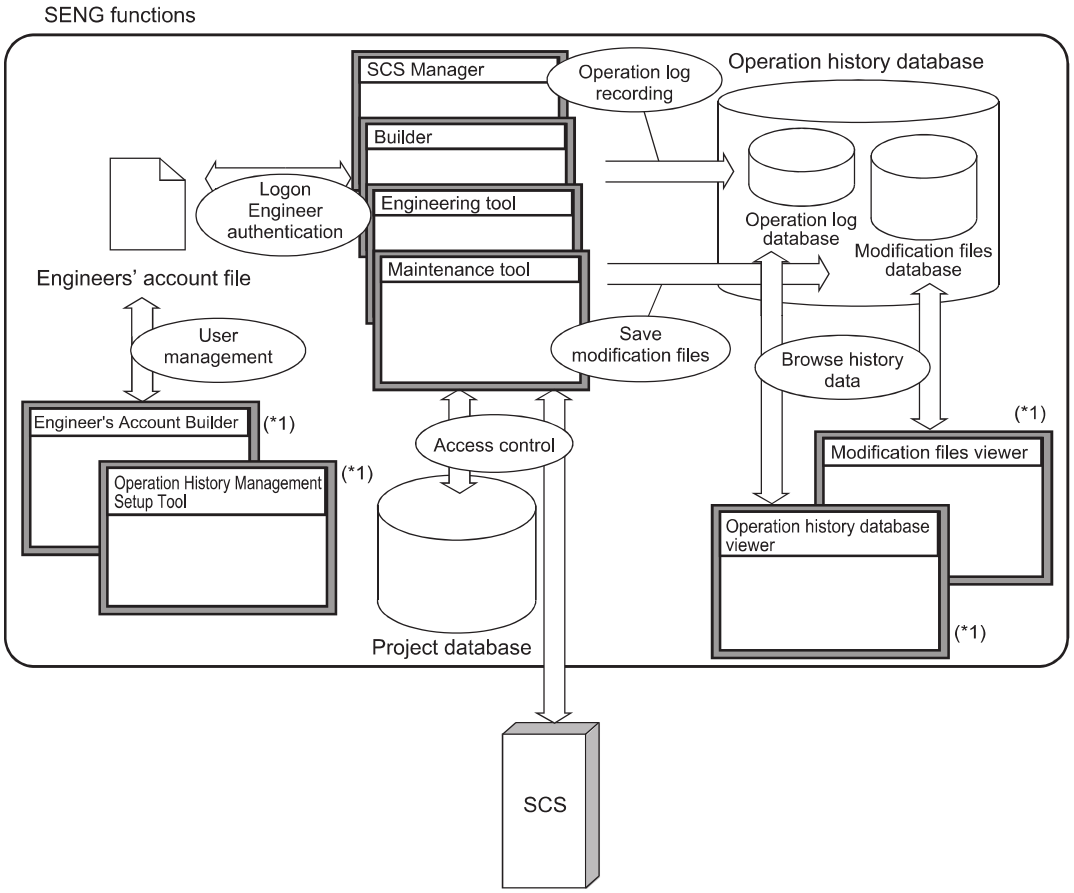
The Access Control/Operation History Management functions provide user-based restrictions to functions of the SENG software and to record or view the operation history of operations in the SENG software.

The Access Control / Operation History Management functions are made up of the following functions.

- User management
  Manage users (referred to as "engineers" in the following sections) working with SCS Manager and SCS Maintenance Support Tool.
- Logon / Engineer Authentication
  Logon is a function that prompts the engineer to enter an engineer name and password when starting a SENG function. Engineer Authentication is a function that prompts the engineer to enter a password when executing a specific operation after Logon. The user can select the configuration whether or not to perform Engineer Authentication.
- Access Control
  A function for specifying whether individual engineers have the authority to perform an operation and to control whether or not the operation is available to perform based on that specification.
- Record Operation History
  A function for recording operation information in the form of a history when an engineer has performed that operation.
- View Operation History
  A function for displaying and printing operation histories stored in the History Management Database in order to view them.

E1. Configuration

The following figure shows the overall configuration of the Access Control / Operation History Management functions.



*1: These tools are included in the RS4E5170 Access Control and Operation History Management Package.

Figure E1-1 Overall configuration of the Access Control/Operation History Management functions

Operating environment

- Hardware
  It is recommended that the hard disk of the PC on which the History Management Database is located has at least 100 GB of free space. It is recommended that you provide an auxiliary memory device to back up the History Management Database.

TIP

The size of the History Management Database will increase by up to around 10 MB during a single download. 100 GB of free space therefore equates to 10000 downloads (1000 downloads per SCS if you have 10 SCSs.)

- Software
  In addition to Safety System Engineering and Maintenance Function, the following package is required on the SENG where you apply the access control and operation history management functions:

  RS4E5170 Access Control and Operation History Management Package

  The package is not required on PCs that are only for registering the History Management Database.

If the number of connections to the PC on which the History Management Database is installed is five or more, use a server OS on this PC.

System configuration

The following figure shows an example of a system configuration using the Access Control / Operation History Management functions.

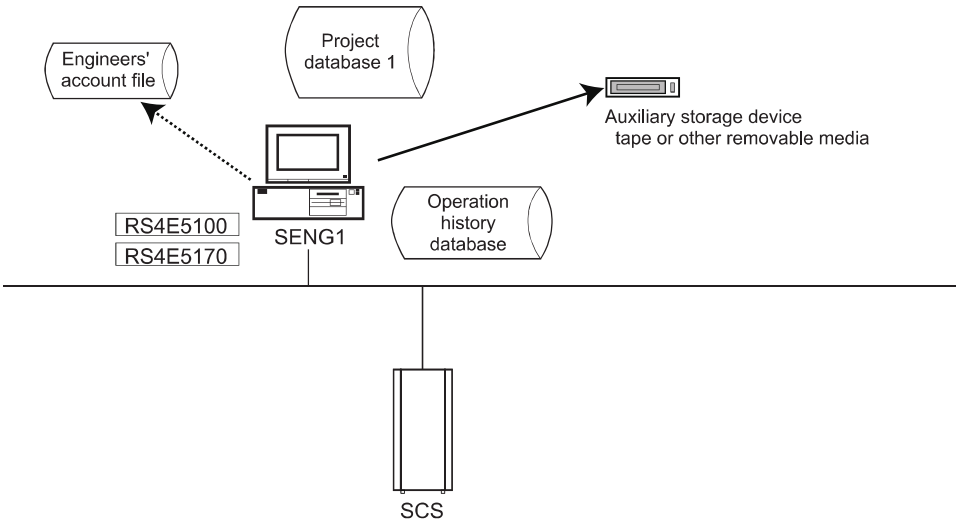


Figure E1-2 Example of a minimum configuration

The following figure shows an example in which the functions are deployed on multiple SENGs. The History Management database is located on a dedicated PC. The engineer registration information is also located on the dedicated History Management PC so that it is referenced commonly by multiple SENGs, and set as shared.

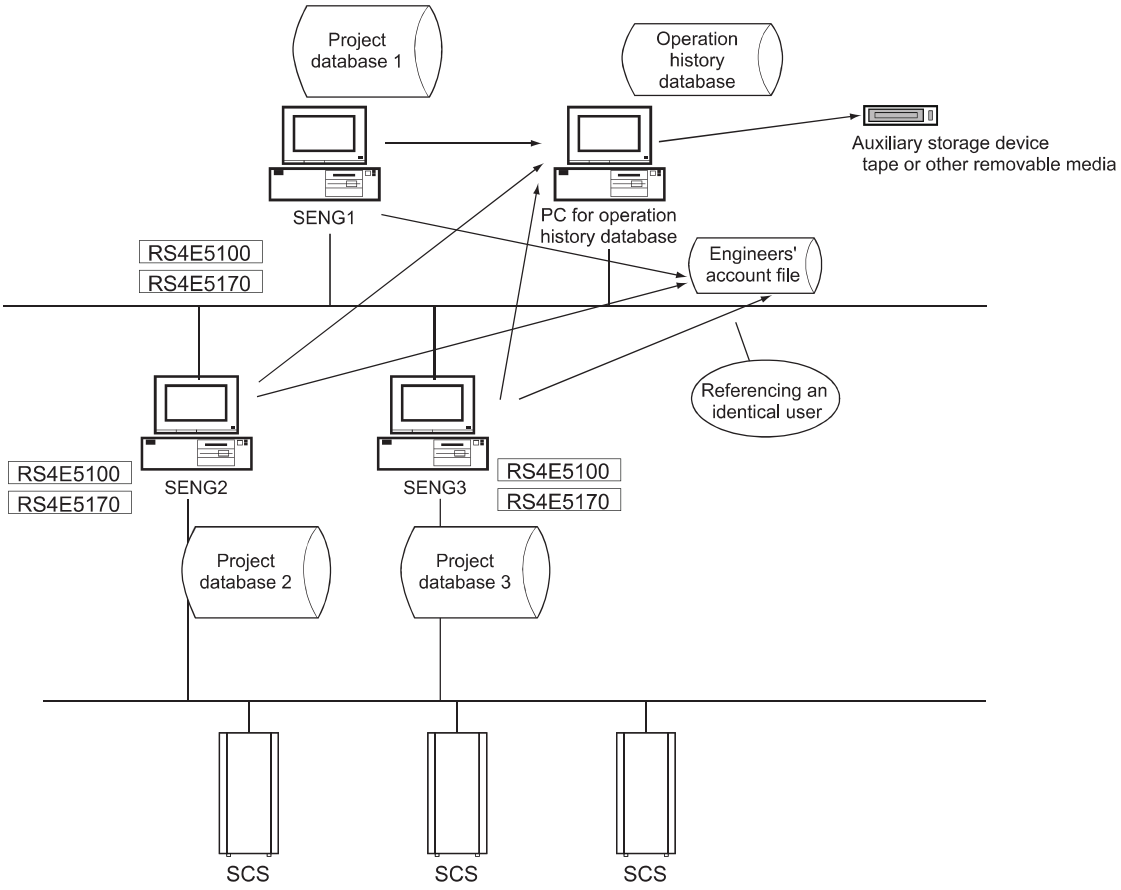


Figure E1-3 Example of use on multiple SENGs

IMPORTANT

When using the Windows authentication mode, ensure that the system to which Domain management or Combination management is applied consists of a single Windows domain in order to unify user management and passwords on all terminals. Otherwise, a security loophole is created.

Guidelines for the locations of the Engineer Registration file and History Management Database

Ensure that the locations of the Engineer Registration File and History Management Database specified in the Operation History Management Settings Tool are fully secure.

Make sure that these folders are not inadvertently opened in Explorer. It is recommended that you set access permissions that give access to no one but administrators and engineers.

- If the PC on which the History Management Database is located does not have a server OS installed on it, make sure that the number of PCs accessing the disks on that PC is no more than four. To perform History Management functions from five or more SENGs, locate the History Management Database on a PC with a server OS installed on it.
- For the PC where the History Management Database is located, you must create the folder for placing the database before applying the IT security tool.
- If the PC where the History Management Database is located does not have a server OS installed on it, ensure that, as a rule, the CENTUM project database is not located on that PC.

The storing of history data in the History Management Database and the clearing of the History Management Database may fail if the History Management Database and the CENTUM project database are on the same PC.

TIP

- If the storage of history data fails during the operation to start History Management, cancel and perform the start operation again.
- If clearing of the History Management Database fails, perform the clear operation again.

Combined use with Product Security functions

The Access Control / Operation History Management functions are additional to the Product Security functions provided as standard in ProSafe-RS. They are functionally independent, and can therefore be used in combination. However, if you use the Access Control / Operation History Management functions, the password entry function in the SCS Maintenance Support Tool is suppressed.

When using the Access Control / Operation History Management functions in combination with the Product Security functions, configure the Product Security settings as follows.

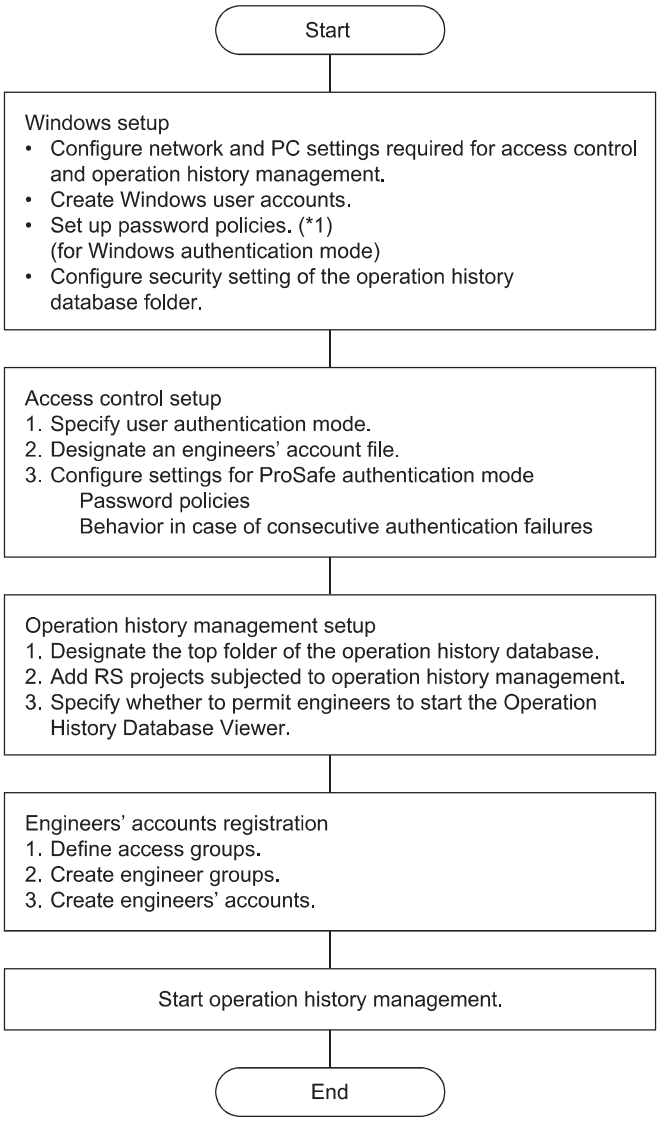
- Project password
  The project password gives permissions to users for opening and viewing the project (except when the project is set to allow Read Only opening). When you need to restrict some registered engineers' access to view the project, manage the project by applying a project password (set not to allow Read Only opening) and circulating it only to engineers who are allowed to view the project.
- POU password
  The POU password gives permissions to users for opening and viewing specific POU. When you need to restrict some registered engineers' access to open and view the particular POU, manage the project by applying a password to the POU and circulating it only to engineers who are allowed to view the project.
- SCS security level password
  An SCS security level password is a separate password for each SCS that is independent of the SENG users, and provides a system for determining whether execution is possible on the SCS. Ensure that an SCS security level password is always set.
- SCS Maintenance Support Tool password
  The password entry function in the SCS Maintenance Support Tool is suppressed when the Access Control / Operation History Management functions are being run. Log on is necessary in Logon / Engineer authentication function instead. Use the password for the SCS Maintenance Support Tool when you are not running the Access Control / Operation History Management functions.

Access Control/Operation History Management procedure

Before you start the first operation, the Access Control/Operation History Management functions need to be set up by an administrator. The following settings are configured, using mainly the Operation History Management Settings Tool.

- Specify the authentication mode
- Register the engineer
- Set the password policy
- Specify whether or not to implement Engineer Authentication
- Specify the path for the History Management Database
- Start / stop History Management

The task sequence is as follows:



*1: You can set password policies any time before operation history management is started.

Figure E1-4 Access Control/Operation History Management sequence

Executing Operation History Management

Engineers must first log on when starting an operation with a SENG function. Enter an engineer name and password as a logon operation. If the engineer name and password are entered correctly, subsequent SENG operations can be executed. If the engineer chooses Cancel, the operation cannot be executed. After logon, the following processes are executed whenever an engineer performs an operation managed with History Management.

- Access Right Check
  The system checks whether the engineer who has logged on has the access right to perform the operation in question. If the engineer has access right, he/she can perform the operation. If the engineer does not have access right, an error occurs and he/she cannot perform the operation.
- Engineer Authentication (only if the option "Do not require engineer authentication on individual operations" is unchecked)
  When an engineer executes an operation, he/she enters the engineer password under which he/she is logged on and an optional comment. If the engineer enters the correct password, he/she can execute the operation. If the engineer chooses Cancel, the operation cannot be executed.

- Store Operation History
  Once the operation is complete, a history log is recorded for the operation and a modification file is saved based on the type of operation (the modification file is only saved if the option "Do not save modification files" is unchecked.)

The engineering procedures carried out by engineers after History Management is started are the same as the ones when History Management is not being run except for these procedures.

Operation History Management process flow

The History Management process flow is shown in the following figure.

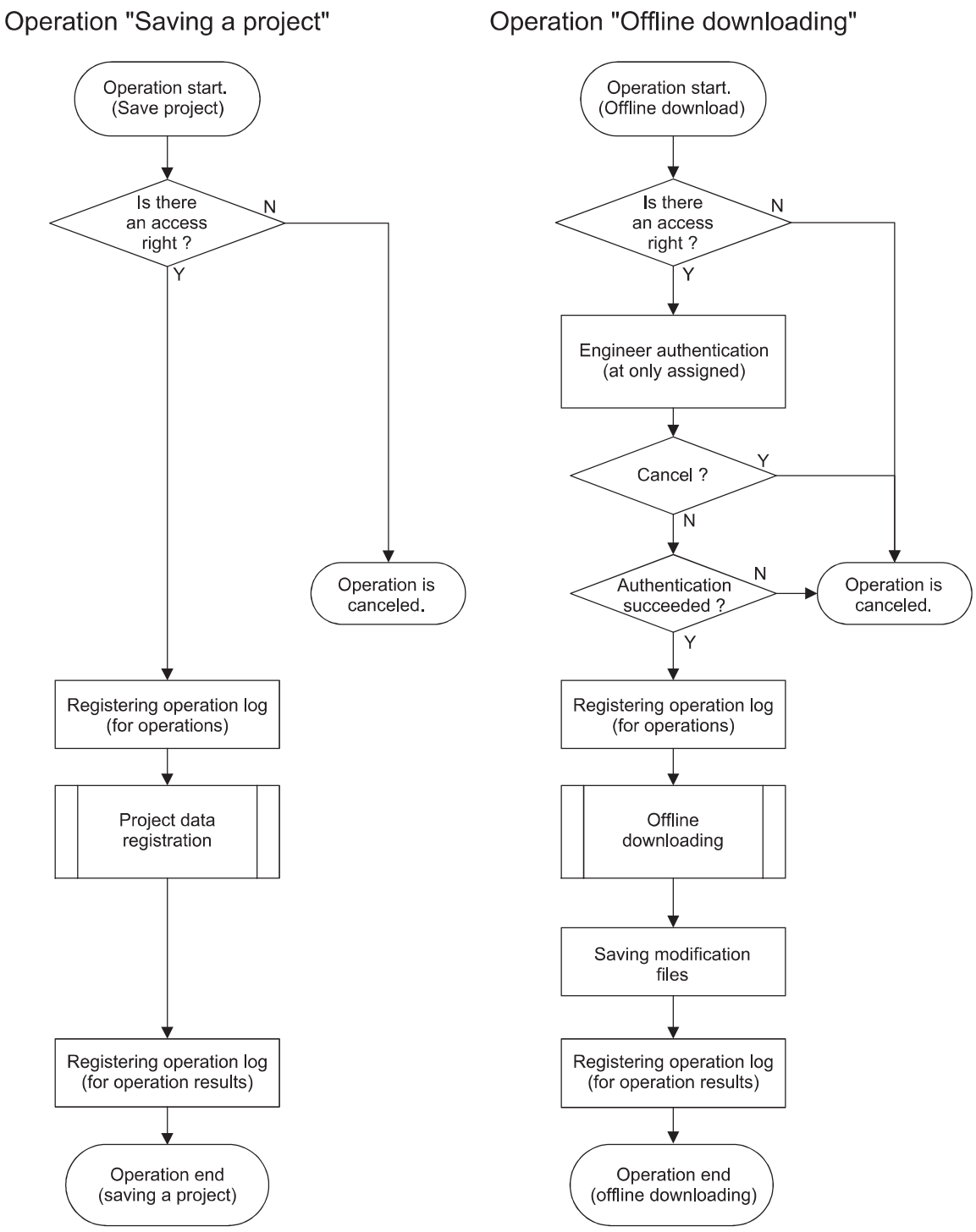


Figure E1-5 Example of a history management process flow

Access right

With the SENG Access Control and Operation History Management functions, access rights for project databases and access rights for SCS/SCS simulators are handled. These access rights are further broken down into categories.

SEE ALSO For more information about setting access rights, refer to:

E2.2.3, “Registering engineers” on page E2-19

For more information about categories of access rights, refer to:

E2.5.2, “Access rights category list” on page E2-72

E2. Access Control/Operation History Management function

ProSafe-RS access control/operation history management is one of the functions related to ProSafe-RS security. To use this function, the Access Control and Operation History Management Package is required.

The basic security functions of ProSafe-RS provide password protection for project databases and for certain operations that affect SCS. On the other hand, the access control/operation history management function controls security for individual SENG users.

E2.1 Overview of Access Control/Operation History Management

This section describes an overview of access control/operation history management.

Access Control

ProSafe-RS access control consists of "log-on/engineer authentication" and "access right check."

Log-on/engineer authentication is performed to confirm the engineer performing operations on SENG. The Authentication dialog box appears for certain operations and if the entered engineer name and password do not match the registered ones, the user cannot log on to SENG or cannot perform the certain engineering operations.

When an engineer attempts to perform an engineering operation, the access right checking function checks whether or not the engineer has the right to perform that operation, and if not, prohibits that operation. Operations by an unauthorized engineer can be thereby prevented.

Operation History Management

In ProSafe-RS operation history management, each operation performed by an engineer on SENG is recorded in an operation log file. Additionally, when a download to SCS is performed, information of changed project data (modification files) is saved. The operation logs and modification files are saved to a database specified in advance, and can be browsed using dedicated viewers. This allows you to keep track of "who," "when," "what " and "how" a change was made.

Roles of engineers and the administrator

There are two types of users in systems where access control/operation history management is used: "administrator of access control/operation history management" and "engineer." In this chapter, the "administrator of access control/operation history management" is simply called an "administrator."

SEE ALSO For more information about windows user groups to which the administrator and engineers should belong, refer to:

"■ Windows User Groups to which Administrators and Engineers Belong" in B4.6, "Setup when Using the Access Control and Operation History Management Package" in Installation Guide (IM 32P01C50-01EN)

Role of the administrator

The administrator is in charge of all the tasks related to access control and operation history management shown as follows.

- Managing networks and PCs
- Setting up access control/operation history management
- Starting/stopping operation history management
- Managing operation history database capacity
- Browsing operation history data

Role of engineers

SENG users other than the administrator are engineers.

Engineers are responsible for engineering and maintenance tasks, but they cannot execute operations if they do not have the rights. The following operations are added.

- Performing log-on operation when starting use of SENG function
- Entering password when performing certain operations
- Browsing history data (if permitted by Operation History Management Setup Tool)

E2.1.1 Overview of access control for engineers

The access control function restricts the operations by which engineers access project databases and SCS.

Units of access control

Access control is performed per PC. An engineers' account file which defines engineers, engineer groups and access rights is specified for each PC. If one common engineers' account file is specified for multiple PCs, the same access control can be performed for multiple PCs.

Access rights of engineers

An engineer needs to belong to an engineer group, and his/her engineer name and password need to be registered. An engineer belonging to a certain engineer group can perform engineering operations and maintenance operations within the rights granted to that group.

The rights of an engineer group are set by the following two kinds of settings.

- Access rights that are set for each operation category
- Range of enabled access rights

For example, rights are enabled or disabled for operations classified in categories such as new project creation, general settings, create/modify POU and downloading. Furthermore, the range of enabled access rights granted is set in RS project/SCS project units.

ProSafe authentication mode and Windows authentication mode

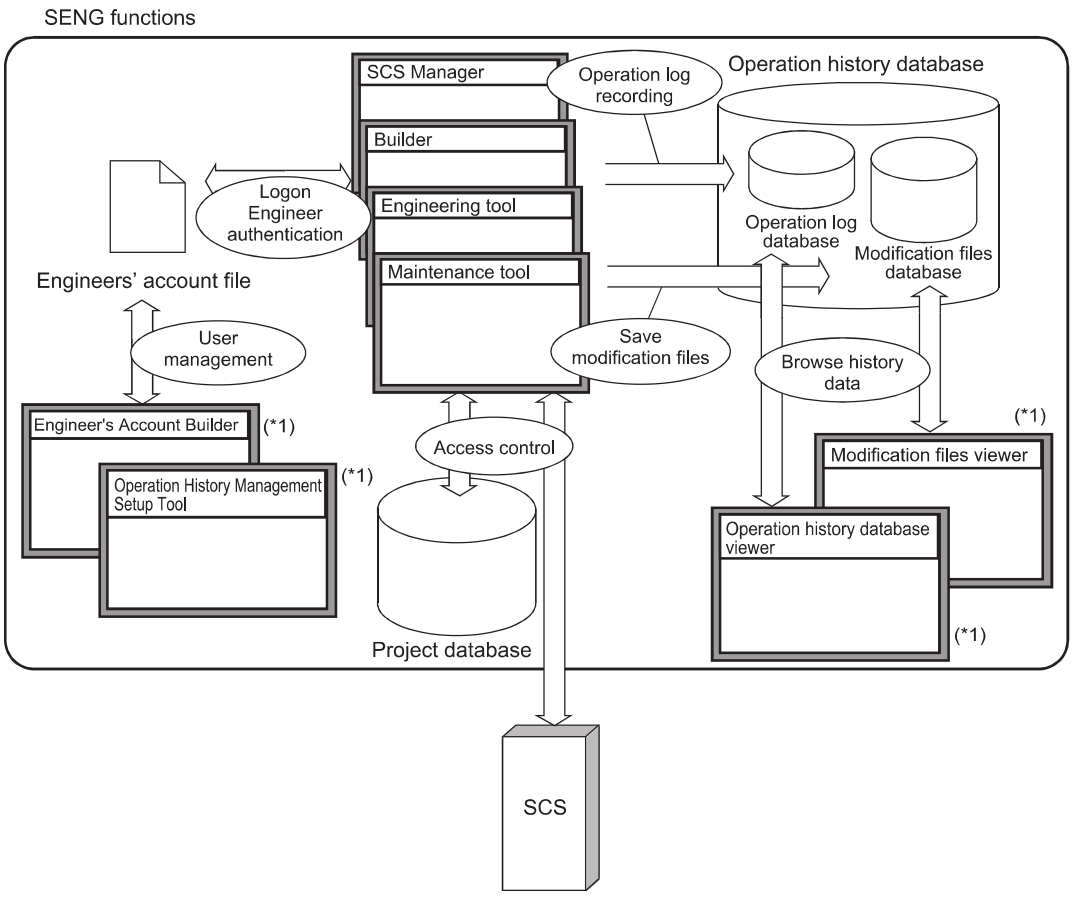
There are two types of user authentication available in ProSafe-RS.

ProSafe authentication mode uses engineer accounts that are independent from Windows user accounts, and applies the passwords and password policies that are set for ProSafe-RS.

Windows authentication mode uses Windows user accounts as the engineer accounts. When performing user management in Windows authentication mode, Windows user accounts to be used as engineers must be registered. In Windows authentication mode, the passwords and password policies of Windows users are applied to engineers.

E2.1.2 Structure of Access Control/Operation History Management function

The following figure shows the overall structure of the access control/operation history management function.



*1: These tools are included in the RS4E5170 Access Control and Operation History Management Package.

Figure E2.1.2-1 Structure of the Access Control/Operation History Management function

A summary of the components and their mutual relationships are described as follows.

Operation History Management Setup Tool

This is a tool for setting up access control/operation history management.

It performs primarily the following settings.

- Specification of engineers' account file
- Specification of user authentication mode (ProSafe authentication mode or Windows authentication mode)
- Specification of top folder of operation history database
- Setting of password policies in ProSafe authentication mode
- Starting/stopping of operation history management

Engineers' Account Builder

This is a builder for registering engineer names and setting up access rights for engineers.

- Registering engineer names
  When in ProSafe authentication mode, any engineer names can be registered. When in Windows authentication mode, engineer names that are already registered as Windows user names should be registered.
- Creating engineer groups
  You can create engineer groups, which are the units in which access rights to project databases and SCS are specified. The access rights an engineer has are determined by assigning the engineer to an engineer group.

Engineers' Account file

This is the file that contains engineer account information and the access rights information set for engineers. It is specified for each SENG on which engineering is performed. The information set in the Engineers' Account Builder are saved to this file.

Operation History Database

This is the database that stores operation history information (operation logs and modification files). It is generated for each RS project in the location specified in the Operation History Management Setup Tool.

Operation History Database Viewer

This is a viewer for browsing operation history information (operation logs) saved in the operation history database.

It can display all operation logs or a filtered list, and can export operation logs to a file in CSV format. From this viewer, you can start up the Modification Files Viewer.

Modification Files Viewer

This is a viewer for browsing modification files saved in the operation history database.

If modification files corresponding to an operation log are browsed, it is possible to check the modification contents of the project data modified by that operation. Also, the differences between modification files corresponding to an operation log at any two points in time can be displayed.

SCS Manager, Builders, Engineering Tools and Maintenance Tools

Logon/engineer authentication, access control by rights checking and operation history management are performed for engineers' operations performed by using these programs and tools.

E2.1.3 Access Control/Operation History Management target operation list

The operations that are the targets of access control/operation history management are as follows.

"Yes" indicates that the process such as Log-on/Engineer Authentication or Access Rights Check is executed, and an empty box indicates that the process is not executed.

Table E2.1.3-1 Access Control/Operation History Management target operations

Operation Name	Log-on/Engineer Authentication	Access Rights Check	Operation Log Recording	Save modification files (*1)
Start SCS Manager	Yes (log on)		Yes (*2)	
Close SCS Manager			Yes (*2)	
Create new SCS project		Yes	Yes	Yes
Open SCS project			Yes	Yes (when upgrading)
Save project		Yes	Yes	
Import by SCS Manager		Yes	Yes	Yes
Save dictionary		Yes	Yes	
Save I/O wiring		Yes	Yes	
Save binding list		Yes	Yes	
Save library dependencies		Yes	Yes	
Open POU			Yes	
Save POU		Yes	Yes	
Open by builder			Yes	
Save by builder		Yes	Yes	
Change SCS project properties		Yes	Yes	
Build		Yes	Yes	Yes (user-defined projects only)
Clean		Yes	Yes	
Save analyzer's results		Yes	Yes	
Start document generator			Yes	
Start master database restoring function	Yes (log on)		Yes (*2)	
Close master database restoring function			Yes (*2)	
Restore master database		Yes	Yes	Yes
Start version control tool	Yes (log on)		Yes (*2)	
Close version control tool			Yes (*2)	
Check in to version control		Yes	Yes	
Check out from version control		Yes	Yes (if the checked out project is a target of operation history management)	Yes (if the checked out project is a target of operation history management)

Continues on the next page

Table E2.1.3-1 Access Control/Operation History Management target operations (Table continued)

Operation Name	Log-on/Engineer Authentication	Access Rights Check	Operation Log Recording	Save modification files (*1)
Offline download	Yes (engineer authentication) (*3)	Yes	Yes	Yes
Master database offline download	Yes (engineer authentication) (*3)	Yes	Yes	
Online change download	Yes (engineer authentication) (*3)	Yes	Yes	Yes
Restart SCS	Yes (engineer authentication) (*3)	Yes	Yes	
Save operation marks		Yes	Yes	
Download operation marks		Yes	Yes	
Start debug mode		Yes	Yes	
Exit debug mode			Yes	
Start logic simulation		Yes	Yes	
Close logic simulation			Yes	
Start test function		Yes	Yes	
Update test database		Yes	Yes	
Database validity check		Yes	Yes	
Repair database		Yes	Yes	
Start SCS Status Overview window	Yes (logon) (*4) (only when started from Start menu)		Yes (*2)	
Close SCS Status Overview window			Yes (*2)	
Start SCS State Management window			Yes	
Close SCS State Management window			Yes	
Change SCS security level		Yes	Yes	
Change security level password	Yes (engineer authentication) (*3)	Yes	Yes	
Lock		Yes	Yes	
Unlock		Yes	Yes	
Set values		Yes	Yes	
Enable output	Yes (engineer authentication) (*3)	Yes	Yes	
Start output module	Yes (engineer authentication) (*3)	Yes	Yes	
IOM download	Yes (engineer authentication) (*3)	Yes	Yes	

Continues on the next page

Table E2.1.3-1 Access Control/Operation History Management target operations (Table continued)

Operation Name	Log-on/Engineer Authentication	Access Rights Check	Operation Log Recording	Save modification files (*1)
NIU maintenance port setting	Yes (engineer authentication) (*3)	Yes	Yes	
Time setting		Yes (*5)	Yes (*2)	
Acknowledge/delete diagnostic information messages		Yes (*5)	Yes	
Change SCS Maintenance Support Tool settings		Yes (*5)	Yes (*2)	
Start IOM Control Right Switching Tool	Yes (log on)		Yes (*2)	
Close IOM Control Right Switching Tool			Yes (*2)	
Switch IOM control right		Yes	Yes	
Start Message Cache Tool	Yes (log on)(*4)		Yes (*2)	
Close Message Cache Tool			Yes (*2)	
Operate Message Cache Tool		Yes (*6)	Yes (trip information initialization)	
Pause message acquisition		Yes (*5)	Yes (*2)	
Resume message acquisition		Yes (*5)	Yes (*2)	
Start operation history management (operation by administrator)			Yes (*7)	Yes
Stop operation history management (operation by administrator)			Yes (*7)	
Exceeded number of authentications			Yes (*2)	
Local user logon in domain environment			Yes (*2)	
Record a comment (operation by administrator)			Yes (*2)	

*1: Saved if "Do not save in modification files" check box is not selected in Operation History Management Tool.
*2: Not recorded in operation log database for each SCS project, but recorded in common operation log database.
*3: Performed if "Do not require engineer authentication on individual operations" check box is not selected in Operation History Management Tool.
*4: Enter engineer name and password instead of entering password of SCS Maintenance Support Tool in standard security function.
*5: Whether or not to enable access rights is decided regardless of the range of enabled access rights that are granted to Engineers by using the Engineers' Account Builder.
*6: Whether or not to enable access rights for trip information initialization is decided depending on the range of enabled access rights that are granted to Engineers by using the Engineers' Account Builder. Whether or not to enable access rights for other operations is decided regardless of the range of enabled access rights that are granted to Engineers by using the Engineers' Account Builder.
*7: Recorded both in operation log database for each SCS project and in common operation log database.

E2.2 Setting up Access Control/Operation History Management

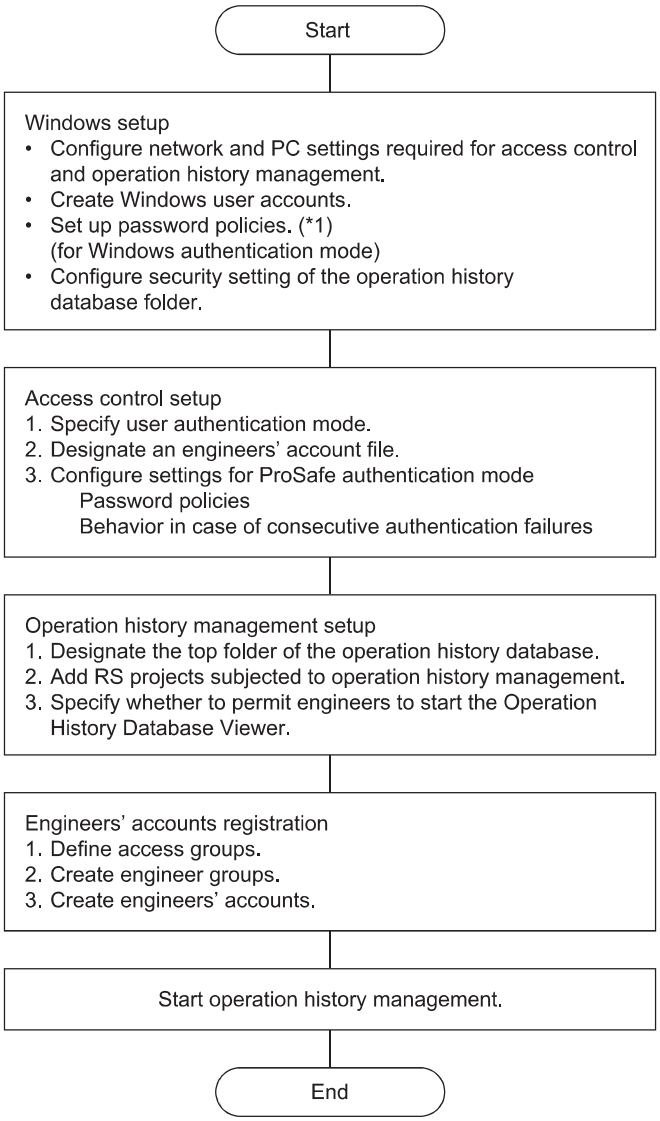
Setup of access control/operation history management is performed using the Operation History Management Setup Tool and the Engineers' Account Builder after setting up the network and PCs.

This section shows the flow of setup operations, and describes the setup procedures performed using the Operation History Management Setup Tool and the Engineers' Account Builder.

Flow of setup operations

The administrator first sets up the network and computers, and checks that the required Windows user accounts have been created. When performing user management in Windows authentication mode, register the Windows user accounts to be used for the engineers. Also, security is set to folders where the operation history database is located. After that, set up the access control/operation history management function on an SENG having a license for Access Control and Operation History Management Package.

The following figure shows the work flow.



*1: You can set password policies any time before operation history management is started.

Figure E2.2-1 Setting up Access Control/Operation History Management

E2.2.1 Settings for access control

On the Access Control tab sheet of the Operation History Management Setup Tool, perform common settings for access control.

After setup has been performed on the Access Control tab sheet and engineers have been registered in the Engineers' Account Builder, rights checking and log-on/engineer authentication are started when [OK] or [Apply] is clicked on the Operation History Management Setup Tool.

Starting the Operation History Management Setup Tool

The Operation History Management Setup Tool can be started by administrators only.

1. Start the Operation History Management Setup Tool.

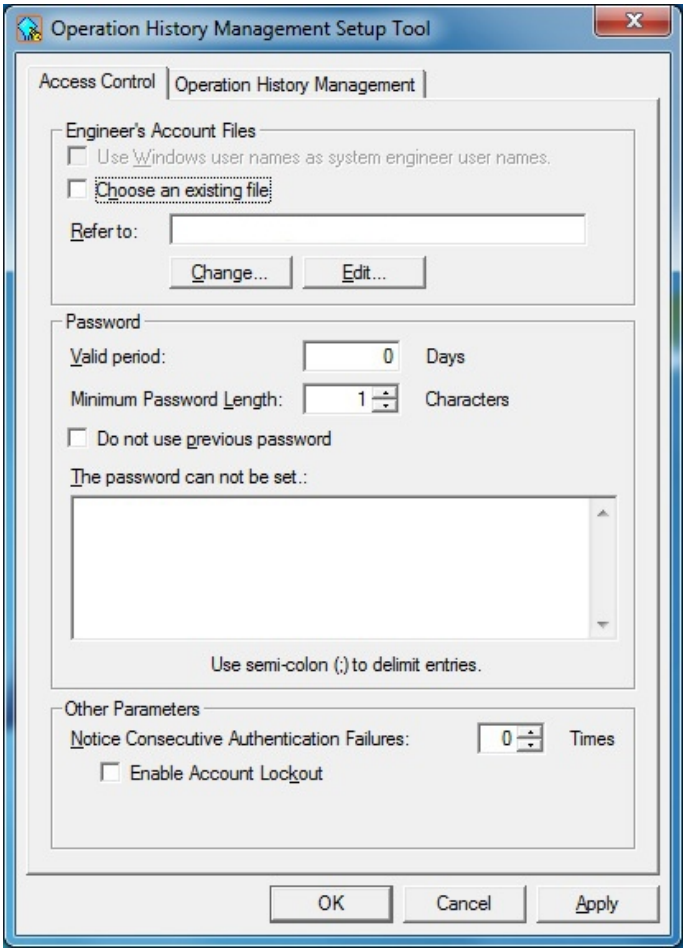


Figure E2.2.1-1 Operation History Management Startup Tool (Access Control tab sheet)

Specifying the user authentication mode

Specify whether to use ProSafe authentication mode or Windows authentication mode. Windows authentication mode can be used when the standard model security is set on the SENG PC and cannot be used when the legacy model security is set. The default setting is ProSafe authentication mode.

1. Perform the following setting on the Access Control tab sheet of the Operation History Management Setup Tool.
   - To use Windows authentication mode, select the "Use Windows user names as system engineer names" check box.

- To use ProSafe authentication mode, clear the "Use Windows user names as system engineer names" check box.

When the [OK] or [Apply] button is clicked, the setting becomes valid.

In Windows authentication mode, "Windows Authentication Mode" is displayed in the title bar of the Engineers' Account Builder. If you change from ProSafe authentication mode to Windows authentication mode, the set values of items in the categories of "Password" and "Other Parameters" are cleared.

Specifying an Engineers' Account file

The engineers' account file is the file that contains the engineers' account information edited in the Engineers' Account Builder and the access rights information set for engineers. This file is specified for each SENG PC.

After an engineers' account file is specified, the Engineers' Account Builder can be started up to register engineers and set access rights.

When creating a new engineers' account file

To create a new engineers' account file, perform the following procedure.

1. On the Access Control tab sheet of the Operation History Management Setup Tool, clear the "Choose an existing file" check box.
2. In "Refer to:", specify the folder where the engineers' account file is to be saved.

Thereafter, the default engineers' account file is created in the specified folder when the [OK] or [Apply] button is clicked.

When using an existing engineers' account file

In a system that uses multiple SENGs to allow multiple SENGs to use the same engineer names, engineer groups and access control settings such as rights, specify the existing engineers' account file on each SENG so that multiple SENGs can reference the same file.

To specify the existing engineers' account file, perform the following procedure.

1. On the Access Control tab sheet of the Operation History Management Setup Tool, select the "Choose an existing file" check box.
2. Click the [Change] button.
   The dialog box for selecting a file appears.
3. In the File Selection dialog box, specify the engineers' account file (SengSecurity.sva) to be used, and click [OK].
   The path to the engineers' account file appears in the "Refer to:" box.

Settings required when ProSafe authentication mode is selected

If you have selected ProSafe authentication mode on the Access Control tab sheet, set the password policies and the behavior when authentication fails consecutively.

Setting the password policy

To set the password policy for ProSafe authentication mode, perform the following procedure.

1. In the "Valid period" box on the Access Control tab sheet, specify the number of days passwords are valid. If 0 is specified, the valid period is unlimited. The default value is 0.
2. In the "Minimum password length" box, specify the minimum number of characters that can be registered as a password. Integers from 1 to 32 may be specified. The default value is 1.

3. To prohibit use of a password that is the same as a previously set password when a password is changed, select the "Do not use previous password" check box. By default, this is not prohibited (check box is empty).

4. If there are character strings that you wish to prohibit as passwords, enter them in the "The password can not be set" box. Setting strings that someone could easily guess can prevent the SENG from being improperly used. To specify multiple strings, separate them by semicolons. Up to 2048 single-byte characters can be specified. Nothing is specified by default.

Setting up the behavior in case of consecutive authentication failures

To set up the behavior of the system when authentication fails in ProSafe authentication mode, set the following items.

- Notice Consecutive Authentication Failures
  If a wrong password is entered consecutive times when logging onto SENG or performing engineer authentication, it can be regarded as an attempt at improper access, and can be recorded as an authentication error in the operation log. The number of times a wrong password is entered is specified, and when authentication fails consecutively the specified number of times, an authentication error occurs. If 0 is specified, an authentication error does not occur. The default value is 0.

- Enable Account Lockout
  When authentication fails consecutive times, that engineer can be locked out. Since the locked-out engineer cannot perform log-on or engineer authentication, he/she cannot perform engineering work. By default, the lockout function is disabled.

To set up the behavior in case of consecutive authentication failures, perform the following procedure.

1. To log authentication errors, specify the number of consecutive times the wrong password in the "Notice Consecutive Authentication Failures" box of the Access Control tab sheet. Specify 0 if you do not wish to log the errors.

2. To use the lockout function, select the "Enable Account Lockout" check box, and set the "Notice Consecutive Authentication Failures" to 1 or more.

TIP

If the lockout function is changed to disabled, the lockout of previously locked-out engineers is released.

Settings required when Windows authentication mode is selected

If you have selected Windows authentication mode, set the password policies and the behavior in case of consecutive authentication failures in Windows.

E2.2.2 Setup related to Operation History Management

Operation history management is performed in RS project units. To perform setup related to operation history management, perform the following settings.

Set the following items as PC settings.

- Top folder of operation history database
- Permission to start the Operation History Database Viewer

Add the RS projects for which operation history management is to be performed, and set the following items for each project.

- Free disk space when backup warning is displayed
- Whether or not to save modification files
- Whether or not to perform engineer authentication

IMPORTANT

A project for which operation history management is performed and the operation history database are associated with each other. If not correctly associated, operation history management will not work. If the project database is moved or an SCS project is added or deleted, promptly perform the required operations on the Operation History Management tab sheet.

SEE ALSO For more information about tasks required after adding, moving or deleting a project database, refer to:

"■ Tasks required after adding, moving or deleting a project database" on page E2-47

■ Specifying top folder of Operation History Database

The top folder of the operation history database is done during the procedure for adding RS projects for which operation history management is to be performed.

■ Adding an RS project for history management

To perform operation history management for a certain RS project, add it as a target of operation history management. Perform this according to the following procedure.

1. In the Operation History Management Setup Tool, display the Operation History Management tab sheet.

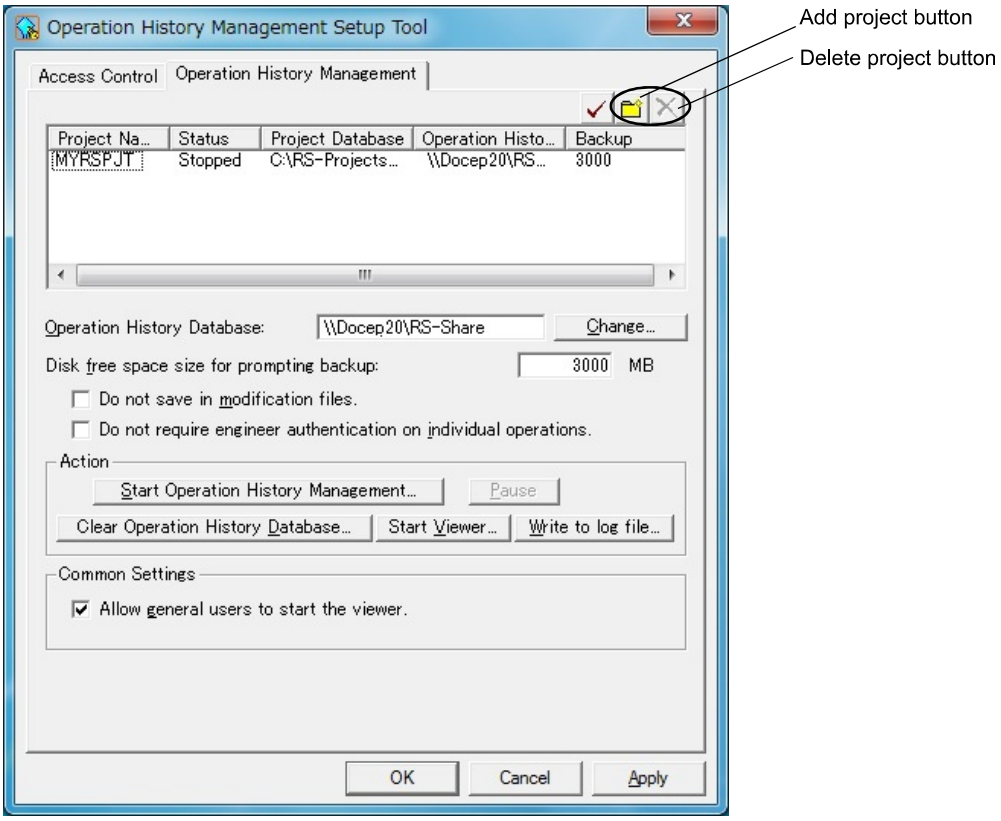


Figure E2.2.2-1 Operation History Management Setup Tool (Operation History Management tab sheet)

2. Click the Add Project button on the top right of the Operation History Management tab sheet.
   The following dialog box appears.

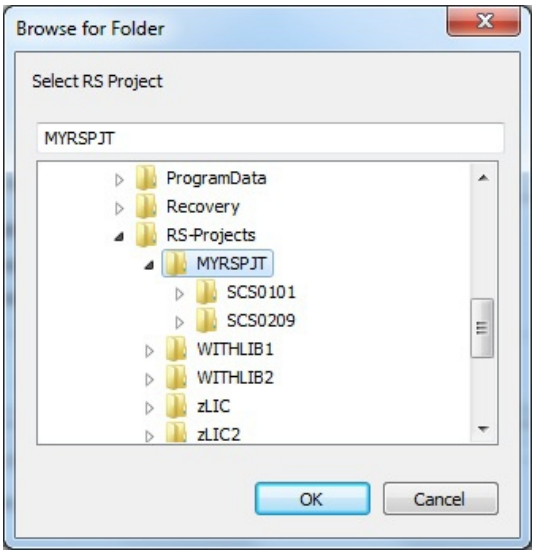


Figure E2.2.2-2 Project Selection dialog box

3. Select the folder of the RS project and click [OK].
   The selected RS project name appears in the list.

TIP

When performing operation history management on multiple PCs, use the same method of referencing the project on each PC. (Whether to reference by a network drive or in UNC format. If by a network drive, use the same drive name.)

A dialog box for selecting the top folder of the operation history database appears.

4. When adding an RS project for the first time, select the top folder of the operation history database, and click [OK].

IMPORTANT

When adding a second RS project or thereafter, the dialog box for selecting the top folder of the operation history database appears. If there is no need to change the top folder location, click [OK] in the dialog box as is.

TIP

The same operation history database folder cannot be specified for another RS project of the same name in a different location. An error message appears if there is such a duplication.

5. Specify the empty disk space for prompting backup of the operation history database. Select the RS project in the list and enter in units of MB in the "Disk free space size for prompting backup" box. The default value is 3000 MB.

IMPORTANT

As modification files accumulate in the operation history database, the amount of free disk space gradually decreases. When the remaining free space almost reaches to the specified free disk space, a dialog box appears to alert low disk space. When the remaining free space becomes lower than the specified free disk space, a dialog box appears to prompt backup and further operations to log the operation history can not be performed. When an alert dialog box appears, you should be ready to backup.

6. If you do not wish to save modification files in the operation history database, select the "Do not save in modification files" check box. By default, modification files are saved.
7. If you do not wish to perform engineer authentication (password input) for individual operations, select the "Do not require engineer authentication on individual operations" check box. By default, engineering authentication is required.

TIP

When the "Do not require engineer authentication on individual operations" check box is selected, password input is required only at logon.

Deleting an RS project from the targets of Operation History Management

To delete an RS project for which operation history management is being performed from the targets of operation history management, perform the following procedure.

1. In the list on the Operation History Management tab sheet, click the project you wish to delete.
2. Click the Delete Project button on the top right of the tab sheet.
3. In the confirmation dialog box, click [OK].
   The RS project is deleted from the list, and operation history management of the RS project stops.

The data in the operation history data base is not deleted when an RS project is deleted.

Permission to start Operation History Database Viewer

By default, only administrators can browse the operation history database.

To also enable general engineers to browse the operation history database, perform the following settings.

1. On the Operation History Management tab sheet, select the "Allow general users to start the viewer" check box.

When this is set, general engineers can start the Operation History Database Viewer. As a result, they can also start the Modification Files Viewer.

E2.2.3 Registering engineers

This section first describes the mechanism of engineer registration including initial engineers' access rights setup and shows examples of settings. The operations for registering an engineer using the Engineers' Account Builder are described next.

Flow of engineer registration operations

Engineer registration operations are performed using the Engineers' Account Builder. The contents set by the Engineers' Account Builder are saved in the engineers' account file.

To perform engineer registration operations, perform the following procedure.

1. Determine the policy for access control. (Determine the contents to be set by builder.)
2. Define access groups.
3. Create engineer groups.
4. Register each engineer's account, and assign it to an engineer group.

Steps 1 through 3 are required when using access control/operation history management for the first time. After use has begun, perform only engineer account registration for the engineer registration operations.

Determining policies for access control

Before you start working with the Engineers' Account Builder, determine the policies for access control.

- Access groups required in the system and their definition contents (determine the rights of assumed users while referring to the default access groups)
- Engineer group names to be created
- Which access group rights to grant to each engineer group
- Range of RS projects/SCS projects that each engineer group is responsible for
- Which engineer group to assign engineers to

Relationship between engineers, engineer groups and access groups

Access control in ProSafe-RS sets the access rights of engineers by assigning engineers to user groups called "engineer groups."

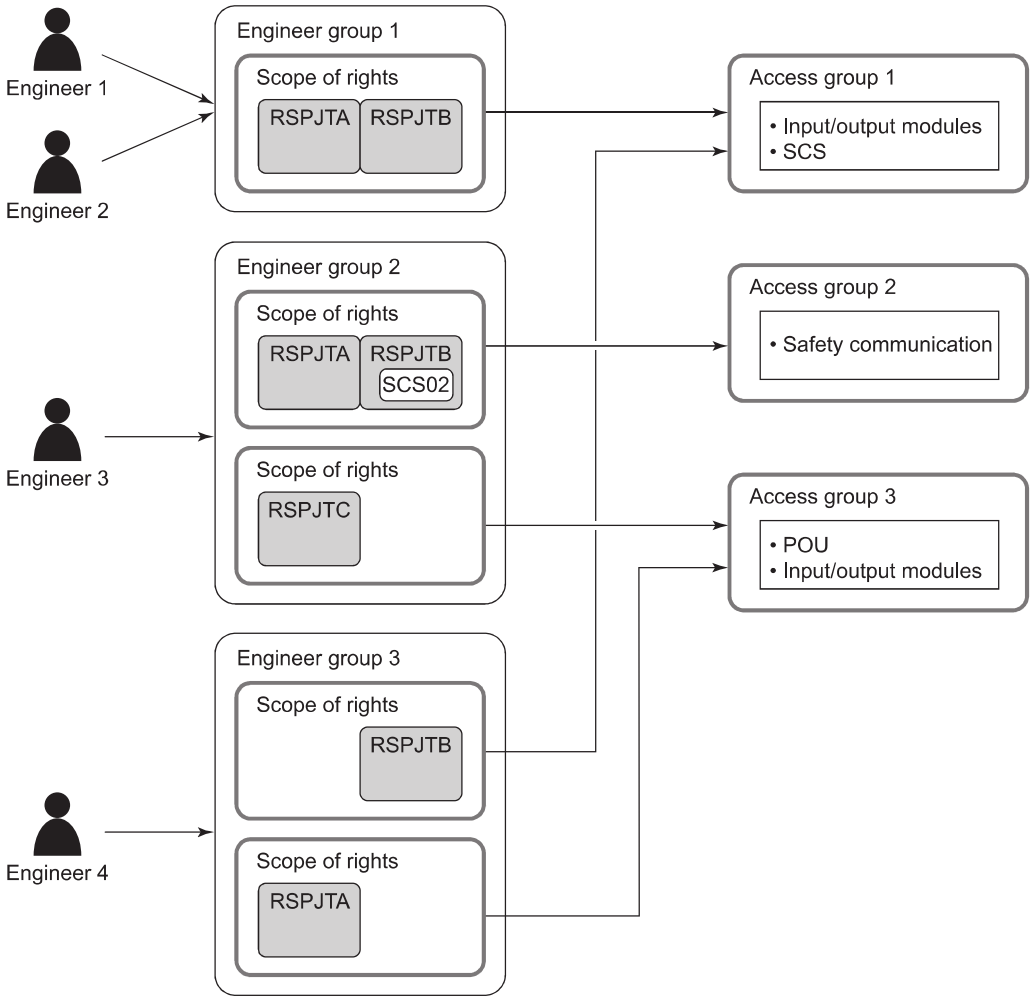


Figure E2.2.3-1 Relationship between engineers, engineer groups and access groups

One engineer may belong to one engineer group. For each engineer group, the access rights to project databases and/or SCS and the range of RS projects/SCS projects for which those rights are enabled are specified.

Access rights are set by assigning an "access group" to each engineer group. An access group is a combination of rights to execute various operations that access project databases or SCS, and needs to be predefined for the assumed user types.

Types of access rights

There are access rights for project databases and access rights for SCS/SCS simulators. These access rights are further broken down into categories.

If an engineer has access rights of a certain category, that engineer can execute the operations that pertain to that category. If he does not have access rights, he cannot execute those operations.

<Example>

- If an engineer has access rights for the Project Creation category, he can execute operations to create new SCS projects in the SCS Manager.
- If an engineer has access rights for any of the categories General Settings, POU, I/O, Safety Communication, External Communication, CENTUM Alarm Definition, Offline Download, Online Change Download and SCS Simulator, the engineer can execute the operations of build, acknowledgement by analyzers and database validity check.

SEE ALSO For more information about categories of access rights, refer to:

E2.5.2, “Access rights category list” on page E2-72

Default access groups

Default access groups are predefined in the Engineers' Account Builder.

The default access groups are ALL, which provides access rights for all categories, NONE, which provides no access rights for any categories, and Operator1, Operator2, Engineer1, Engineer2, Maintenance1 and Maintenance2, which provide typical operator, engineer and maintenance rights.

Access rights can be set up efficiently by editing these access groups. The access rights settings of each access group are as follows.

Category	ALL	NONE	Operator1	Operator2	Engineer1	Engineer2	Maintenance1	Maintenance2
Project Creation	Y					Y		
General Settings	Y					Y		
POU	Y				Y	Y		
I/O	Y				Y	Y		
Safety communication	Y					Y		
External communication	Y				Y	Y		
CENTUM Alarm Definition	Y					Y		
Version Control Tool (Check-in)	Y				Y	Y		
Version Control Tool (Check-out)	Y					Y		
Master Database Restore	Y				Y	Y		
Offline Download	Y					Y		
Online Change Download	Y				Y	Y		
Operation Mark Save	Y			Y	Y	Y	Y	Y
SCS Simulator	Y				Y	Y		
Debug	Y			Y	Y	Y		Y
Forcing	Y				Y	Y		Y
Maintenance	Y				Y	Y	Y	Y
Diagnosis Acknowledgment	Y				Y	Y	Y	Y
Message Cache	Y					Y		Y

Y: Right is granted. Blank: Right is not granted.

Figure E2.2.3-2 Default access groups

Example of adding an access group

To set up rights other than those of the default access groups, create a new access group. For example, for a certain engineer group, you may wish to add download rights to the rights of the default access group Operator2. In this case, first, copy the Operator2 access group to create a new access group named PowerOperator. Then, set the categories Offline Download and Online Change Download to Yes.

Category	PowerOperator
Project Creation	
General Settings	
POU	
I/O	
Safety communication	
External communication	
CENTUM Alarm Definition	
Version Control Tool (Check-in)	
Version Control Tool (Check-out)	
Master Database Restore	
Offline Download	Y
Online Change Download	Y
Operation Mark Save	Y
SCS Simulator	
Debug	Y
Forcing	
Maintenance	
Diagnosis Acknowledgment	
Message Cache	

Y: Right is granted. Blank: Right is not granted.

Figure E2.2.3-3 Example of adding an access group

Default engineer groups

The engineer groups shown in the following table are predefined in the Engineers' Account Builder.

Table E2.2.3-1 Default engineer groups

Engineer Group	Access Group	RS PJT Range	SCS PJT Range	Exclude RS PJT	Exclude SCS PJT
DEFGRP	ALL	*			
NONEGRP	NONE				
OPE1GRP	Operator1	*			
OPE2GRP	Operator2	*			
ENG1GRP	Engineer1	*			
ENG2GRP	Engineer2	*			
MNT1GRP	Maintenance1	*			
MNT2GRP	Maintenance2	*			

For example, access group ALL is assigned to DEFGRP for all RS projects. Access group NONE is assigned to NONEGRP for all RS projects. Engineers belonging to DEFGRP can perform all operations on all SCS projects in all RS projects. Engineers belonging to NONEGRP can only reference files in all SCS projects in all RS projects. They cannot change, create or delete files, and cannot perform operations on SCS.

The default engineer group settings are as follows.

Range of enabled access rights

Assign an access group to each engineer group, and set the range of enabled access rights. This section describes specification of the range of enabled access rights.

Setting the range of enabled access rights

By setting the following items on the Engineer Group tab sheet of the Engineers' Account Builder, the range of RS projects and SCS projects for which rights defined by the access group are enabled is specified.

- RS project range (RS PJT Range)
  Enter the RS project names for which rights specified by the access group are enabled. If "*" is specified, the rights will be enabled for all RS projects.
- SCS project range (SCS PJT Range)
  If you wish to enable rights specified by the access group only for certain SCS projects within the specified RS project range, enter the SCS project name (SCSddss or library project name). If the section is blank, rights are enabled for all SCS projects included in the specified RS project range.
- RS project exclusion range (Exclude RS PJT)
  Two types of specification may be performed for this item.
  1. If there is an RS project that you wish to exclude among the RS projects specified by the RS project range, enter that RS project name. If the section is blank, there is no exclusion range.

     For example, if "*" is specified in the "RS PJT Range" section and "MYRSPJT" is entered in the "Exclude RS PJT" section, rights specified by the access group are enabled in all RS projects except MYRSPJT.
  2. When you specify any SCS that you wish to exclude in the "Exclude SCS PJT" cell, specify the RS project to which that SCS belongs.
- SCS project exclusion range (Exclude SCS PJT)
  If there is an SCS project you wish to exclude among those included in the RS projects specified as the enabled range, enter that SCS project name (SCSddss or library project name). In this case, set the RS project to which that SCS project belongs in the "Exclude RS PJT" cell.

  If the "Exclude SCS PJT" cell is blank, the exclusion range is not set.

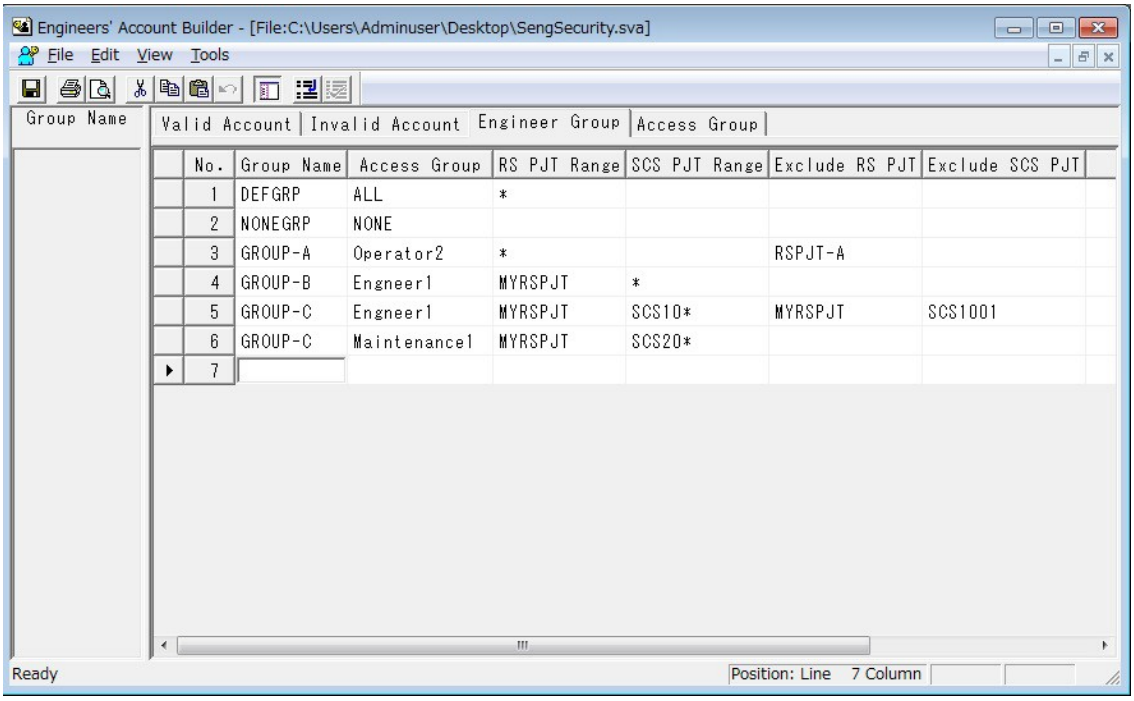


Figure E2.2.3-4 Engineer group tab sheet

Input rules for specifying the range of enabled access rights

The input rules for the "RS PJT Range," "SCS PJT Range," "Exclude RS PJT" and "Exclude SCS PJT" columns are as follows.

- When multiple items are entered in one cell, they are to be separated by commas.
- When "*" is specified, all RS projects or SCS projects are specified.

  (In SCS PJT Range, this is the same as a blank cell.)
- A wildcard "*" may be used only at the end of an RS/SCS project name.
  For example, if "MYRS*" is entered, all RS projects that begin with MYRS are specified.

  If "SCS10*" is entered, all SCS projects that begin with SCS10 are specified.

  "*" cannot be used in the middle of a project name, as in "MY*PJT" or "SCS*16".
- "RS PJT Range" and "Exclude RS PJT" may be up to 50 characters each.
  "SCS PJT Range" and "Exclude SCS PJT" may be up to 200 characters each. However, the total of the character strings specified in the four columns that define the range of enabled access rights on one line must be up to 250 characters.
- If a range of rights cannot be specified on one line, it may be specified by creating multiple lines with the same engineer group name. The range of rights in this case encompasses all ranges specified on all lines (logical OR). When an exclusion range is set on a certain line, the ranges on the other lines are not excluded.

Specifying the range of enabled access rights in SCS project units

To specify access rights ranges in SCS project units, the range of enabled access rights can be set by a combination of "RS PJT Range" and "SCS PJT Range," and the range of rights exclusion can be set by a combination of "Exclude RS PJT" and "Exclude SCS PJT." These settings may be blank but obey the following rules.

Table E2.2.3-2 Combinations of range of enabled access rights specifications

RS PJT Range (*1)	SCS PJT Range (*1)	Range of Enabled Access Rights That Is Set
-	-	Rights are not granted.
-	Specified	Setting prohibited (results in error when saved in Builder.)
Specified	-	Rights are granted for all SCS projects included in the specified RS project.
Specified	Specified	Rights are granted for the specified SCS project, among the SCS projects included in the specified RS project.

*1: -: Range is not specified and column is left blank.

Table E2.2.3-3 Combinations of range of rights exclusion specifications

Exclude RS PJT Range (*1)	Exclude SCS PJT (*1)	Range of Rights Exclusions That Is Set
-	-	There is no range of rights exclusion.
-	Specified	Setting prohibited (results in error when saved in Builder.)
Specified	-	Rights are disabled for all SCS projects included in the RS project specified by Exclude RS PJT.
Specified	Specified	Rights are disabled for the specified SCS project, among the SCS projects included in the RS project specified by Exclude RS PJT.

*1: -: Range is not specified and column is left blank.

Examples for engineer group assignment

Examples of engineer groups settings in the following system configuration are shown.

Table E2.2.3-4 Example for system configuration

RS Project Name	SCS Project Configuration
RSPJT-A	SCS0101-SCS0116
RSPJT-B	SCS1001-SCS1032
RSPJT-C	SCS2001-SCS2064

Example 1: Specifying RS project ranges

Table E2.2.3-5 Engineer group assignment example (1)

Engineer Group	Access Group	RS PJT Range	SCS PJT Range	Exclude RS PJT	Exclude SCS PJT
ENG	Engineer1	RSPJT-A	*		
MAINTE	Maintenance2	RSPJT-A	SCS011*		
OPR1	PowerOperator	*	*	RSPJT-A	

When set as shown above, the rights that each engineer group has are as follows.

- Engineers belonging to the engineer group ENG have the rights of Engineer1 for all SCS projects of the RS project RSPJT-A.
- Engineers belonging to the engineer group MAINTE have the rights of Maintenance2 for the SCS projects from SCS0110 to SCS016 of the RS project RSPJT-A.
- Engineers belonging to the engineer group OPR1 have the rights of PowerOperator for all RS projects except RSPJT-A.

Example 2: Excluding a certain SCS project

Table E2.2.3-6 Engineer group assignment example (2)

Engineer Group	Access Group	RS PJT Range	SCS PJT Range	Exclude RS PJT	Exclude SCS PJT
ENG 1	Engineer	RSPJT-A	*	RSPJT-A	SCS0101, SCS0105

When set as shown above, engineers belonging to the engineer group ENG1 have the rights of Engineer for SCS projects other than SCS0101 and SCS0105 among the SCS projects of RS project RSPJT-A. In this case, "Exclude RS PJT" specifies the location of the excluded SCS project.

Example 3: Specifying a range of enabled rights on multiple lines

A range of enabled rights can be specified on multiple lines.

Table E2.2.3-7 Engineer group assignment example (3)

Engineer Group	No.	Access Group	RS PJT Range	SCS PJT Range	Exclude RS PJT	Exclude SCS PJT
ENG 1	1	Engineer	RSPJT-A	*		
	2	Engineer	RSPJT-B	*	RSPJT-B	SCS1001

The resulting range of enabled rights of engineer group ENG1 is as follows.

Table E2.2.3-8 Rights of ENG1

RS Project	SCS Project	Result due to 1 (*1)	Result due to 2 (*1)	Granted rights
RSPJT-A	SCS0101-SCS0116	Yes	No	Engineer
RSPJT-B	SCS1001	No	No	No
	SCS1002-SCS1032	No	Yes	Engineer
RSPJT-C	SCS2001-SCS2064	No	No	No

*1: Yes: Rights are granted.
No: Rights are not granted.

Starting the Engineers' Account Builder

The Engineers' Account Builder starts up from the Operation History Management Setup Tool. Before starting it, the engineers' account file must be specified.

1. Start the Operation History Management Setup Tool.
   The Operation History Management Tool is started, and the Access Control tab appears.
2. In the "Refer to:" box, check that the path to the engineers' account file is displayed, and click the [Edit] button.
   The Engineers' Account Builder starts up.

SEE ALSO For more information about how to register an engineer registration file, refer to:

"■ Specifying an Engineers' Account file" on page E2-13

Defining access groups

To set up access rights for engineer groups, access groups must be defined in advance.

Creation of a new access group can be performed efficiently by copying a default access group or another existing access group and then editing its contents.

SEE ALSO For more information about default access groups, refer to:

"■ Default access groups" on page E2-21

Adding access groups

To add access groups, perform the following procedure.

1. Start the Engineers' Account Builder, and display the Access Group tab sheet.

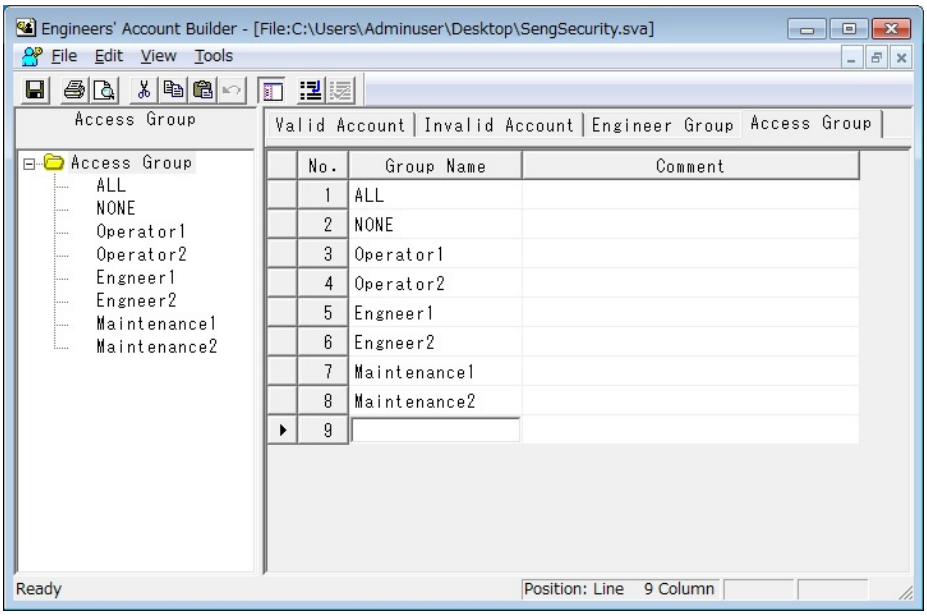


Figure E2.2.3-5 Engineers' Account Builder (Access Group tab sheet: Access Group list)

The currently defined access groups are listed.

TIP Among the access groups, ALL, NONE, Operator1, Operator2, Engineer1, Engineer2, Maintenance1 and Maintenance2 are default access groups predefined in the Builder.

2. Add a new access group to the end of the list. To create a copy of an access group that is already defined, perform the following operations.
   a. In the list, right-click the line of the access group you wish to copy, and select [Copy] from the pop-up menu. Alternatively, select a line, then select [Edit] > [Copy] from the menu bar.
   b. Right-click the blank line at the end of the list, and select [Paste] from the pop-up menu. Alternatively, select a blank line, then select [Edit] > [Paste] from the menu bar.

TIP Access groups may not only be added on the last line, but may be inserted between existing lines as well. To insert a line, select the position where you wish to insert a line in the list, and select [Edit] > [Insert Line] from the menu bar. Alternatively, select [Insert Line] from the right-click menu.

3. On the added access group line, enter the access group name and a comment.
   An access group name may be up to 16 single-byte characters. A comment may be up to 32 single-byte characters or 16 double-byte characters.

After that, set the access rights for the added access group.

Setting the rights of access groups

1. In the tree display of the Access Group tab sheet, select an access group.
   The contents of the access rights settings are listed on the right.

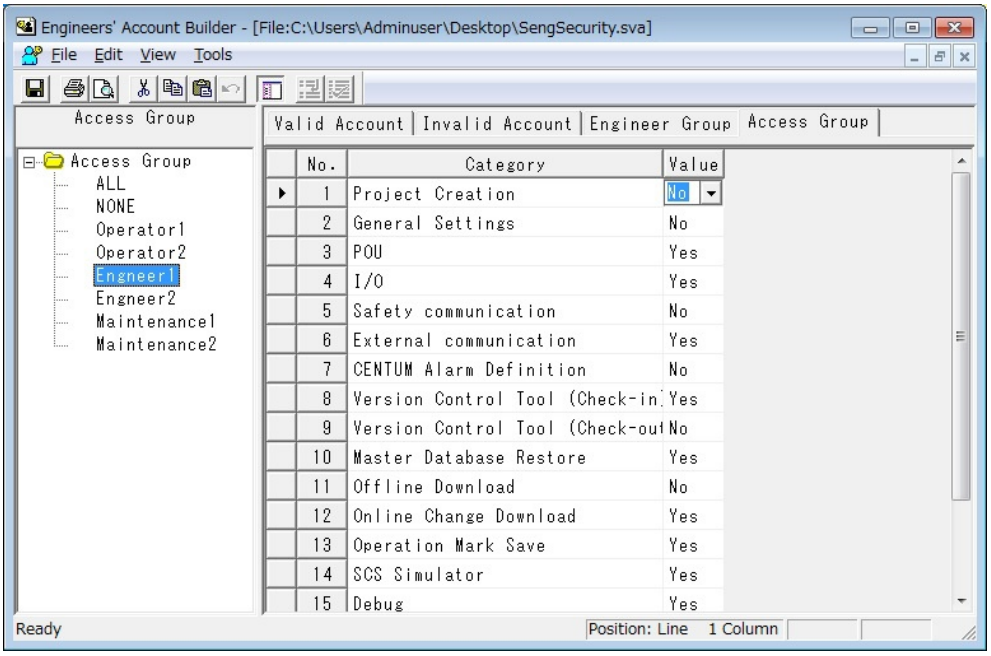


Figure E2.2.3-6 Engineers' Account Builder (Access Group tab sheet:Individual Access Group)

2. Click on the "Value" cell of each category, and select [Yes] (has rights) or [No] (does not have rights).

TIP

When the mouse pointer is placed on a category name in the list, the operations included in that category are displayed in a tooltip.

SEE ALSO

For more information about categories of access rights, refer to:

E2.5.2, “Access rights category list” on page E2-72

Deleting access groups

To delete an unnecessary access group, perform the following procedure. However, access groups that are assigned to any engineer group cannot be deleted.

1. In the tree display of the Access Group tab sheet, select the [Access Group] folder.
   Access groups are listed on the right.
2. Select the line of the access group you wish to delete, and from the right-click menu, select [Delete Line]. Alternatively, select [Edit] > [Delete Line] from the menu bar.

Saving access group definition contents

Once all of the required settings have been entered on the Access Group tab sheet, save the contents that were set.

1. From the menu bar, select [File] > [Save]. Alternatively, click the "Save" button on the toolbar.
   The new definition contents are saved to the engineers' account file.

TIP

If an access group name has been changed and that access group is assigned to an engineer group, the new access group name will be reflected in the registered information of the engineer group to which the access group is assigned.

Creating engineer groups

Once the access groups required in the system are defined, create the engineer groups. For each engineer group, assign an access group and set the range of enabled access rights defined by the access group.

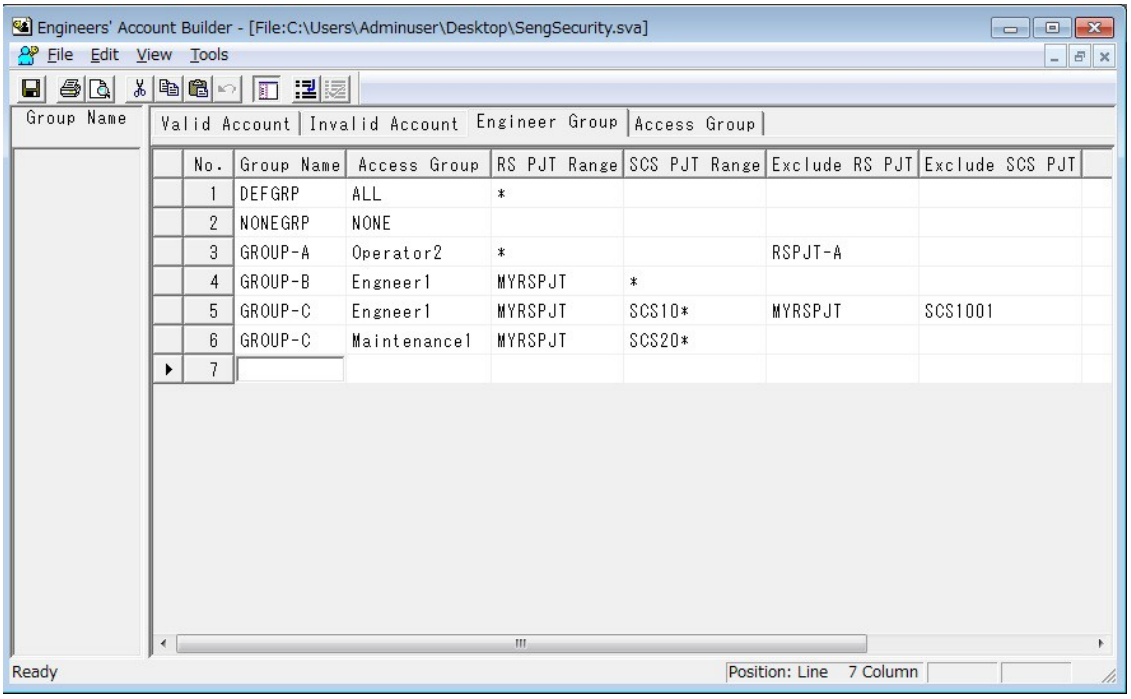


Figure E2.2.3-7 Engineer Group tab sheet

To create engineer groups, perform the following procedure.

1. Start the Engineers' Account Builder, and display the Engineer Group tab sheet.

TIP

The engineer groups DEFGRP and NONEGRP displayed in the list are the default engineer groups.

2. Click inside a cell in the "Group Name" column, and enter an engineer group name. Engineer group names may be up to 8 alphanumeric characters (not case sensitive).
3. In the combo box in the "Access Group" column, select or enter the access group you wish to assign to that engineer group.

TIP

Multiple access groups may be assigned to the same engineer group. In this case, create multiple lines with the same engineer group name, and specify different access groups on each line.

To insert a line between existing lines, right-click the position where you wish to insert it, and select [Insert Line] from the right-click menu. Alternatively, select [Edit] > [Insert Line] from the menu bar.

4. Set "RS PJT Range," "SCS PJT Range," "Exclude RS PJT" and "Exclude SCS PJT," and specify the range of enabled rights.
5. Enter comments for the engineer group if necessary. A comment may be up to 32 single-byte characters or 16 double-byte characters.
6. Similarly, create all required engineer groups.

7. Select [Save] from the [File] menu or click the "Save" button on the toolbar.
   The entered contents are saved in the engineers' account file.

After the required engineer groups are set up, engineers can be registered.

SEE ALSO For more information about items for specifying the range of enabled access rights, refer to:

"■ Range of enabled access rights" on page E2-23

For more information about examples of engineer group settings, refer to:

"■ Examples for engineer group assignment" on page E2-25

■ Registering an engineer's account

Once the access groups and engineer groups required in the system have been defined, engineers can be registered.

- An engineer name that is already registered or an engineer name that was registered and then deleted after a password was set cannot be specified. If such an engineer name is specified, an error dialog box will appear when you try to save the contents.
- Engineer names that were deleted in the past can be confirmed on the Invalid Account tab sheet.
- In Windows, upper-case and lower-case letters can be used, but in Windows authentication mode, in which the same names as Windows user names are used as engineer names, ProSafe-RS does not distinguish between upper case and lower case letters.

To register an engineer, perform the following procedure.

1. Start the Engineers' Account Builder, and display the Valid Account tab sheet.

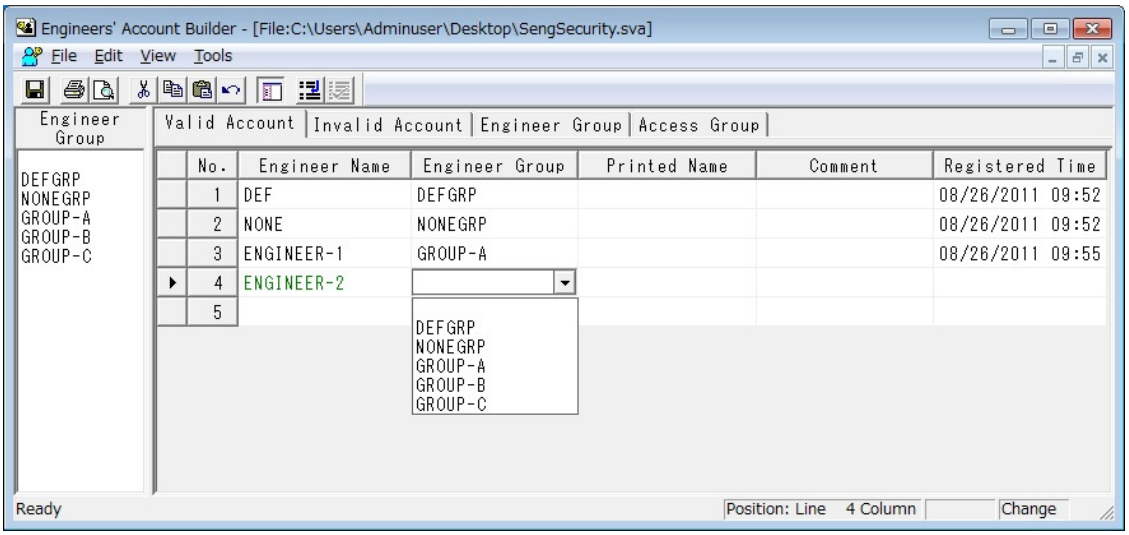


Figure E2.2.3-8 Engineers' Account Builder (Valid Account tab)

The Valid Account tab displays a list of currently registered engineers.

2. Enter the engineer name in the "Engineer Name" column on a blank line.
   Up to 16 alphanumeric characters and ASCII symbols can be specified.
   - Only uppercase characters can be used.
   - The following ASCII symbols and space characters can be used:
     ! # $ % ( ) - . ^ _ { | } ~
   - Hyphens (-) and underscores (_) may be used except as the first character.

- Names ending with a period (.) is not allowed.
- The ASCII symbols that can be used as the first characters are the following: ^ _ { | } ~

IMPORTANT

When using Windows authentication mode, make sure that the pertinent Windows user names follow the above naming rules.

3. Specify the engineer group in the "Engineer Group" column. Select an engineer group from the registered engineer group names displayed in the drop-down list.
4. In the "Printed Name" column, enter the name of the person who uses the engineer name.
   Up to 64 single-byte characters or 32 double-byte characters can be specified.
5. Enter comments in the "Comment" column.
   Up to 32 single-byte characters or 16 double-byte characters can be specified.
6. Enter all engineers in the same way.

TIP

To delete a line from the Valid Account tab sheet, select the line you wish to delete, and select [Delete Line] from the [Edit] menu.

7. For Windows authentication mode, check whether the entered engineer names exist as Windows users.
   a. From the menu bar, select [Tools] > [Check user names]. Alternatively, click the "Check user names" button in the toolbar.
      If there is an engineer name that does not exist as a Windows user, it is output in the message display area.
   b. If you wish to register an engineer name that does not exist as a Windows user, create a Windows user account of that name.
8. From the menu bar, select [File] > [Save], or click the "Save" button in the toolbar.
   The newly registered contents are saved in the engineers' account file, and the time at which the engineer was registered is displayed in the "Registered Time" column.

A password is not yet set for the newly registered engineer. The first time the engineer logs onto SENG, a dialog box for setting a password appears, and a password should be set there.

TIP

Users for local authentication:

When the system is used in a domain environment and Windows authentication mode is used, you need to create users for local authentication in order to enable log-on to SENG in an emergency situation such as when the domain controller has failed.

A user name starting with an underscore (_) is handled as a local authentication user and, for a Windows authentication, the user is authenticated on the local computer regardless of whether domain management or workgroup management is applied.

Local authentication users are not for use in normal situations. If someone attempts to log on with this user name while the domain controller is accessible, a warning message is displayed and the following message is recorded in the operation log.

Local Authentication Detected User=_xxxxxxxx

This is because there may be a problem in security if a local user account, which is for emergency use, is used while user authentication is available on the domain.

Checking invalid engineer accounts

An engineer name that was once registered and deleted after a password was set cannot be registered again. You can check such engineer names on the Invalid Account tab sheet.

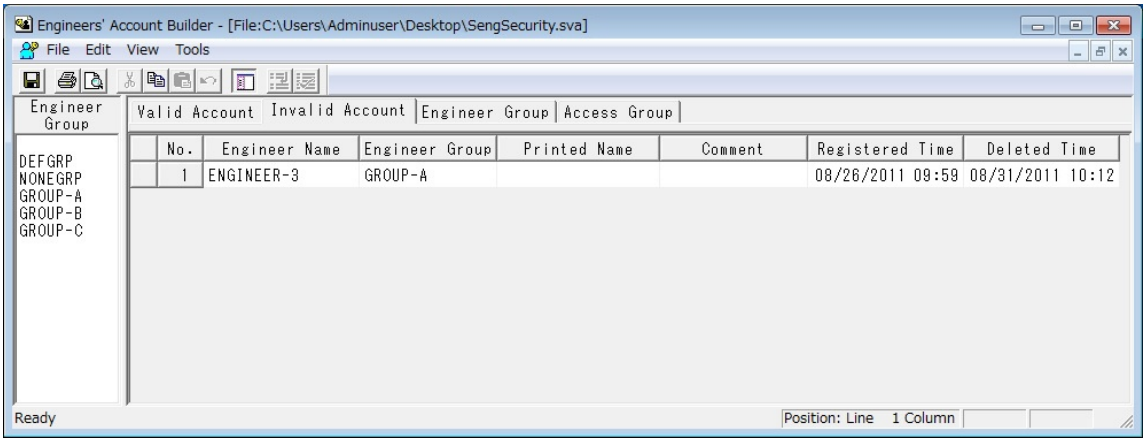


Figure E2.2.3-9 Engineers' Account Builder (Invalid Account tab sheet)

The Invalid Account tab sheet displays a list of deleted engineers. Only browsing is possible on this tab sheet, and editing cannot be performed. In addition to the information at the time of account registration, the time at which the engineer was deleted is displayed in the "Deleted Time" column.

Printing the contents set in Engineers' Account Builder

To print the contents set in the Engineers' Account Builder, perform either of the following operations.

- From the menu bar, select [File] > [Print].
- Click the "Print" button on the toolbar.

The engineer's account file name is printed in the header, and the date/time and page number are printed in the footer.

E2.2.4 Starting Operation History Management

Once the settings required for operation history management have been completed, start operation history management. Operation history management can be started in RS project units.

To start operation history management, perform the following procedure.

1. In the Operation History Management Setup Tool, display the Operation History Management tab sheet.
2. From the list, select the RS project for which you wish to begin operation history management.
3. Click the [Start Operation History Management] button.
   A dialog box for confirming start of operation history management appears.

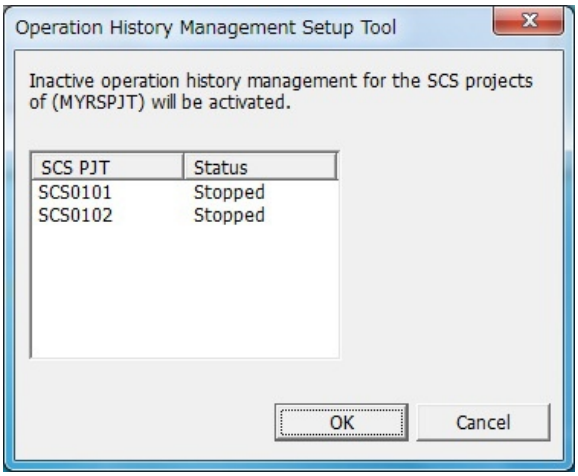


Figure E2.2.4-1 Operation History Management Start Confirmation dialog box

4. Click [OK].
   Saving of operation logs and modification files to the operation history database begins, and the operation history management start operation is logged.

TIP

- The [Start Operation History Management] button can be used when the status of the selected RS project is "Stopped" or "******". "******" means that the status of operation history management is "Running" for some SCS projects and "Stopped" for the other SCS projects that belong to the RS project.
- When operation history management is started, the newest RS project database is copied to the operation history database. For this reason, if the project database and the operation history database have become inconsistent with each other, the consistency can be recovered by starting operation history management.

E2.2.5 Window configuration of Engineers' Account Builder

This section describes the window configuration of the Engineers' Account Builder.

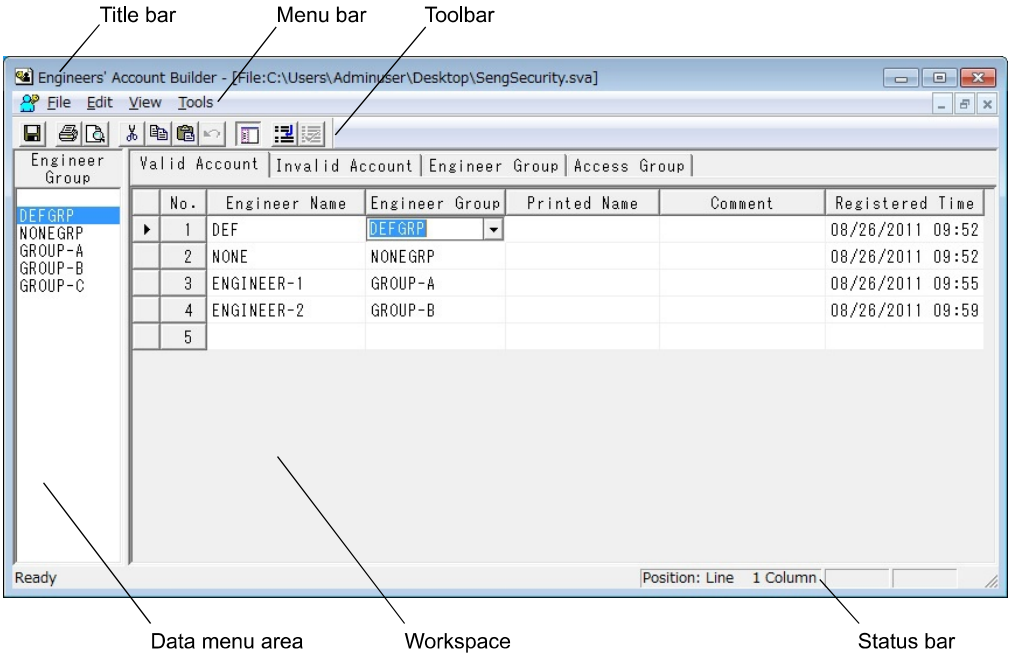


Figure E2.2.5-1 Window configuration of Engineers' Account Builder

The following tabs can be displayed in the workspace.

- Valid Account tab: Sets up engineer accounts.
- Invalid Account tab: Displays invalid engineer accounts.
- Engineer Group tab: Sets up engineer groups.
- Access Group tab: Sets up access groups.

Menu bar

This section describes the following menu bar items.

- [File] menu
- [Edit] menu
- [Tool] menu

Table E2.2.5-1 File menu

Menu Item	Description
Save	Save the contents set in the Builder into the engineers' account file.
Properties	Display the property information of the file.
Print Preview	Display the print image.
Print	Print the set contents.
Exit Builder	Close the Engineers' Account Builder.

Table E2.2.5-2 Edit menu

Menu Item	Description
Undo	Cancel the previously performed edit operation.
Cut	Delete the selected character string and copy it onto the clipboard.
Copy	Copy the selected character string onto the clipboard.
Paste	Insert the character string stored on the clipboard.
Clear	Clear the character string of the selected field.
Select All	Select all cells.
Deselect All	Cancel selected status.
Insert Line	Insert a line before the selected line.
Delete Line	Delete the selected line.
Find	Search for a character string in the set data.
Replace	Replace a character string of the set data.
Release Lockout Account	Release lockout (can be selected only in ProSafe authentication mode).
Reset Password	Reset the password (can be selected only in ProSafe authentication mode).

Table E2.2.5-3 Tool menu

Menu Item	Description
Options	Specify options.
Check User Names	Check engineer names (can be selected only in Windows authentication mode).

Toolbar

The functions of each button on the toolbar are as follows.

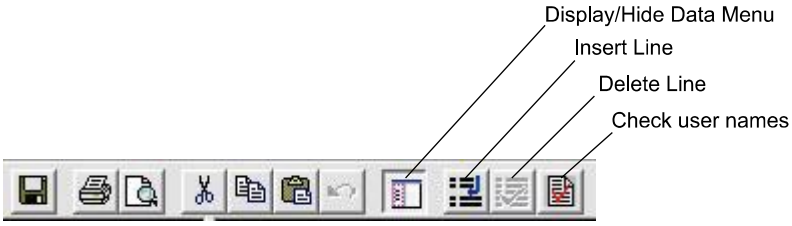


Figure E2.2.5-2 Toolbar buttons and names

Table E2.2.5-4 Functions of toolbar

Name	Description
Display/Hide Data Menu	Shows or hides the data menu area
Insert Line	Inserts a line before the selected line
Delete Line	Deletes the selected line
Check User Names	Performs engineer name check (available only in Windows authentication mode)

E2.3 Operations of SENG that use Access Control/Operation History Management

This section describes the operations of engineers and the operations of administrators in a system that uses access control/operation history management.

SEE ALSO For more information about operations that are subject to access control / operation history management, refer to:

E2.1.3, “Access Control/Operation History Management target operation list” on page E2-7

E2.3.1 Engineer operations under access control

In systems where access control/operation history management is used, when an engineer operates the SCS Manager, the various builders, the Engineering Tool or the SCS Maintenance Support Tool, logon/engineer authentication and rights checking are performed for operation control and operations are logged.

This section describes the following access control-related operations, which are performed when an engineer uses SENG.

- Logging on to SENG function
- Engineer authentication
- Operation control by rights checking
- Changing a password

Logging on to SENG function

Logon is performed to check that the engineer who attempts to start SENG operations is a registered engineer.

After starting SENG, when any of the following programs is started, a Logon dialog box appears, and the engineer name and password are requested.

- SCS Manager
- SCS Status Overview window (only when started from the Start menu)
- IOM Control Right Switching Tool
- Master Database Restoring Function
- Version Control Tool
- Message Cache Tool

TIP

After logging on to any of the above programs, logon is not required when starting any other program. In this case, a confirmation dialog box appears, showing the currently logged on engineer.

Logon operations are as follows.

1. Perform operations to start a program that requires logon.
   The Logon dialog box appears.

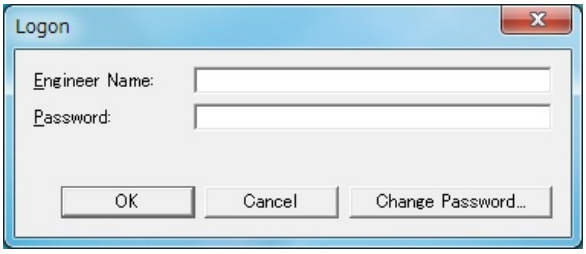


Figure E2.3.1-1 Logon dialog box (ProSafe authentication mode)

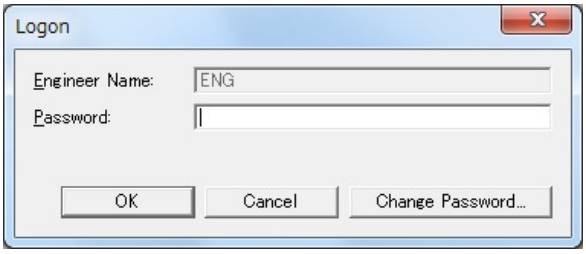


Figure E2.3.1-2 Logon dialog box (Windows authentication mode)

In the case of Windows authentication mode, the user name logged on to Windows as an engineer is displayed in gray, and cannot be changed.

2. In the case of ProSafe authentication mode, enter the engineer name and password, and click [OK]. In the case of Windows authentication mode, enter the password for the Windows user, and click [OK].
   If the engineer name and password match the registered information, the program is started.

Once work using SENG is finished, log out by closing all programs that require logon when started.

● Logon operation immediately after engineer registration

In ProSafe authentication mode, when an engineer logs on for the first time after being registered, no password is set for the engineer. In this case, perform the following operations.

1. In the Logon dialog box, enter the engineer name and click [OK].
   A dialog box that prompts password registration appears.
2. Click [OK].
   In the Password Change dialog box that appears, set a password.

   You can use up to 63 alphanumeric characters and ASCII symbols for a password.

   - Passwords are case sensitive.
   - The following ASCII symbols and space characters can be used:

     ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ { | } ~

     However, semicolons (;) are not allowed in ProSafe authentication mode.
   - In ProSafe authentication mode, passwords need to follow the password policies set with the Operation History Management Setup Tool.
   - In Windows authentication mode, passwords need to follow the password policies set for Windows.

■ Engineer authentication

Engineer authentication is performed to confirm the engineer who attempts an SENG operation that affects an actual SCS. The operation cannot be executed unless the password of the engineer logged on is entered. The operations that require engineer authentication are as follows.

- Offline Download
- Master Offline Download
- Online Change Download
- SCS Restart
- SCS Security Level Password Change
- Output Enable Operation

- Output Module Start
- IOM Download

The engineer authentication operations are as follows.

1. When any of the above operations is performed, the Engineer Authentication dialog box appears.

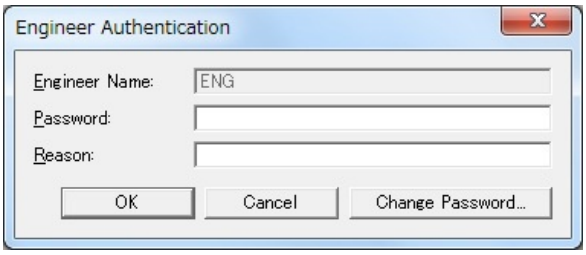


Figure E2.3.1-3 Engineer Authentication dialog box

   The name of the engineer logged on is displayed in gray in the engineer name box.

2. Enter the password and the reason for performing the operation, and click [OK].

If the engineer name and password match the registered information, the operation is executed. The "Reason" character string that was entered is recorded in the operation log.

Operations when Log-on/Engineer authentication fails

If log-on/engineer authentication fails consecutively the set number of times, an error message is displayed and an authentication error is recorded in the operation log. The behavior after an authentication error has occurred is as follows.

- If the lockout function is enabled, the engineer is locked out. The Log-on/Engineer Authentication dialog box appears even after lockout, but authentication will not succeed for the locked-out engineer name. An authentication error is not generated in this case. To release lockout, ask the administrator.
- If the lockout function is disabled, an authentication error is recorded each time the engineer enters the wrong password. If the correct password is entered, authentication is successful.

SEE ALSO For more information about setting a lockout due to an authentication failure, refer to:

"■ Settings required when ProSafe authentication mode is selected" on page E2-13

For more information about how to release a locked-out engineer, refer to:

"■ Releasing a locked-out engineer" on page E2-42

Operation control by rights checking

When an engineer attempts to perform an operation on a project database or SCS, if the engineer does not have the right to perform that operation, a warning dialog box appears and that operation cannot be performed. Or, the relevant menu may be grayed out to disable the operation.

Also, when a project is opened in SCS Manager, the following warning dialog box appears, according to the rights of the engineer.

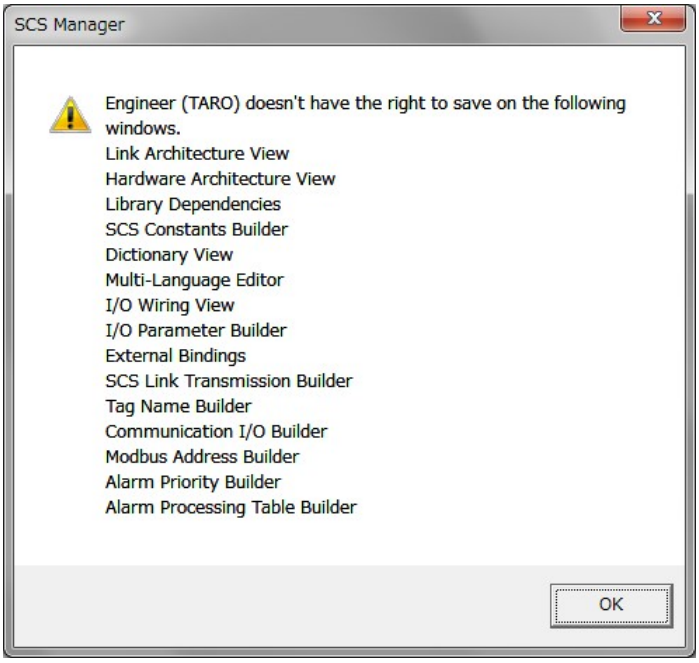


Figure E2.3.1-4 Warning dialog box when project is opened (example where all items are displayed)

Changing a password

To change the password for logon and engineer authentication, perform the following procedure.

1. Perform an operation that requires logon or engineer authentication.
   The Logon dialog box or Engineer Authentication dialog box appears.
2. Enter the engineer name and password, and click [Change Password].
   The Password Change dialog box appears.

   If the entered engineer name and password are incorrect, it results in an authentication error and the password cannot be changed.
3. Enter the new password in "New Password:" and "Confirm New Password:", and click [OK].

TIP

- If a valid period for passwords has been set, a warning dialog box appears if an operation that requires logon or engineer authentication is performed within 14 days before the end of the valid period. Change the password ahead of time.
- If the valid period for passwords has passed, the Password Change dialog box appears. Set a new password. If the password is not changed, logon/engineer authentication will fail.

SEE ALSO

For more information about characters that can be used in the password, refer to:

"● Logon operation immediately after engineer registration" on page E2-38

For more information about structuring the operation history database , refer to:

E2.5.1, "Operation history database structure" on page E2-71

E2.3.2 Operations performed by administrators

This section describes the operations performed by administrators in a system that uses access control/operation history management.

Checking the operating status of Operation History Management of each project

On the Operation History Management tab of the Operation History Management Setup Tool, it can be confirmed whether operation history management is running for each project.

To confirm the operating status of operation history management, perform the following procedure.

1. Start the Operation History Management Setup Tool.
   The Operation History Management Setup Tool starts.
2. Display the Operation History Management tab sheet, and confirm the operation history management status of RS projects in the "Status" column of the project list.

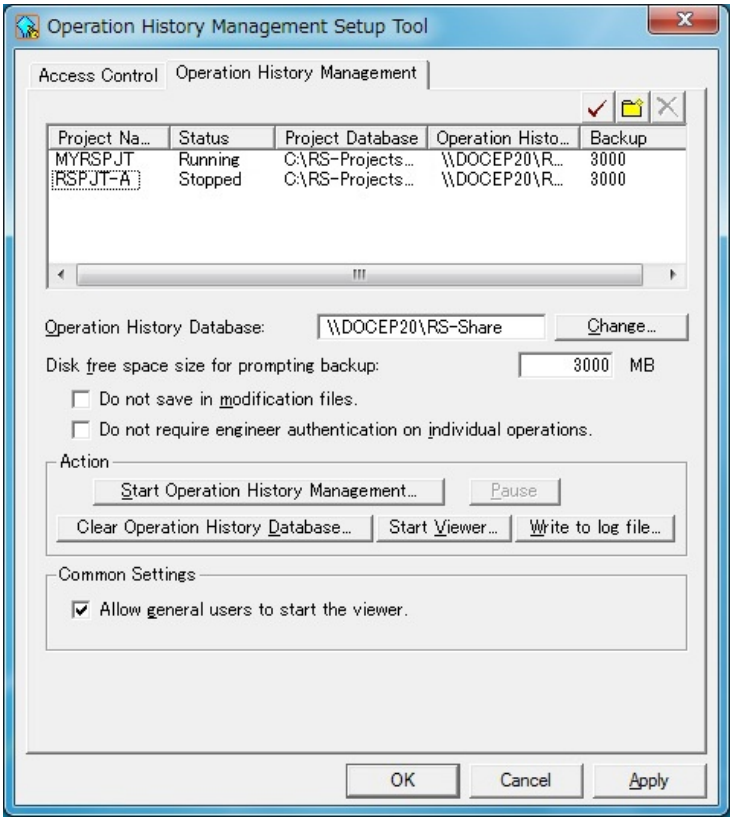


Figure E2.3.2-1 Operation History Management tab sheet

3. Except when the display in the Status column is "Running," confirm whether or not operation history management is running for each SCS project included in the RS project.
   a. Select an RS project on the project list and right-click.
   b. From the displayed pop-up menu, select [Display Details].
      The detailed statuses of the SCS projects appears.

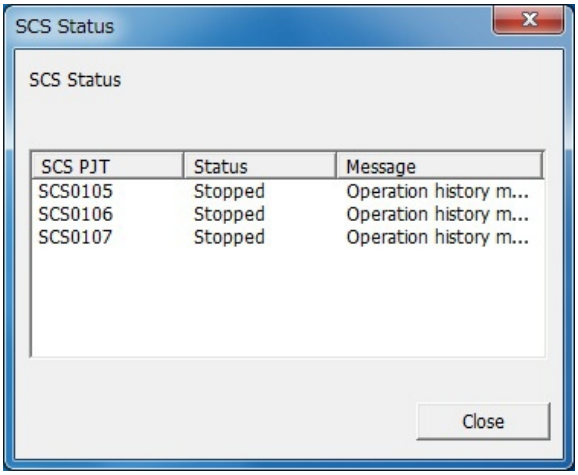


Figure E2.3.2-2 Detailed status display of SCS projects

● Operation History Management statuses of RS projects

The operation history management statuses of RS projects displayed on the Operation History Management tab of the Operation History Management Setup Tool are shown in the following table.

Table E2.3.2-1 Operation History Management statuses of RS projects

Status	Description
Running	The operation history management function is running for all SCS projects belonging to the RS project.
******	• Of the SCS projects belonging to the RS project, the operation history management function is running for some SCS projects and stopped for other SCS projects. (*1) • The RS project does not exist.
Stopped	The operation history management function has not been started or is stopped for all SCS projects belonging to the RS project.

*1: Even if operation history management was started in a batch for the RS project, subsequent actions of copying SCS project and adding it to RS project will result in a mix of SCS projects, some with operation history management running and some with operation history management not running.
When a SCS project is newly generated and added to a RS project, the RS project in the state of running allows the added SCS project to run.

● Messages displayed in the SCS Detailed Status dialog box

In the SCS Detailed Status dialog box, the following two types of messages are displayed in the Message column of SCS projects whose status is "Stopped."

Table E2.3.2-2 Messages displayed in the SCS Detailed Status dialog box

Message	Description
Inconsistent with the operation history database.	Inconsistent with the operation history database. In this case, to recover consistency, start operation history management for the RS project that includes this SCS.
Operation history management is not set up.	Operation history management has not been started.

■ Releasing a locked-out engineer

An engineer who has failed in logon or engineer authentication consecutively the set number of times is locked out. The administrator releases locked-out engineers as necessary.

In ProSafe authentication mode

Lockout is released on the Valid Account tab sheet of the Engineers' Account Builder.

On the Valid Account tab sheet, an asterisk (*) is displayed next to the names of locked-out engineers, and the setting contents of those engineers cannot be changed.

To release locked-out engineers, perform the following procedure.

1. Start the Operation History Management Setup Tool.
2. Click the [Edit] button on the Access Control tab sheet.
   The Engineers' Account Builder is started.
3. On the Valid Account tab sheet, select the line of the engineer you wish to release from lockout. Multiple lines can be selected.
4. From the [Edit] menu, select [Release Lockout Account].
5. A dialog box appears to confirm lockout release, beginning at the top, for locked-out engineers among the selected engineers. To release lockout, click [OK].

When lockout is released, the asterisk next to the engineer name is deleted, and the contents of that line can be changed.

In Windows authentication mode

When in Windows authentication mode, release locked-out users by management tools on the Windows side. Note that in the Engineers' Account Builder, an asterisk (*) is not displayed next to locked-out engineers.

Resetting a password

This section describes the procedure for resetting an engineer's password when in ProSafe authentication mode. When in Windows authentication mode, reset the password using management tools on the Windows side.

1. Start the Operation History Management Setup Tool.
2. Click the [Edit] button on the Access Control tab sheet.
   The Engineers' Account Builder is started.
3. In the Valid Account tab sheet, select the line of the engineer whose password you wish to reset (multiple lines may be selected).
4. From the menu bar, select [Edit] > [Reset Password].
   A dialog box appears to confirm password reset, beginning at the top for the selected engineers.
5. To reset the password, click [OK].

Writing comments to Operation log files

Log entries of any character strings may be written to the operation log files of a specified project. The written comments may be viewed as operation logs in the Operation History Database Viewer.

To write a comment to an operation log file, perform the following procedure.

1. Start the Operation History Management Setup Tool, and display the Operation History Management tab sheet.
2. Select an RS project from the list and click the [Write to log file] button.
   The following dialog box appears.

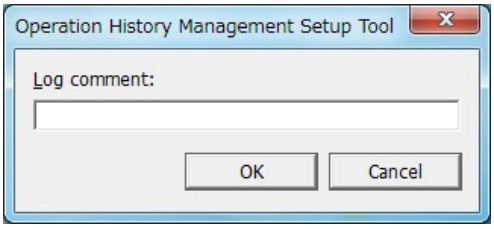


Figure E2.3.2-3 Log Writing dialog box

3. Enter a comment.
   A comment may be up to 64 single-byte characters or 32 double-byte characters.
4. Click [OK].
   The comment is written to the operation log file.

Backing up

Creating a backup copy of operation history database has to be performed manually.

IMPORTANT

Browsing a backup copy of operation history database also requires a backup copy of the target RS project for the operation history management. You must perform backup both of them. Please note that you will no longer be able to browse the contents in the operation history database of a SCS project once you delete the SCS project in RS project. When you wish to delete a SCS project, ensure to make a backup copy of the relative RS project so that you can browse the backup copy of the operation history database later.

Steps to backup

1. Using Windows Explorer, create backup copies of the top folder and all its subfolders of the operation history database into an auxiliary storage device. This operation allows you to backup the entire operation log database and modification file database.
2. Stop the operation history management.
3. Delete modification file database by means of the operation history setup tool. Since the operation log database remains untouched, the entire operation logs can be shown in the viewer.
4. Create a backup copy of the target RS project for the operation history management into an auxiliary storage device.
5. Restart the operation history management.

Operations when warning message prompting backup appears

When you perform an operation that causes saving of modification files or operation log, a warning message prompting backup of the operation history database may appear. If such message appears, make a backup of the operation history database, and delete the operation history management data saved in SENG.

Normally, free disk space can be secured by deleting only the modification files in the operation history database. By the following procedure, only the modification files are deleted, so you can still view all operation logs in the viewer after the deletion.

When a warning message prompting backup is displayed, perform the following procedure.

1. Using Windows Explorer, copy the top folder and all its subfolders of the operation history database to an auxiliary storage device.

By so doing, the entire operation log database and modification file database are backed up.

2. Start the Operation History Management Setup Tool, and display the Operation History Management tab sheet.
3. For each RS project, perform the following steps to stop operation history management, delete modification files, and then resume operation history management.
   a. Select an RS project on the project list and click the [Pause] button.
      Operation history management of the selected RS project stops.
   b. Click the [Clear Operation History Database] button.
      The following dialog box appears.

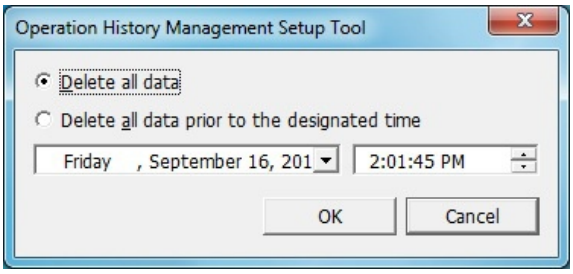


Figure E2.3.2-4 Delete Operation History Database dialog box

   c. To delete all modification files, select "Delete all data." To delete only the modification files prior to a specified time, select "Delete all data prior to the designated time," and enter the date and time.
   d. Click [OK].
      The selected modification files of the RS project are deleted.
   e. Click the [Start Operation History Management] button to resume operation history management of the RS project.
4. Repeat the above procedure, and delete the modification files for all RS projects.

SEE ALSO For more information about how to browse the data of a backed-up operation history database, refer to:

E2.4.3, “Steps to browse backed-up operation history database” on page E2-67

Initializing the Operation History Database

The procedure for initializing the operation history database and starting operation history management with a new operation history database in the same location will be described. By this procedure, all operation log files and modification files accumulated on the PC are deleted.

To initialize the operation history database and restart operation history management, perform the following procedure.

1. Start the Operation History Management Setup Tool, and display the Operation History Management tab sheet.
2. Select the RS project from the project list and click the [Pause] button.
   Operation history management of the selected RS project stops.
3. Similarly, stop operation history management of all RS projects.
4. To make a backup, using Windows Explorer, copy the top folder of the operation history database and all its subfolders to an auxiliary storage device.
5. Using Windows Explorer, delete all folders and files under the top folder of the operation history database of the RS project for which operation history management was stopped.

6. On the Operation History Management tab sheet, select the RS project, and click the [Start Operation History Management] button to restart operation history management.
7. Similarly, restart operation history management of all RS projects.

After operation history management is restarted, the serial numbers of the operation logs start at one.

■ Adding an engineer

To add an engineer, register the engineer's account on the Valid Account tab sheet of the Engineers' Account Builder.

SEE ALSO For more information about how to register the account of an engineer, refer to:

"■ Registering an engineer's account" on page E2-30

■ Deleting an engineer

Deletion of engineers is performed on the Valid Account tab sheet of the Engineers' Account Builder.

To delete engineers, perform the following procedure.

1. Start the Operation History Management Setup Tool.
2. Click the [Edit] button on the Access Control tab sheet.
   The Engineers' Account Builder is started.
3. On the Valid Account tab sheet, select the line of the engineer name you wish to delete, and select [Delete Line] from the [Edit] menu.
   The selected line is deleted.
4. Select [Save] from the [File] menu.
   The changed contents are saved in the engineers' account file, and the deleted engineer's account becomes invalid.

IMPORTANT

If you delete a registered engineer for whom a password is already set, that engineer name is deleted from the table on the Valid Account tab, and is added to the Invalid Account tab. It cannot be completely deleted from the database. An engineer name of this type cannot be registered again.

■ Changing an engineer's rights

To change the rights of a registered engineer, the following operations may be required.

- Change the engineer group to which the engineer belongs.
- Change the access group assigned to the engineer group.
- Change the range/exclusion range of RS projects/SCS projects assigned to the engineer group.
- Change the access group definitions.

Perform these operations in accordance with the rights to be changed.

SEE ALSO For more information about how to change the above settings in order to change the rights of an engineer, refer to:

E2.2.3, "Registering engineers" on page E2-19

Operations when inconsistency is detected between project and operation history database

When the Operation History Management tab sheet of the Operation History Management Setup Tool is displayed, consistency between the project and operation history database is checked. If an inconsistency is detected, the following message is displayed.

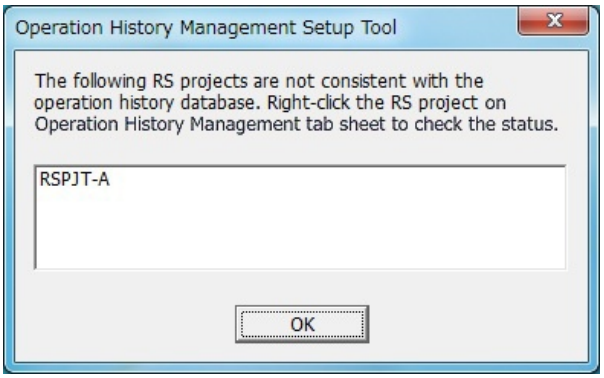


Figure E2.3.2-5 Message when inconsistency detected (Example)

Perform the following procedure to resolve the database inconsistency.

1. On the Operation History Management tab sheet, check the status of the RS projects displayed in the preceding message and the detailed status of their SCS projects.
2. Select an applicable RS project on the project list and click the [Start Operation History Management] button.

TIP

If the [Start Operation History Management] button is grayed out and disabled, click the [Pause] button to stop operation history management of the selected RS project, and then click the [Start Operation History Management] button.

SEE ALSO

For more information about checking the status of an RS project and the detailed status of the SCS, refer to:

"■ Checking the operating status of Operation History Management of each project" on page E2-41

Tasks required after adding, moving or deleting a project database

When the database of a project that is the target of operation history management is moved, or when an SCS project is added or deleted, the project database and the operation history database become inconsistent with each other. Also, operation history management is not executed for the added or moved SCS project.

IMPORTANT

A project for which operation history management is performed and the operation history database must be associated with each other. If not correctly associated, operation history management will not work. The following operations must be performed after adding, moving or deleting a project database.

For operation history management to be executed correctly, the following operations are required on the Operation History Management tab sheet of the Operation History Management Setup Tool.

- If an RS project was added

After adding the added RS project as a target of operation history management and performing the required setup, start operation history management.

- If an RS project for which operation history management was already being executed was moved
  After temporarily deleting the RS project as a target of operation history management and then adding it anew and performing the required setup, start operation history management.
- If an RS project was deleted
  Delete the deleted RS project as a target of operation history management.
- If an SCS project was added, moved or deleted
  For an RS project for which operation history management was already being executed, after an SCS project has been added, moved or deleted, stop operation history management of the RS project that includes that SCS project, and then start operation history management again.

SEE ALSO For more information about how to add or delete an RS project as a subject of operation history management and settings related to the operation history management, refer to:

E2.2.2, “Setup related to Operation History Management” on page E2-15

For more information about how to stop or start operation history management, refer to:

“■ Stopping/Resuming Operation History Management” on page E2-49

■ Tasks required after changing user authentication mode

This section describes the operations required after changing the user authentication mode. Note that the engineer's account information does not change if the user authentication mode is changed.

● When changed from ProSafe authentication mode to Windows authentication mode

The Windows password policy and user lockout settings are applied. The status of a user who has been locked out is not inherited.

- Execute an engineer name check to clear out the names that are not registered in Windows, and set up accounts if necessary.
- Since passwords are not inherited, set up passwords in Windows.
- If you wish the status of locked out users to continue, set this up in management tools on the Windows side.

● When changed from Windows authentication mode to ProSafe authentication mode

Password policy and user lockout settings must be set anew on the ProSafe-RS side. The status of a user who has been locked out is not inherited.

- In the operation history management setup tool, perform password policy and user lockout settings.
- Set a password when your are prompted to when logging onto the SENG function for the first time.

SEE ALSO For more information about how to set up password policies and user lockout unique to ProSafe-RS, refer to:

“■ Settings required when ProSafe authentication mode is selected” on page E2-13

Checking engineer names in Windows authentication mode

In Windows authentication mode, engineer names registered on the builder must be registered as Windows users.

To check whether or not a registered engineer name exists as a Windows user, perform the following procedure.

1. Start the Operation History Management Setup Tool.
2. Click the [Edit] button on the Access Control tab sheet.
   The Engineers' Account Builder is started.
3. From the start menu, select [Tools] > [Check user names].
   Engineer names that do not exist as Windows users are output in the message display area.

If there is a user name that does not exist, create a user account in Windows.

Stopping/Resuming Operation History Management

You must stop history management before backing up or deleting the operation history database, and resume it after you finish the task. Operation history management can be stopped/resumed for each RS project individually.

Stopping Operation History Management

1. Start the Operation History Management Setup Tool, and display the Operation History Management tab sheet.
2. On the project list, select the RS project for which you wish to stop operation history management and click the [Pause] button, and then click [OK].

After the stopping operation log is recorded, saving of the operation logs and modification files stops.

Resuming Operation History Management

The operations are the same as starting operation history management.

1. In the project list of the Operation History Management tab sheet, select the RS project for which operation history management is to be resumed, and click the [Start Operation History Management] button.
2. In the confirmation dialog box, click [OK].

Saving of operation logs and modification files to the operation history database begins, and the operation history management start operation is logged.

Steps to update at PC failures

Updating a PC where Operation History Management function is running

When you wish to replace a PC where operation history management is performed due to PC failures, register operation history database of the relative RS project on the restored PC by means of the operation history setup tool and then restart the operation history management.

Updating a PC where operation history database is implemented

When you wish to replace a PC where operation history database is implemented due to PC failures, create a shared folder "RS-Share" in the replacement PC, perform IT security tool and then perform the following steps to start operation history management by means of operation history setup tool in a PC where operation history management function runs.

- When you wish to create new operation history database:
  1. If operation history management is being performed for an RS project, you need to remove its registration.
  2. Register the location of RS project and operation history database again.
  3. Start operation history management.
- When you wish to use a backup copy of the operation history database:
  1. If operation history management is being performed for an RS project, you need to remove its registration.
  2. Restore the operation history database to the original location.
  3. Register the location of RS project and operation history database again.
  4. Start operation history management.

E2.4 Browsing operation history data

Operation history data such as operation logs and modification files saved in the operation history database can be browsed in the Operation History Database Viewer and Modification Files Viewer.

IMPORTANT

By default, only administrators can browse operation history data. To also enable general engineers to browse operation history data, perform the following settings in the Operation History Management Setup Tool.

SEE ALSO For more information about how to allow browsing of operation history data by general engineers, refer to:

"■ Permission to start Operation History Database Viewer" on page E2-17

■ Functions of Operation History Database Viewer

The Operation History Database Viewer is for browsing operation logs in the operation history database, and has the following functions.

- List display of operation logs
- Searching of operation logs
- Sorting of operation logs
- Displaying details of operation logs
- Printing of operation logs
- Exporting of operation log lists to CSV files
- Startup of the Modification Files Viewer

■ Functions of Modification Files Viewer

The Modification Files Viewer is a viewer for browsing modification files in the operation history database, and has the following functions.

- Displaying the modification files database tree
- Searching modification files
- Acquiring modification files
- Displaying the contents of modification files
- Displaying differences of modification files
- Printing modification files

E2.4.1 Browsing and printing operation logs

This section describes how to browse and print operation logs saved in the operation history database in the Operation History Database Viewer, and information recorded in operation logs.

Starting the Operation History Database Viewer

The Operation History Database Viewer can be started up from the Windows Start menu or from the Operation History Management Setup Tool.

Startup from the Windows Start menu

A general engineer can start up by this method only when the "Allow general users to start the viewer" check box is selected in the Operation History Management Tool.

1. Start the Operation History Database Viewer.
   The Project Selection dialog box appears.

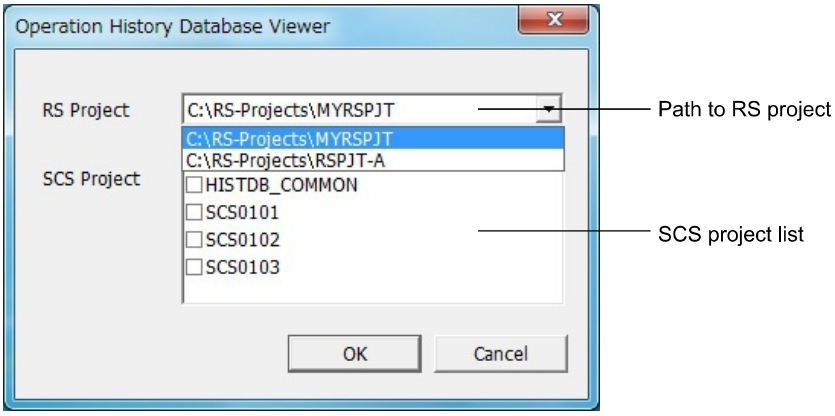


Figure E2.4.1-1 Project Selection dialog box (If started from Windows Start menu)

2. From the "RS Project" drop-down list, select the path of the RS project.
3. In the "SCS Project" box, a list of the SCS projects of the selected RS project and "HISTDB_COMMON" (common operation log) are displayed. Select the check box of the item for which you wish to display the operation log. Multiple check boxes may be selected.

TIP

The common operation log is an operation log of the operations that do not depend on the RS project or SCS project, among the operations performed by SENG. For example, startup of the SCS Manager or startup of the SCS Status Overview window apply to the common operation log.

4. Click [OK].
   The Operation History Database Viewer is started, and the operation logs are displayed as a list.

Starting up from the Operation History Management Setup Tool (administrator only)

Because the Operation History Management Setup Tool can be started up only by administrators, general engineers cannot use this method.

1. Start the Operation History Management Setup Tool.
   The Operation History Management Setup Tool starts.
2. Display the Operation History Management tab.
3. Select an RS project from the RS project list and click the [Start Viewer] button.
   The Project Selection dialog box appears.

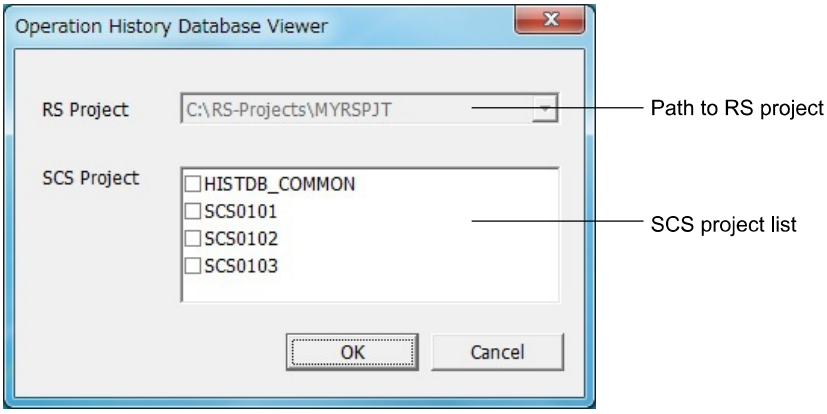


Figure E2.4.1-2 Project Selection dialog box (If started from Operation History Management Setup Tool)

4. In the "SCS Project" box, a list of the SCS projects of the selected RS project and "HISTDB_COMMON" (common operation log) are displayed. Select the check box of the item for which you wish to display the operation log. Multiple check boxes may be selected.

5. Click [OK].
   The Operation History Database Viewer is started, and the operation logs are displayed as a list.

Browsing operation logs

When the Operation History Database Viewer is started, the operation logs of the RS projects/SCS projects specified at startup are listed. If multiple SCS projects have been specified, multiple windows open, one for each SCS project.

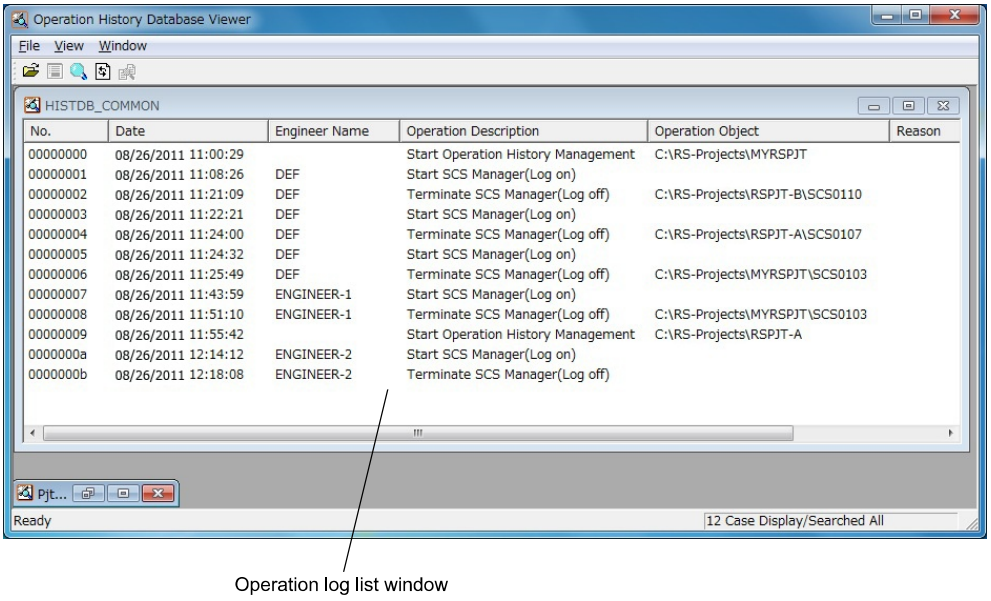


Figure E2.4.1-3 Operation History Database Viewer

SEE ALSO For more information about information recorded in the operation log, refer to:

E2.5.3, “Information recorded in operation logs” on page E2-76

Specifying SCS projects and displaying operation logs

To display a list of operation logs of another SCS project after the Operation History Database Viewer has been started up, perform the following procedure.

1. From the menu bar, select [File] > [Open], or click [Open] button on the toolbar.
   The Project Selection dialog box appears.
2. From the "RS Project" drop-down list, select the path of the RS project.
3. In "SCS Project:", select the check box of the SCS project for which you wish to display the operation log.
4. Click [OK].
   A new window opens, and the operation log of the specified SCS project appears.

Displaying properties

The following information can be displayed for operation logs displayed in the active window in the Operation History Database Viewer.

- SCS project path name
- Path to the top folder of the operation history database
- Date and time of the oldest log
- Date and time of the newest log
- Number of logs

1. Make the window in which you wish to display properties active, and select [Properties] on the [File] menu.

Specifying the number and range of operation logs to be displayed

To specify the number and range of operation logs to be displayed, perform the following procedure.

1. From the menu bar of the Operation History Database Viewer, select [View] > [Settings] or click [Settings] in the toolbar.
   The Display Settings dialog box appears.
2. On the Display tab, specify the maximum number of displayed items and the position to start the search.
   Up to 65535 can be entered as the maximum number of displayed items. (Set value when viewer is started for the first time: 1000.) When "Newest First" is selected as the search direction, results are displayed starting from the newest, and when "Oldest First" is selected, results are displayed starting from the oldest until the maximum number to display the operation logs specified here. (Set value when viewer is started for the first time: Newest First.)

Operation log filtered display

Filter conditions can be set in the Display Settings dialog box so that only operation logs that match the conditions are displayed. When multiple conditions are set, only operation logs that match all conditions are displayed. Note that when the viewer is started, no filters are set.

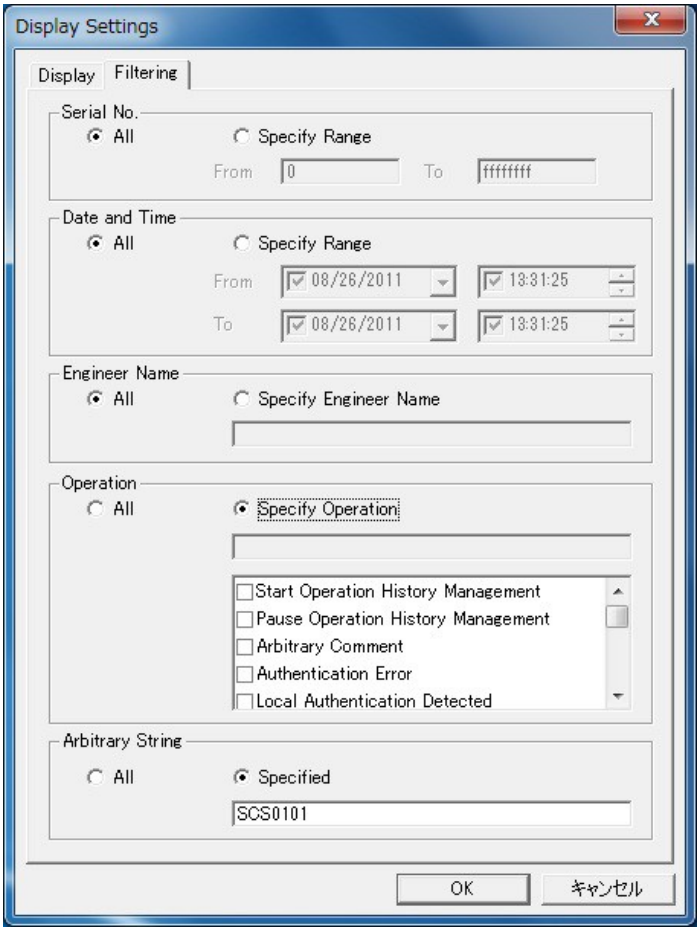


Figure E2.4.1-4 Display Settings dialog box (Filtering tab sheet)

The conditions that can be specified are shown in the following table.

Table E2.4.1-1 Filtered display conditions

Filter Condition	Description
Serial number	A range of serial numbers (8-digit hexadecimal numbers) can be specified. When a range is specified, specification of either the lowest number or the highest number can be omitted.
Date and time	A range of dates and times can be specified. When a range is specified, specification of either the earliest date or the latest date can be omitted.
Engineer name	When specifying multiple items, separate them by a space.
Operation description	Multiple operations can be selected by check boxes.
Arbitrary string	Any character string can be specified. Wildcards may not be used. When the specified character string is contained in any of the following items in an operation log, that operation log is considered to have matched the condition. Computer name, engineer name, font, program name, object of operation, reason (serial number, date/time and result of operation are not search targets).

To display filtered operation logs, perform the following procedure.

1. From the menu bar, select [View] > [Settings], or click Settings button in the tool bar.
   The Display Settings dialog box appears.
2. Set up the filter conditions on the Filtering tab
3. Click [OK].
   The search begins, and a list of operation logs that match all filter conditions appears.

TIP

During search, the Searching dialog box is displayed. When [Cancel] is clicked, the search results up to that point are displayed.

At the point when all operation logs in the operation history database have been searched, or the number of operation log search results has reached the maximum number of displayed items specified as a display condition, the search ends and the search results are displayed.

At this time, if all operation logs in the operation history database have been searched, the following is displayed on the bottom right of the Operation History Database Viewer.

"874 Case Display/Searched All"

If the maximum number of displayed items (1000) has been reached and there are still unsearched operation logs remaining, the following is displayed.

"1000 Case Display/Not Searched All"

Updating the display

To update the operation log list display, select [View] > [Update] from the menu bar. Alternatively, click [Update] on the toolbar.

The operation logs are searched again under the conditions set in the Display Settings dialog box, and the display is updated.

Sorting operation logs

Click an header item in the operation log list.

The operation logs currently displayed are sorted in the order of that item.

Each time the header item is clicked, the sorted list switches between ascending and descending orders.

Displaying operation log details

To display the detailed contents of the operation log, double-click an operation log. Alternatively, right-click an operation log, and select [Details] from the pop-up menu.

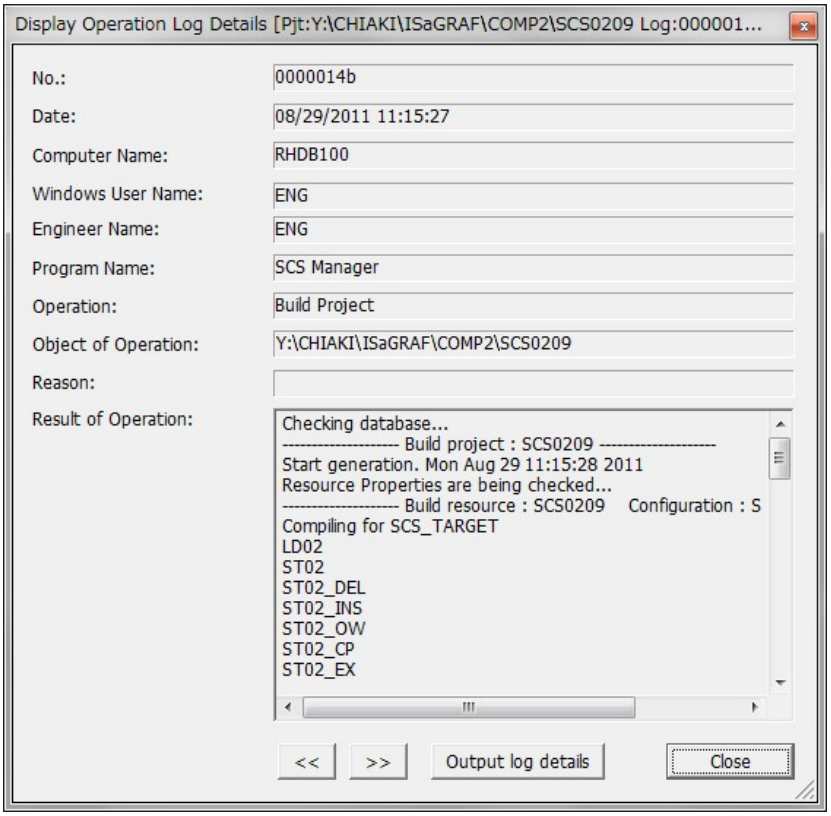


Figure E2.4.1-5 Display example of operation log detail display dialog box

The Operation Log Detail Display dialog box appears.

When [>>] is clicked, the details of the next operation log are displayed.

When [<<] is clicked, the details of the previous operation log are displayed.

When [Output log details] is clicked, the detailed information of the operation log is output to a file.

Saving operation logs to a file

The list of operation logs displayed in the viewer and detailed information can be saved to a file.

Outputting operation log list to a file

Perform this procedure to output the operation log list displayed in the viewer to a CSV text file.

1. From the menu bar, select [File] > [Export] > [Output log overview].
   The File Selection dialog box appears.
2. In the File Selection dialog box, specify the save destination file path, and click [Save].
   An example of output is shown as follows.

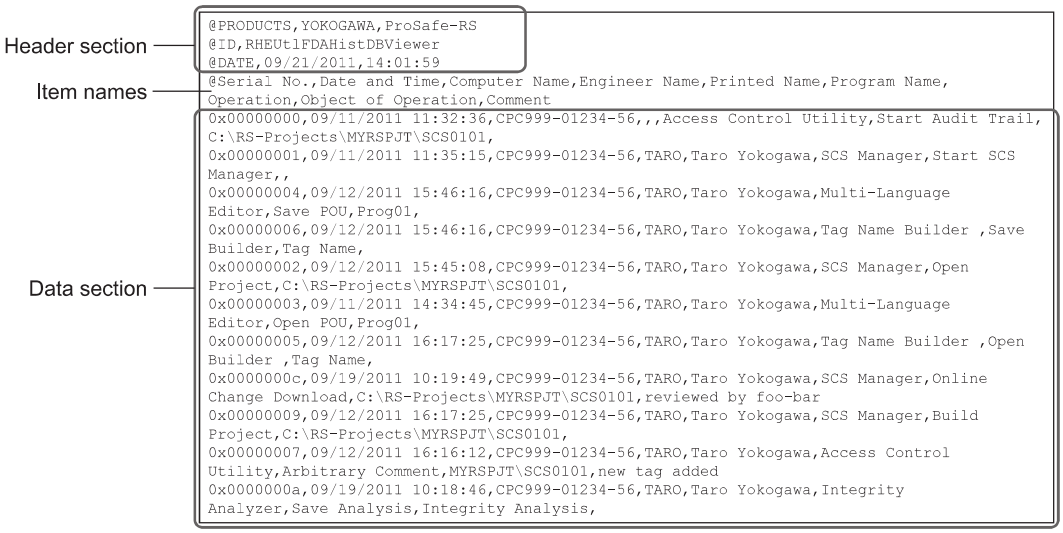


Figure E2.4.1-6 Example of operation log list output

Outputting operation log detailed information to a file

Detailed information of operation logs can be output in .rtf format or .txt format.

This section describes how to output the detailed information of all the listed operation logs.

1. Display a list of operation logs. If multiple windows that display operation logs have been opened, activate the window of the operation log you wish to output.
2. From the [File] menu, select [Export] > [Output log details].
   The File Selection dialog box appears.
3. Specify the file name and file format (.rtf or .txt) of the output destination, and click [OK].
   The detailed information of all the displayed operation logs is output to the file in the same order as the list display.

Printing operation logs

This section describes how to print the contents of the operation log list and detailed information.

Printing an operation log list

1. Display a list of operation logs. If multiple windows that display operation logs have been opened, activate the window of the operation log you wish to print.
2. Choose [Print] from the [File] menu.
   The Print dialog box appears.
3. Specify the printer in the Print dialog box, and click [OK].
   The contents displayed in the Operation Log List Display window are printed.

Printing detailed information of operation logs

To print detailed information of operation logs, output the detailed information data to a file in .rtf format or .txt format, and print them using the general print function.

E2.4.2 Browsing and printing modification files

This section describes how to browse and print modification files saved in the operation history database in the Modification Files Viewer.

Overview of Modification Files Viewer

In the Modification Files Viewer, you can look into the saved modification files from the following viewpoints.

- Modification files associated with a certain operation log
- By type of modification file

By searching for modification files by operation log serial number, modification files associated with a specific operation log can be found. Modification files are stored by type in folders in the database, and by selecting a folder in the tree display, modification files of the same type saved up to that point can be displayed in a list.

The modification file contents can be browsed in the following two formats.

- Detailed display
- Detailed difference display

When a modification file is opened in the Modification Files Viewer, a builder or the Multi-language Editor starts up in "viewer mode" according to the type of the modification file, and the contents are displayed. In viewer mode, the contents of files cannot be edited or saved. For modification files that cannot be displayed in a builder or the Multi-language editor, a dedicated viewer is started up.

About modification files

Modification files are the files that store information that was changed in a project database when an engineer executed an operation.

One or multiple modification files can correspond to one operation corresponding to a certain operation log (that is, serial number). There are also operations for which no corresponding modification file exists.

Modification files list

The types of modification files are as follows:

Table E2.4.2-1 Types of modification files

Data Hierarchy	Type	Description	Content Display Tool (*1)
Project	ProjectProp	Project properties information	Dedicated viewer
	DefinedWords	Defined words information	Dedicated viewer
Configuration	ConfigurationProp	Configuration properties information	Dedicated viewer
	SCSProjectProp	SCS project properties information	Dedicated viewer
	StnDef	SCS Constants Builder definition information	SCS Constants Builder

Continues on the next page

Table E2.4.2-1 Types of modification files (Table continued)

Data Hierarchy	Type	Description	Content Display Tool (*1)
Resource	ResourceProp	Resource properties information	Dedicated viewer
	GlobalVariables	Global variables information	Dedicated viewer
	IODev	I/O module information	Dedicated viewer
	IOMDefSB	I/O parameters	I/O Parameter Builder
	CommIO	Communicaiton I/O definition information	Communication I/O Builder
	ModbusDef	Modbus address definition information	Modbus Address Builder
	DNP3Def	DNP3 communication definition information	DNP3 Communication Builder
	LinkTrans	Link transmission definition information	Link Transmission Builder
	Binding	Binding information	Dedicated viewer
	Tag	Tag name definition information	Tag Name Builder
	AlmPri	Alarm priority level definition information	Alarm Priority Builder
	AlmTbl	Alarm processing table definition information	Alarm Processing Table Builder
	ResourceContent	POU list information/POU property information	Dedicated viewer
	LocalVarsParams	Local variables/parameters information	Dedicated viewer
POU	Source	POU logic information	Multi-language Editor

*1: The tool started up when the file contents are displayed in Modification Files Viewer. The builder and Multi-language Editor are started up in viewer mode.

Timing of saving modification files

Modification files are normally saved at the point when a download operation has succeeded.

The operation by which modification files are saved and the types of saved modification files are shown as follows.

Table E2.4.2-2 Operation by which modification files are saved

Operation Name	Type of Saved Modification File	Remarks
Create New Project	All modification files.	
Open Project	Modification files added by upgrading.	Saved when first opened after upgrading if any files have been added by upgrading.
Import SCS Manager	Modification files corresponding to modified information.	
Build	Modification files corresponding to modified information.	Saved only for user-defined projects.
Offline Download	Modification files corresponding to modified information.	
Online Change Download	Modification files corresponding to modified information.	
Master Database Restoring	All modification files.	
Version Control Check Out	All modification files.	Saved only when check-out destination is a target of operation history management.

Continues on the next page

Table E2.4.2-2 Operation by which modification files are saved (Table continued)

Operation Name	Type of Saved Modification File	Remarks
Start Operation History Management	When operation history management is started for the first time: All modification files. Otherwise: Modification files corresponding to modified information.	

TIP

- If you do not wish to save modification files, select the "Do not save in modification files" check box on the History Management tab of the Operation History Management Setup Tool. By default, modification files are saved.
- If you perform saving in a builder without making any modifications or if you set, change, or delete the password of a POU, the operation is also considered as a modification and saved as a modification file.

Browsing modification files

This section describes operations for starting the Modification Files Viewer and browsing modification files. The Modification Files Viewer is started up from the Operation History Database Viewer.

Starting the Modification Files Viewer

To browse modification files, perform the following procedure.

1. Select one operation log in the operation history database.
2. From the menu bar, select [View] > [View Modification Files]. Alternatively, click [Start Modification Files Viewer] button on the toolbar.
3. When the dialog box for entering the project password appears, enter the project password and click [OK].
   The Modification Files Viewer starts.

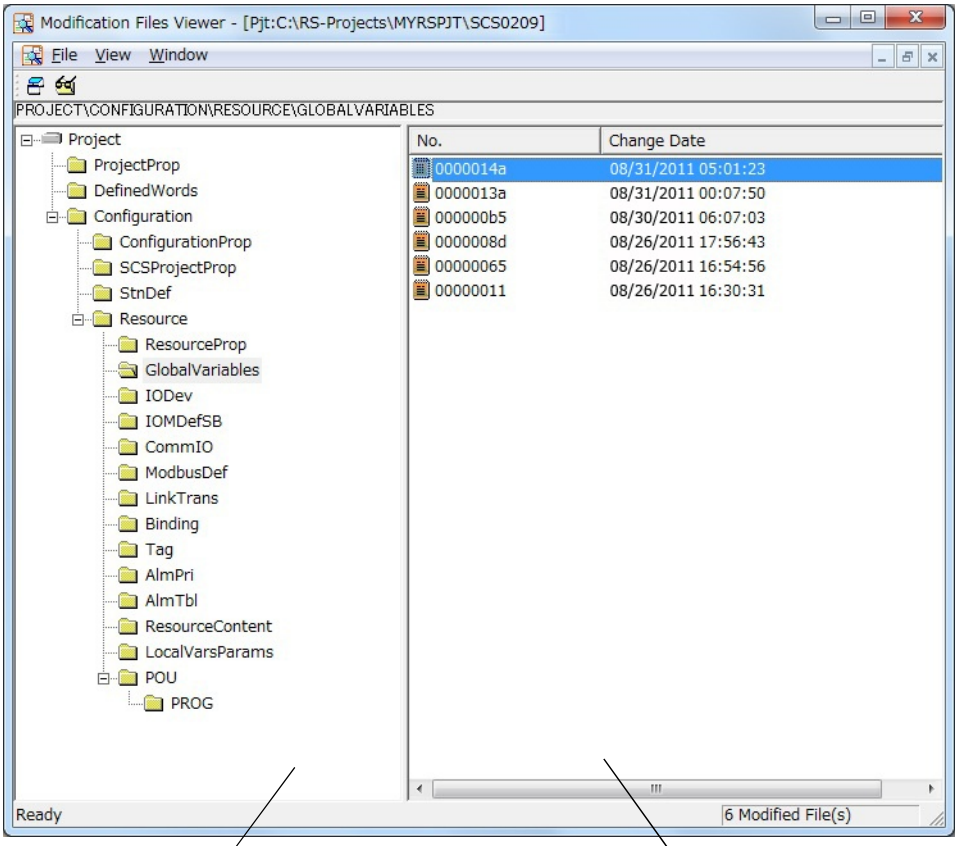


Figure E2.4.2-1 Modification Files Viewer

TIP

- In the tree display when the Modification Files Viewer starts, the focus is on the folder of the modification files corresponding to the selected operation log. If there are multiple modification files corresponding to that operation log (serial number), the focus is on the modification file found first. If there are no modification files corresponding to that operation log, it is started without the tree view being expanded.
- If the wrong password is entered in the dialog box for entering the project password, the Password Input dialog box appears up to two times.

Listing modification files by type

In the left pane of the Modification Files Viewer, the contents of the modification files database are displayed in a tree. Modification files are stored by type in each folder. Modification files of POUs deleted during the course of engineering are also retained.

1. To display a list of modification files by type, select the folder of the targeted modification files in the tree display.
   In the right pane, all modification files of the selected type are displayed in a list.

The display contents are as follows.

- Icon
  Indicates whether the modification file is a builder file, other modification file or POU source.
- Serial number
  This is the serial number of the operation log corresponding to the operation associated with the modification file.
- Change date

TIP

Each time the heading [No.] or [Change Date] is clicked, the modification file list display in the Modification Files Viewer switches between ascending and descending order. When the viewer is started, the list is displayed in descending order by serial number (No.).

SEE ALSO

For more information about types of modification files, refer to:

"● Modification files list" on page E2-59

● Searching modification files

Modification files can be searched by the serial number of the operation log.

1. From the menu bar, select [View] > [Find]. Alternatively, click [Find] on the toolbar.
   A Search dialog box appears.

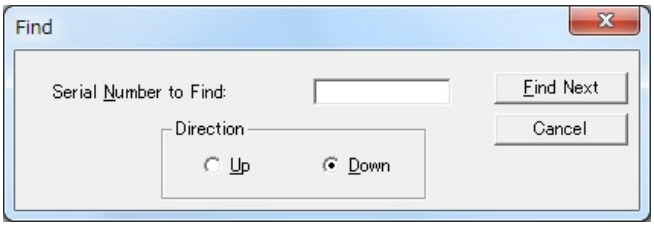


Figure E2.4.2-2 Search dialog box

2. Specify the serial number and search direction.
3. Click [Find Next].
   If a relevant file is found, the folder of this modification file becomes selected in the tree display. All modification files associated with the specified serial number can be searched by repeatedly clicking [Find Next].

● Displaying the contents of modification files

If SCS Manager is running, the contents of files cannot be displayed. Perform the display operation after confirming that SCS Manager is not running. Password input is required when displaying a modification file of a POU for which a password was set when the modification file was last saved.

To display the contents of a modification file, perform the following procedure.

1. In the Modification Files Viewer, display the files whose contents you wish to display in the list display.
2. In the list display of the Modification Files Viewer, double-click the modification file. Alternatively, select a file, right-click, and select [Details] from the pop-up menu.
3. When the dialog box for entering the POU password appears, enter the POU password and click [OK].
   The corresponding builder or the Multi-language Editor is started, or the dedicated viewer is started, and the contents are displayed.

   An example when displayed in the dedicated viewer is as follows.

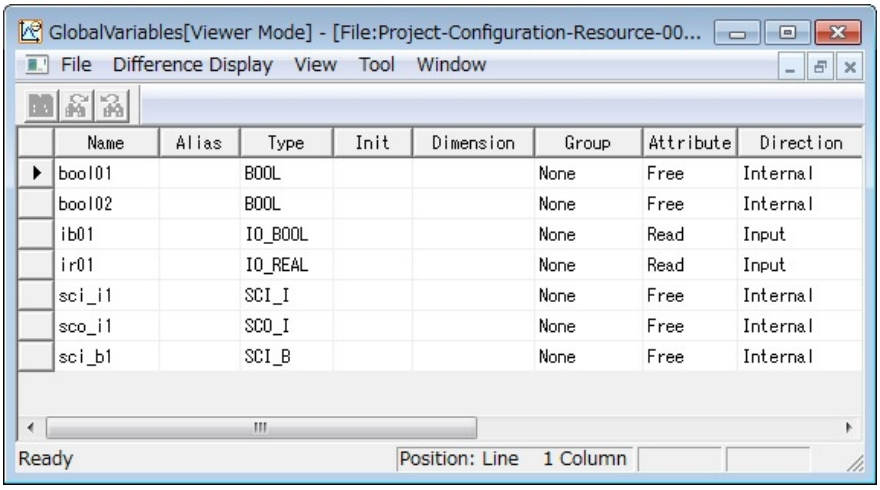


Figure E2.4.2-3 Dedicated viewer example (Global Variables)

SEE ALSO For more information about builders, multi-language editor, and dedicated viewers corresponding to the type of modification file, refer to:

"● Modification files list" on page E2-59

● Displaying differences of two modification files

This section describes the procedure for displaying the differences of two modification files of the same type.

Differences cannot be displayed if the SCS Manager is running. Perform the display operation after checking that the SCS Manager is not running. Password input is required to display a modification file of a POU for which a password was set when the modification file was last saved.

1. In the tree display of the modification file viewer, select the folder of the modification file of the type for which you wish to display the differences.
   A list of modification files appears in the right pane.
2. Double-click a modification file in the modification file list display, and display the contents of the file.
3. If the dialog box for POU password input appears, enter the password of that POU and click [OK].
   The corresponding builder or the Multi-language Editor starts up in viewer mode, and the contents appear.
4. Similarly, display the contents of another modification file.
5. Click [Start Difference Display] button on the toolbar. Alternatively, from the menu bar, select [Difference Display] > [Start Difference Display].
   The windows of the two files are aligned, and items or objects containing differences are displayed in red.

An example of the display when POU modification files have been selected is as follows.

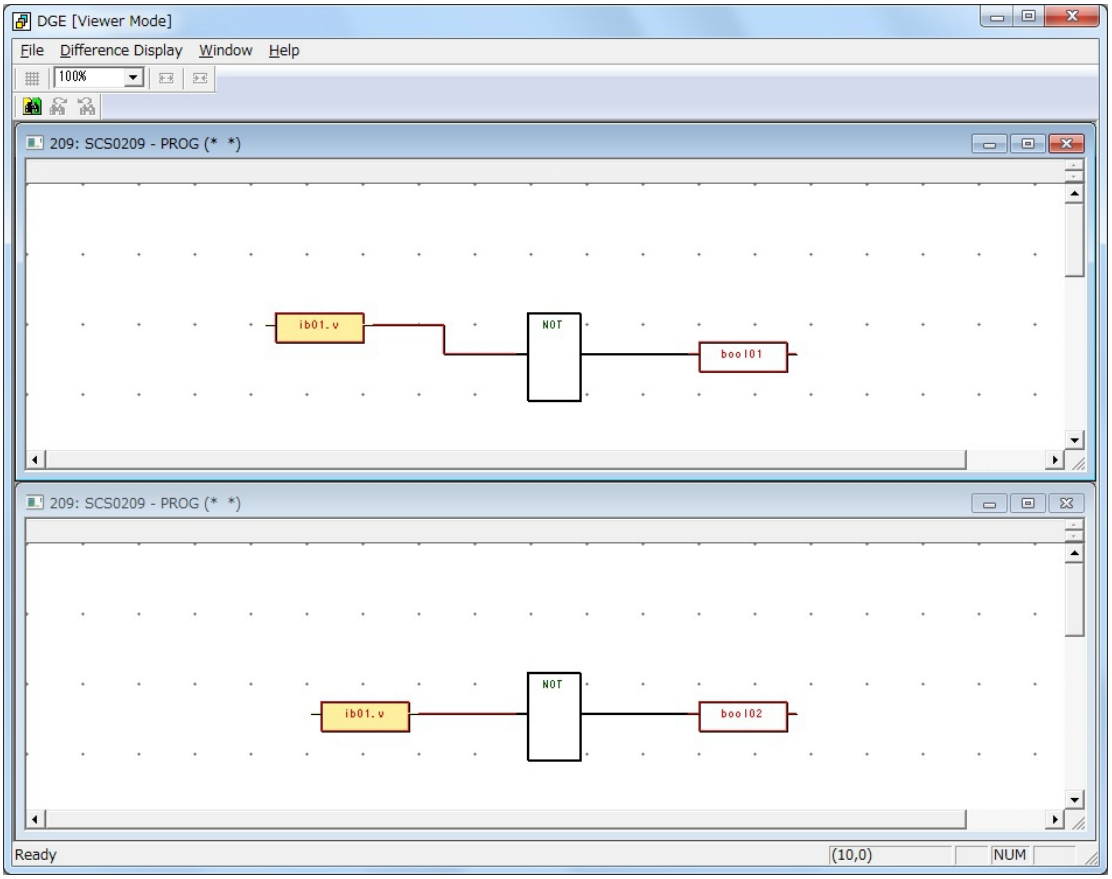


Figure E2.4.2-4 Example of detailed difference display (for POU modification files)

When difference display is executed, the two windows come out with the first difference selected. If the item or object selected in one window does not exist in the other window, nothing is selected.

TIP

In builders or a viewer that is dedicated to viewer mode, order of the data in a document window will be sorted according to the data order in the active document window when difference display is executed in a spreadsheet type window such as tag name builder. Consequently, choosing different active window makes the order of displayed data different when you execute difference display.

The selected state (focus) on the difference can be moved to the next or previous difference by the following operations.

- Each time [Find Next] button on the toolbar is clicked, the focus shifts to the next difference.
- Each time [Find Previous] button on the toolbar is clicked, the focus shifts to the previous difference.

The same focus shifts occur when [Difference Display] > [Find Next] or [Find Previous] is selected from the menu bar. For a builder with multiple tabs, the tab also switches.

TIP

The units of differences in the Multi-language Editor depend on the type of the diagram as follows.

- FBD: Object (variable, function block, link, text comment)
- LD: Rung
- ST: Line

Differences that have no effect on logic operations, such as the position or shape of an object, are also displayed as differences.

Acquiring modification files

Some modification files can be acquired as temporary files of the Builder (file extension .sva) into the specified folder by the specified name. The acquired temporary files can be imported to their corresponding builders. Files that can be acquired are shown in the following table.

Table E2.4.2-3 Modification files that can be acquired

Type of Modification File	Corresponding Builder
StnDef (*1)	SCS Constants Builder
IOMDefSB	I/O Parameter Builder
CommIO	Communication I/O Builder
LinkTrans	SCS Link Transmission Builder
ModbusDef	Modbus Address Builder
DNP3Def	DNP3 Communication Builder
Tag	Tag Name Builder
AlmPri	Alarm Priority Builder
AlmTbl	Alarm Processing Table Builder

*1: Two files, those with "-s" or "-i" appended to the base of the specified file name, are acquired.

To acquire modification files, perform the following procedure.

1. In the list display of the Modification Files Viewer, select one modification file.
2. From the menu bar, select [File] > [Acquire]. Alternatively, right-click and select [Acquire] from the pop-up menu.
   The File Selection dialog box appears.
3. Specify the folder where the modification file is to be saved and the file name, and click [Save].
   The modification file is saved in the specified folder.

Printing modification files

This section describes the operations for printing the contents of modification files and operations for printing the differences between two selected modification files. Since printing cannot be performed while the SCS Manager is running, print after closing the SCS Manager.

Printing the contents of modification files

1. In the list display of the Modification Files Viewer, select a modification file.
2. From the menu bar, select [File] > [Print].
   The Print dialog box appears.
3. Click the [OK] button.
   Printing begins.

Printing differences between two modification files

1. In the list display of the Modification Files Viewer, select two modification files.
2. From the menu bar, select [File] > [Print].
   The Print dialog box appears.
3. Click [OK].
   Printing begins.

E2.4.3 Steps to browse backed-up operation history database

When you try to browse the contents of backed-up operation history database, perform following steps in a PC where operation history management function is performed.

TIP

Use the following backup copies to browse the contents of backed-up operation history database.

- Backup copy of the operation history database that you wish to browse.
- Backup copy of RS project that possesses the SCS project you wish to browse.

1. Prepare a folder where operation history database and RS project to be restored in a PC or in a file server under the share name “RS-Share”.
   a. When you first use the shared folder “RS-Share”, perform appropriate IT security settings.
   b. Create a folder for restoration under the shared folder “RS-Share”.
2. Restore the backup copy of operation history database into the folder created at the above step.
3. Restore the backup copy of RS project into the folder created at the above step.
4. Register the restored RS project and the restored operation history database by means of operation history setup tool.
5. Start operation history management of the registered operation history database. Log of this manipulation to start operation history management can be ignored.
6. Specify the restored operation history database to open operation history database viewer.

SEE ALSO

For more information about how to browse the operation log and modification files, refer to:

- E2.4.1, “Browsing and printing operation logs” on page E2-52
- E2.4.2, “Browsing and printing modification files” on page E2-59

E2.4.4 Lists of Viewer Tool buttons

The functions of the buttons on the toolbar of the Operation History Database Viewer, Modification Files Viewer and Builder in viewer mode are as follows.

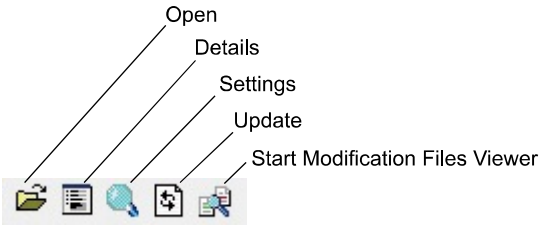


Figure E2.4.4-1 Toolbar buttons and names (Operation History Database Viewer)

Table E2.4.4-1 Toolbar buttons (Operation History Database Viewer)

Name	Description
Open	Specify the SCS project and display the list of operation logs. Same as [Open] of the [File] menu.
Details	Display detailed information of the operation log. Enabled only when one operation log has been selected. Same as [Details] of the [View] menu.
Settings	Set the display conditions for the list of operation logs. Same as [Settings] of the [View] menu.
Update	Update the display of the list of operation logs according to the latest display conditions. Same as [Update] of the [View] menu.
Start Modification Files Viewer	Start the Modification Files Viewer. Enabled only when one operation log has been selected. Same as [View Modification Files] of the [View] menu.

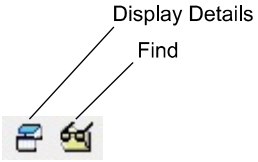


Figure E2.4.4-2 Toolbar buttons and names (Modification Files Viewer)

Table E2.4.4-2 Toolbar buttons (Modification Files Viewer)

Name	Description
Display Details	Display the contents of modification files. Enabled only when one modification file has been selected. Same as [Display Details] of the [View] menu.
Find	Searches for modification files by serial number of operation log. Same as [Find] of the [View] menu.

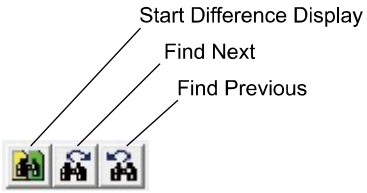


Figure E2.4.4-3 Toolbar buttons and names (Builder in viewer mode)

Table E2.4.4-3 Toolbar buttons (Builder in viewer mode)

Name	Description
Start Difference Display	Display the differences between two modification files. Enabled only when the contents of two modification files are displayed. Same as [Start Difference Display] of the [Difference Display] menu.
Find Next	Move focus to the next difference in the difference display. Same as [Find Next] of the [Difference Display] menu.
Find Previous	Move focus to the previous difference in the difference display. Same as [Find Previous] of the [Difference Display] menu.

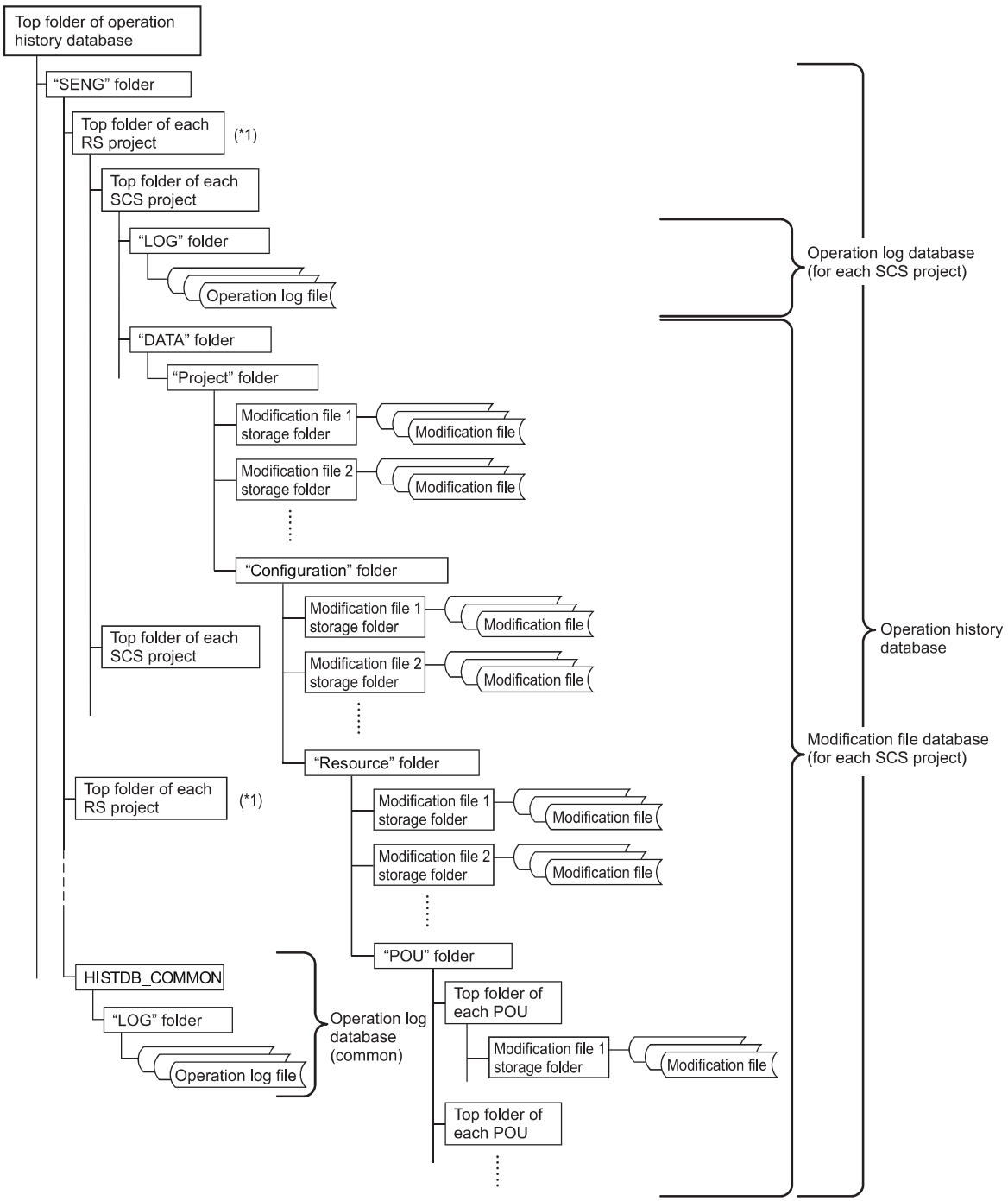
E2.5 Detailed information of Access Control/ Operation History Management

This section describes the detailed information pertaining to access control and operation history management.

E2.5.1 Operation history database structure

The operation history database is generated for each RS project in the location specified in the Operation History Management Setup Tool. The operation history database of each RS project consists of the operation log database and modification files database of each SCS project. The operation log of operations common to all RS projects, such as SCS Manager startup, is recorded in the common operation log database. Modification files are stored by type below the folder of the modification file type name.

The folder structure of the operation history database is shown in the following figure.



*1: The folder name is the same as the RS project name.
*2: The folder name is the same as the SCS project name.

Figure E2.5.1-1 Operation history database structure

E2.5.2 Access rights category list

The following table shows a list of access right categories.

Table E2.5.2-1 Access rights categories (access rights to project database)

Category	Operation Description	Operation Program Tool
Project Creation	Creation of new SCS projects/libraries	SCS Manager
General Settings	Change of project properties, project descriptions Change of configuration names, configuration properties, configuration descriptions Change of connection properties (IP addresses) Change of resource names, resource properties, resource descriptions Change of POU properties, POU descriptions Addition, deletion or name change of POU Addition, deletion or change of variable groups Clean Build Addition, deletion or change of library dependencies Import by SCS Manager (*1)	SCS Manager
	Change of SCS project properties	SCS Project Properties
	Change of SCS constants definitions	SCS Constants Builder
	Acknowledgement by analyzer	Integrity Analyzer, Cross Reference Analyzer
	Database validity check Repair database	Database Validity Check Tool
POU	Change of POU logic Addition, deletion or change of defined words Addition, deletion or change of variables Addition, deletion or change of parameters Build Import by SCS Manager (*1)	SCS Manager
	Acknowledgement by analyzer	Integrity Analyzer, Cross Reference Analyzer
	Database validity check Repair database	Database Validity Check Tool
I/O	Addition, deletion or change of I/O devices Addition, deletion or change of I/O wiring Build Import by SCS Manager(*1)	SCS Manager
	Change of I/O parameter definitions	I/O Parameter Builder
	Acknowledgement by analyzer	Integrity Analyzer, Cross Reference Analyzer
	Database validity check Repair database	Database Validity Check Tool

Continues on the next page

Table E2.5.2-1 Access rights categories (access rights to project database) (Table continued)

Category	Operation Description	Operation Program Tool
Safety Communication	Addition, deletion or change of external bindings Build	SCS Manager
	Change of SCS link transmission definitions	SCS Link Transmission Builder
	Acknowledgement by analyzer	Integrity Analyzer, Cross Reference Analyzer
	Database validity check Repair database	Database Validity Check Tool
External Communication	Change of tag name definitions	Tag Name Builder
	Change of communication I/O definitions	Communication I/O Builder
	Change of modbus address definitions	Modbus Address Builder
	Change of DNP3 communication definitions	DNP3 Communication Builder
	Build	SCS Manager
	Acknowledgement by analyzer	Integrity Analyzer, Cross Reference Analyzer
	Database validity check Repair database	Database Validity Check Tool
CENTUM Alarm Definition	Change of alarm priority definitions	Alarm Priority Builder
	Change of alarm processing table definitions	Alarm Processing Table Builder
	Build	SCS Manager
	Acknowledgement by analyzer	Integrity Analyzer, Cross Reference Analyzer
	Database validity check Repair database	Database Validity Check Tool
Version Control Check In	Version control check in	Version Control Tool
Version Control Check Out	Version control check out	Version Control Tool
Master Database Restore	Restoration of master database	Master Database Restoring Function

*1: The SCS Manager import operation and the reflection operation with RS Generation Manager during implementation of I/O list engineering can be performed only when the user has access rights for the General Setting, POU, and I/O categories.

Table E2.5.2-2 Access rights categories (access rights to SCS)

Category	Operation Description	Operation Program/ Tool
Offline Download	Build	SCS Manager
	Master database offline download	Master Database Off-line Download
	SCS restart	Restart SCS
	SCS security level setting, password change	Set SCS Security Level
	Acknowledgement by analyzer	Integrity Analyzer, Cross Reference Analyzer
	Database validity check Repair database	Database Validity Check Tool
Online Change Download	Build	SCS Manager
	Download operation marks	Download Operation Marks
	SCS security level setting, password change	Set SCS Security Level
	Acknowledgement by analyzer	Integrity Analyzer, Cross Reference Analyzer
	Database validity check Repair database	Database Validity Check Tool
Operation Mark Save	Save operation marks	Save Operation Marks
SCS Simulator	Start test function	SCS Test Function
	Update test database	Update Test Database
	Build	SCS Manager
	SCS security level setting, password change	Set SCS Security Level
	Acknowledgement by analyzer	Integrity Analyzer, Cross Reference Analyzer
	Database validity check Repair database	Database Validity Check Tool
Debug	Start logic simulation, start debug mode	SCS Manager
Forcing	Forcing (lock, unlock, value setting)	SCS Manager I/O Lock Window, Communication I/O Lock Window, SCS Link Transmission Lock Window, Inter-SCS Communication Lock Window
	SCS security level setting, password change	Set SCS Security Level
Maintenance	Output enable operation, output module start, IOM download, time setting, NIU maintenance port setting	SCS State Management Window
	Confirm display fonts, colors and messages, set and change deletion operation method	Setup Tool
	IOM control right switching	I/O Control Right Switching Tool

Continues on the next page

Table E2.5.2-2 Access rights categories (access rights to SCS) (Table continued)

Category	Operation Description	Operation Program/ Tool
Diagnosis Acknowledgment	Acknowledgment and deletion of diagnostic information message	Diagnostic Information
Message Cache	Operations such as setting up message collection, initializing trip information in SCS, saving or deleting cache data Stopping and starting of automatic message acquisition	Message Cache Tool

E2.5.3 Information recorded in operation logs

The following information is recorded in one operation log.

Table E2.5.3-1 Structure of operation logs

	Item	Description
1	Serial number (*1)	Unique identifier corresponding to one operation (8-digit hexadecimal number).
2	Date/time (*1)	Date and time the operation was executed.
3	Computer name	SENG PC name on which the operation was executed.
4	Windows user name	Windows user name at the time the operation was executed.
5	Engineer name (*1)	Name of the engineer who executed the operation.
6	Name	Name of the person corresponding to the engineer who executed the operation. (Character string entry in "Printed Name" field of Engineers' Account Builder)
7	Program name	Name of the program that executed the operation.
8	Operation name (*1)	Executed operation.
9	Object of operation(*1)	Target of executed operation.
10	Reason (*1)	Character string (1 line) input as "Reason" in Engineer Authentication dialog box.
11	Result of operation	Contents output to the message area as the result of operation (multiple lines).

*1: These items are displayed in the operation log list of the Operation History Database Viewer. Other items can be browsed on the detailed information display.

Operation log information lists

Here, the information recorded in operation logs is listed by operation type.

The following are the notes on the items omitted in the following tables.

- "Serial Number," "Date/Time" and "Computer Name" are always recorded in every operation log entry.
- For the operations for which engineer names are recorded, the name of the person corresponding to the engineer name is always recorded in "Name."
- In "Reason," the content entered in the "Reason" field of the Engineer Authentication dialog box is recorded.
- In "Result of Operation," the contents displayed in the message area of SCS Manager, builder, or tool are recorded.

Table E2.5.3-2 Operation log information list (Operations on project database)

Operation Name	Item	Description
Start SCS Manager (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Start SCS Manager (Log on)
	Object of Operation	-

Continues on the next page

Table E2.5.3-2 Operation log information list (Operations on project database) (Table continued)

Operation Name	Item	Description
Close SCS Manager (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Terminate SCS Manger (Log off)
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Create new SCS project	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Create Project
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Open SCS project	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Open Project
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Save project	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Save Project
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Import by SCS Manager	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Import
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Save dictionary	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Save Dictionary
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101

Continues on the next page

Table E2.5.3-2 Operation log information list (Operations on project database) (Table continued)

Operation Name	Item	Description
Save I/O wiring	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Save I/O wiring
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Save binding list	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Save external binding list
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Save library dependencies	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Save dependencies
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Open POU	Engineer Name	Engineer who executed the operation
	Program Name	Multi Language Editor
	Operation Name	Open POU
	Object of Operation	POU name Example: PROG01
Save POU	Engineer Name	Engineer who executed the operation
	Program Name	Multi Language Editor
	Operation Name	Save POU
	Object of Operation	POU name Example: PROG01
Open by builder	Engineer Name	Engineer who executed the operation
	Program Name	Builder name Example: Tag Name Builder
	Operation Name	Open Builder
	Object of Operation	Target data Example: Tag Name

Continues on the next page

Table E2.5.3-2 Operation log information list (Operations on project database) (Table continued)

Operation Name	Item	Description
Save by builder	Engineer Name	Engineer who executed the operation
	Program Name	Builder name Example: Tag Name Builder
	Operation Name	Save Builder
	Object of Operation	Target data Example: Tag Name
Change SCS project properties	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Change SCS Project Properties
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Build	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Build Project
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Clean	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Clean Project
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Save analyzer's results	Engineer Name	Engineer who executed the operation
	Program Name	Analyzer name Example: Integrity Analyzer
	Operation Name	Save Analysis
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Start document generator	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Start Document Generator
	Object of Operation	SCS Project Path Name or Library Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101

Continues on the next page

Table E2.5.3-2 Operation log information list (Operations on project database) (Table continued)

Operation Name	Item	Description
Start master database restoring function (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	Master Database Restoring Function
	Operation Name	Start Master Database Restoring Function (Log on)
	Object of Operation	-
Close master database restoring function (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	IOM Control Right Switching Tool
	Operation Name	Terminate Master Database Restoring Function (Log off)
	Object of Operation	-
Restore master database	Engineer Name	Engineer who executed the operation
	Program Name	Master Database Restoring Function
	Operation Name	Restore Master Database
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Start version control tool (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	Version Control Tool
	Operation Name	Start Version Control Tool (Log on)
	Object of Operation	-
Close version control tool (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	Version Control Tool
	Operation Name	Terminate Version Control Tool (Log off)
	Object of Operation	-
Check in to version control	Engineer Name	Engineer who executed the operation
	Program Name	Version Control Tool
	Operation Name	Check In
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101

Continues on the next page

Table E2.5.3-2 Operation log information list (Operations on project database) (Table continued)

Operation Name	Item	Description
Check out from version control	Engineer Name	Engineer who executed the operation
	Program Name	Version Control Tool
	Operation Name	Check Out
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101

Table E2.5.3-3 Operation log recorded information list (operations on SCS)

Operation Name	Item	Description
Offline download	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Offline Download
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Master offline download	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Master Database Offline Download
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Online change download	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Online Change Download
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Restart SCS	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Restart SCS
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101

Continues on the next page

Table E2.5.3-3 Operation log recorded information list (operations on SCS) (Table continued)

Operation Name	Item	Description
Save operation marks	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Save Operation Marks
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Download operation marks	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Download Operation Marks
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Start debug mode	Engineer Name	Engineer who executed the operation
	Program Name	Example: SCS Manager
	Operation Name	Start Debug
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Exit debug mode	Engineer Name	Engineer who executed the operation
	Program Name	Example: SCS Manager
	Operation Name	Stop Debug
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Start logic simulation	Engineer Name	Engineer who executed the operation
	Program Name	Example: SCS Manager
	Operation Name	Start Simulation
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Close logic simulation	Engineer Name	Engineer who executed the operation
	Program Name	Example: SCS Manager
	Operation Name	Stop Simulation
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101

Continues on the next page

Table E2.5.3-3 Operation log recorded information list (operations on SCS) (Table continued)

Operation Name	Item	Description
Start test function	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	SCS Test Function
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Update test database	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Update SCS Test Database
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Database validity check	Engineer Name	Engineer who executed the operation
	Program Name	Database Validity Check Tool
	Operation Name	Check Database Validity
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Repair database	Engineer Name	Engineer who executed the operation
	Program Name	Database Validity Check Tool
	Operation Name	Repair Database
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Start SCS Status Overview window (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	SCS Status Overview Window
	Operation Name	Open SCS Status Overview Window (Log on)
	Object of Operation	RS Project Path Name Example: C:\RS-Projects\MYRSPJT
Close SCS Status Overview window (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	SCS Status Overview Window
	Operation Name	Close SCS Status Overview Window (Log off)
	Object of Operation	RS Project Path Name Example: C:\RS-Projects\MYRSPJT

Continues on the next page

Table E2.5.3-3 Operation log recorded information list (operations on SCS) (Table continued)

Operation Name	Item	Description
Start SCS State Management window	Engineer Name	Engineer who executed the operation
	Program Name	SCS State Management Window
	Operation Name	Open SCS State Management Window
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Close SCS State Management window	Engineer Name	Engineer who executed the operation
	Program Name	SCS State Management Window
	Operation Name	Close SCS State Management Window (Log off)
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Change SCS security level	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Change SCS Security Level
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Change security level password	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager
	Operation Name	Change SCS Security Password
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Lock	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager or Lock Window Name Example: SCS Manager
	Operation Name	Lock
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Unlock	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager or Lock Window Name Example: SCS Manager
	Operation Name	Unlock
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101

Continues on the next page

Table E2.5.3-3 Operation log recorded information list (operations on SCS) (Table continued)

Operation Name	Item	Description
Set values	Engineer Name	Engineer who executed the operation
	Program Name	SCS Manager or Lock Window Name Example: SCS Manager
	Operation Name	Set Value
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Enable output	Engineer Name	Engineer who executed the operation
	Program Name	SCS State Management Window
	Operation Name	Output Enable
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Start output module	Engineer Name	Engineer who executed the operation
	Program Name	SCS State Management Window
	Operation Name	Start Output Modules
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
IOM download	Engineer Name	Engineer who executed the operation
	Program Name	SCS State Management Window
	Operation Name	IOM Download
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
NIU maintenance port setting	Engineer Name	Engineer who executed the operation
	Program Name	SCS State Management Window
	Operation Name	Set NIU Maintenance Port
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Time setting (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	Adjust Time Window
	Operation Name	Time Setup
	Object of Operation	RS Project Path Name Example: C:\RS-Projects\MYRSPJT

Continues on the next page

Table E2.5.3-3 Operation log recorded information list (operations on SCS) (Table continued)

Operation Name	Item	Description
Acknowledge/delete diagnostic information messages	Engineer Name	Engineer who executed the operation
	Program Name	Diagnostic Information Window
	Operation Name	Diagnosis Acknowledgment
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Change SCS Maintenance Support Tool settings (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	SCS Maintenance Setup
	Operation Name	Setup SCS Maintenance Window
	Object of Operation	RS Project Path Name Example: C:\RS-Projects\MYRSPJT
Start IOM Control Right Switching Tool (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	IOM Control Right Switching Tool
	Operation Name	Start IOM Control Right Switching Tool (Log on)
	Object of Operation	-
Close IOM Control Right Switching Tool (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	IOM Control Right Switching Tool
	Operation Name	Terminate IOM Control Right Switching Tool (Log off)
	Object of Operation	-
Switch IOM control right	Engineer Name	Engineer who executed the operation
	Program Name	IOM Control Right Switching Tool
	Operation Name	Switch IOM Control Right
	Object of Operation	SCS Project Path Name Example: C:\RS-Projects\MYRSPJT\SCS0101
Start Message Cache Tool (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	Message Cache Tool
	Operation Name	Start Message Cache Tool (Log on)
	Object of Operation	-

Continues on the next page

Table E2.5.3-3 Operation log recorded information list (operations on SCS) (Table continued)

Operation Name	Item	Description
Close Message Cache Tool (recorded in common operation log database)	Engineer Name	Engineer who executed the operation
	Program Name	Message Cache Tool
	Operation Name	Terminate Message Cache Tool (Log off)
	Object of Operation	-
Operate Message Cache Tool (initializing trip information)	Engineer Name	Engineer who executed the operation
	Program Name	Message Cache Tool
	Operation Name	Initialize Trip Information
	Object of Operation	SCS name Example: SCS0101
Pause message acquisition	Engineer Name	Engineer who executed the operation
	Program Name	Message Cache Tool
	Operation Name	Pause Message Acquisition
	Object of Operation	Narrowband group name set by the user Example: Narrowband Group No.1
Resume message acquisition	Engineer Name	Engineer who executed the operation
	Program Name	Message Cache Tool
	Operation Name	Resume Message Acquisition
	Object of Operation	Narrowband group name set by the user Example: Narrowband Group No.1

Table E2.5.3-4 Operation log recorded information list (operations related to Access Control/Operation History Management)

Operation Name	Item	Description
Start operation history management (recorded in common and each SCS projects' operation log databases)	Engineer Name	-
	Program Name	Operation History Management Setup Tool
	Operation Name	Start Operation History Management
	Object of Operation	RS Project Path Name Example: C:\RS-Projects\MYRSPJT

Continues on the next page

Table E2.5.3-4 Operation log recorded information list (operations related to Access Control/Operation History Management) (Table continued)

Operation Name	Item	Description
Stop operation history management (recorded in common and each SCS projects' operation log databases)	Engineer Name	-
	Program Name	Operation History Management Setup Tool
	Operation Name	Pause Operation History Management
	Object of Operation	RS Project Path Name Example: C:\RS-Projects\MYRSPJT
Exceeded number of authentications (recorded in common operation log database)	Engineer Name	Engineer name entered for logon or engineer authentication
	Program Name	Name of the program for which logon or engineer authentication was attempted
	Operation Name	Authentication Error
	Object of Operation	-
Local user logon in domain environment (recorded in common operation log database)	Engineer Name	Logged-on engineer name
	Program Name	Logged-on program name
	Operation Name	Local Authentication Detected
	Object of Operation	-
Record a comment (operation by administrator) (recorded in common operation log database)	Engineer Name	-
	Program Name	Operation History Management Setup Tool
	Operation Name	Arbitrary Comment
	Object of Operation	RS Project Path Name Example: C:\RS-Projects\MYRSPJT

F. Tools and functions used with engineering of ProSafe-RS

Tools and functions such as the following can be used when engineering ProSafe-RS.

- SCS Information Dialog
  Used when looking up the capacities or numbers of Program Organization Units (POUs) or variables used in the SCS project. Whether or not the number of logical I/O points in use are within the range of licenses possessed can also be looked up.
- Self Documentation
  Used when printing the content of an SCS project as a document.
- Database Validity Check Tool
  Used to check the mutual validity of the work database, the master database, and the SCS database that has been downloaded onto an SCS.
- Master Database Restoring function
  Used to restore a SCS project being edited to its original state when it was last downloaded.
- Version Control Tool
  Used to manage the history of changes made to SCS projects not registered with an AD project.
- Project Comparing Tool
  Used to display or print the difference between two specified SCS projects.
- Online Monitoring
  Used when monitoring the application logic executed on the SCS.
- Forcing
  Used when changing the values of I/O modules, variables. or FB parameters while they are locked. Dedicated locking windows are used to perform Forcing.
- Software Configuration Viewer
  Used to look up information in regard to software installed on SENG.
- Builder Environment Tool
  Used to customize builders installed on SENG.

F1. Display SCS information

The SCS information including the number of POUs used in the SCS project and the quantity and capacity of variables can be displayed.

This section explains the contents displayed in the SCS Information dialog box.

Overview of SCS information

The number of POUs used in the SCS project and the quantity and capacity of variables are displayed as SCS information. The maximum capacity and the maximum quantity of the variables, and the usage ratio against the maximum capacity in the working database and in the master database are also displayed. Before displaying the SCS information, the SCS project needs to be built.

Call SCS Information dialog box

1. Choose [Engineering] from [Tools] menu of SCS Manager.
   so as to display the Engineering Launcher menu.
2. On Engineering Launcher menu, choose [SCS Information]
   so as to display the SCS Information dialog box.

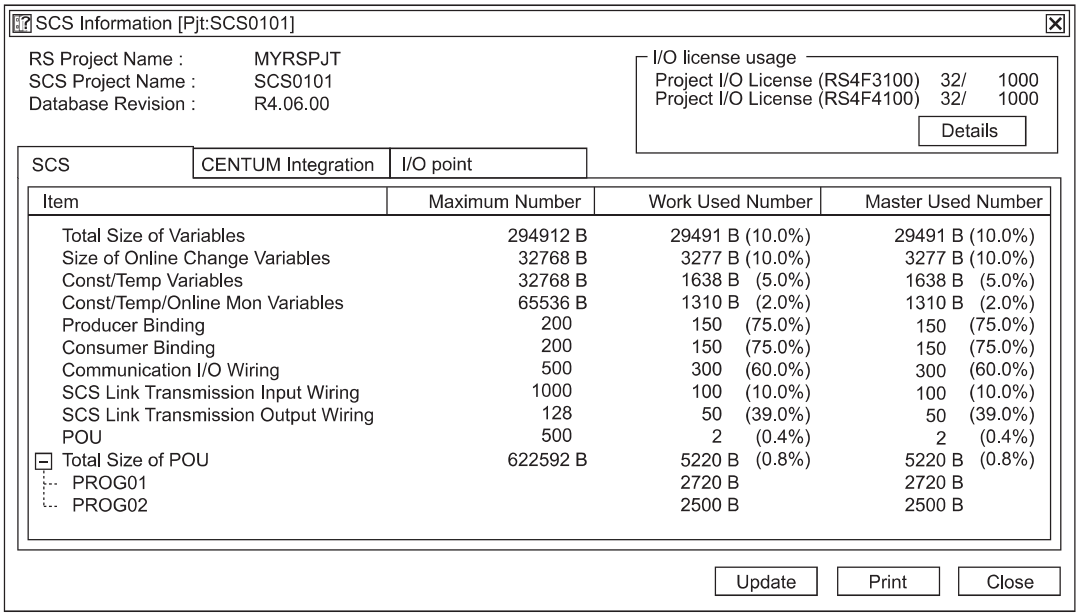


Figure F1-1 SCS Information dialog box

Elements in SCS Information dialog box

The following information is displayed for the selected SCS. The dialog box includes the SCS tab sheet and CENTUM Integration tab sheet. If the CI Server Integration Package is activated, the tab sheets will be SCS and CI Server Integration.

- The corresponding RS project name and the SCS project name
- The revision number of the SCS project database
- The usages of variables and POUs in the SCS project
- Usage status of I/O licenses
- The usage of variables in the case of a CENTUM integration or CI Server integration structure

Moreover, the displayed contents can be updated and can be printed out.

IMPORTANT

Performing a build reflects the latest information onto this dialog. To check correct information, check the details after performing a build.

SCS information items

The following values are shown for each item.

- Maximum Number
  The maximum number for each item that you can define in a SCS.
- Usage in Work Database
  The quantity or number used for the item in the SCS project which is under engineering. The percentage of the maximum is also shown.
- Usage in Master Database
  The quantity or number used for the item in the SCS project which is downloaded to the SCS. The percentage of the maximum is also shown.

The SCS tab shows the following items.

Table F1-1 Items on SCS tab

Item	Description
Total Size of Variables (*1)	Total size of variables after finishing the offline download. Excludes constants and temporary variables.(*2)
Size of Online Change Variables	Size of variables added by online change downloading.
Const/Temp Variables	Total size of all the constants and temporary variables currently in use. Includes those added by an online change download. (*2)
Const/Temp/Online Mon Variables	Total size of constants, temporary variables, and monitoring variables. Includes those added by an online change download. (*2)(*3)
Producer Binding	Number of binding variables on the producing side defined in all producer groups
Consumer Binding	Number of binding variables on the consuming side defined in all consumer groups
Communication I/O wiring	Number of variables defined in the Communication I/O Wiring on Communication I/O Builder
Safety Subsystem Communication I/O Wiring	Number of variables defined in the Safety Subsystem Communication I/O Wiring on Communication I/O Builder. The maximum value is fixed.
SCS Link Transmission Input Wiring	Number of SCS Link Transmission input variables defined on “Data Wiring Definition” of SCS Link Transmission Builder.
SCS Link Transmission Output Wiring	Number of SCS Link Transmission output variables defined on “Data Wiring Definition” of SCS Link Transmission Builder.
DNP3 communication FB (*4)	Total number of instances of the DNP3 communication FBs that are assigned to DNP3 data. Includes those instances that are created inside of the user defined FBs.
AGA FB (*4)	Number of AGA FB (AGA_3, AGA_7) instances. Includes those created as parameters of user defined FBs.
AGA Report FB (*4)	Number of AGA_R FB instances. Includes those created as parameters of user defined FBs.

Continues on the next page

Table F1-1 Items on SCS tab (Table continued)

Item	Description
Retain Data (*4)	Number of bytes used for retain data. Depends on the number of FB (AGA_R, ACCUM, ECWR_B, ECWR_I, ECWR_R) instances that use the retain function.
POU	Number of created POUs
Total Size of POU (*1)(*5)	Total size of POU usage

*1: If the SCS project is built after being edited, the usage in the working database is displayed.
*2: The temporary variables are the variables generated temporarily for executing the POU.
*3: The monitoring variables are the variables for monitoring the POU statuses.
*4: Displayed only for SCSU1.
*5: When clicking the [+] button on the left side, the name and size of each POU will be displayed.

Precautions when building

In SCS, the size of the area for variables used in the application logic differs depending on its station type.

Table F1-2 Size of the area for variables used in the application logic

Station type	Size of the area for variables used in the application logic
SSC10/SSC50/SSC57	384 KB (393216 B)
SSC60/S2SC70/L1SC70	1536 KB (1572864 B)

In the area for variables used in the application logic, if the size of the variable-defined area in use may become too large to reserve the specified size of the area for online changes after the next offline download, the following warning message appears when building.

```
The total size of variables in use is aa.aKB (cc.c%).
The user variables area of on-line changes may not be reserved after the next off
-line download is completed.
```

Also, if the area for online change is not reserved, the following error message appears and the build fails.

```
The total size of variables in use exceeded the maximum value. :the size in use a
a.aKB: the maximum size bb.bKB
```

TIP

aa.a, bb.b, and cc.c displayed in the error message or the warning message denote numerical values.

To avoid generation of warnings and errors, consider additional variables in further online changes, reduce the setting value of one or both of “Size of Online Change Variables (User variable size)” and “Constant/temporary variable size (Memory size for temporary variables)” in the resource properties of SCS Manager, and perform a clean build and offline download.

The warning or the error is not generated if the value displayed in the SCS Information dialog box satisfies the following formula.

(Work Used Number of “Total Size of Variables” (1)) + (Maximum Number of “Size of Online Change Variables” (2)) × 4 + (Maximum Number of “Const/Temp Variables” (3)) ≤ (size of the area for variables used in the application logic)

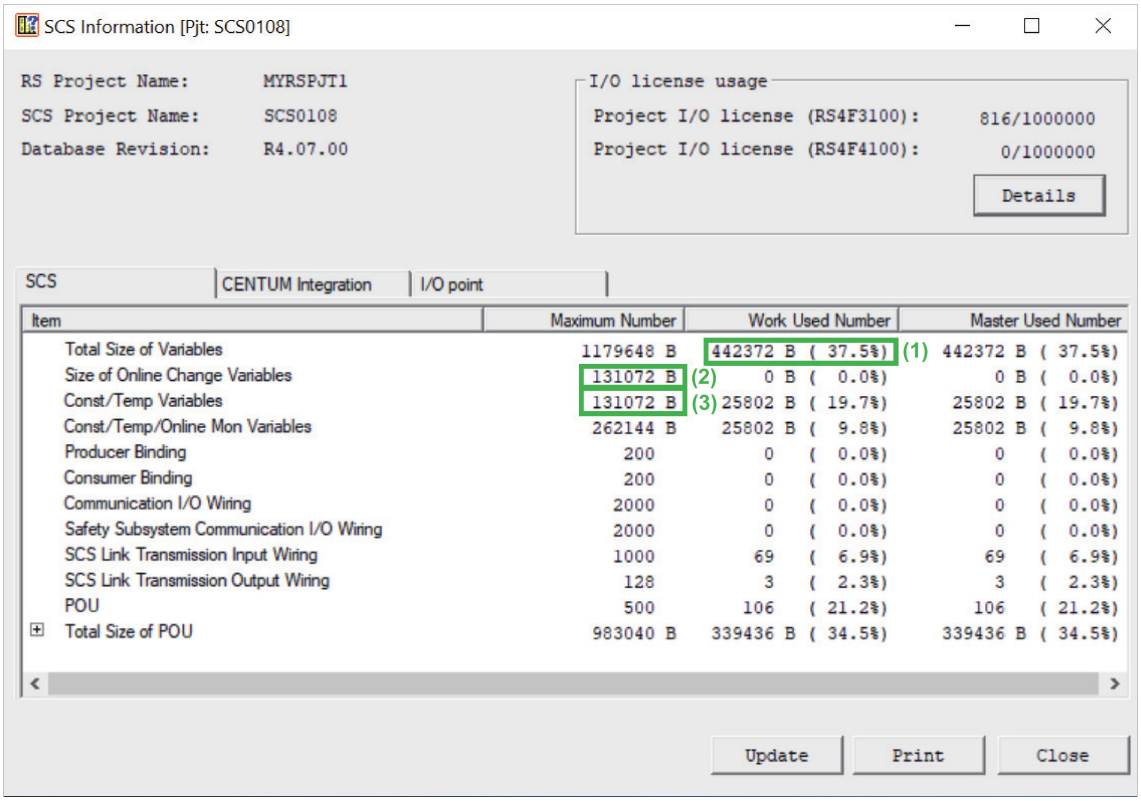


Figure F1-2 SCS Information dialog box

The Work Used Number of “Total Size of Variables” (1) is the size of variables used when performing offline download (excluding constant/temporary variables).

The Maximum Number of “Size of Online Change Variables” (2) is the size set in “Size of Online Change Variables (User variable size)” in the resource properties of SCS Manager.

The Maximum Number of “Const/Temp Variables” (3) is the size set in “Constant/temporary variable size (Memory size for temporary variables)” in the resource properties of SCS Manager.

Checking the usage status of I/O licenses

The current usage status of I/O licenses can be checked from the following:

- I/O license usage section
  - This section shows the number of logical I/O points in use with all SCSs and the number of logical I/O points provided. The numbers are displayed separately for SIL3 license (RS4F3100) and SIL2 license (RSF4100).
  - One license of a project I/O license is equivalent to 100 logical I/O points. The number of project I/O licenses in possession is the displayed number of logical I/O points possessed divided by 100.
  - Clicking Details displays the I/O license usage dialog box, which shows the number of logical I/O points in use for each station.
- I/O point tab
  The following values of each item are displayed on the I/O point tab.
  - Category
    Displayed in the categories of safety I/O, communication I/O, and total. Regarding communication I/O, the total value for subsystem communication I/O wiring and safety subsystem communication I/O wiring is displayed.
  - Number of I/O

The number of physical I/O points of the target SCS is displayed.

- Number of logical I/O
  The number of logical I/O points of the target SCS is displayed.

I/O license usage dialog box

I/O license usage dialog box shows the following information:

- Number of owned licenses section
  - This section shows the number of logical I/O points in use with all SCSs included in the license project and the number of logical I/O points provided, separately for SIL3 license (RS4F3100) and SIL2 license (RSF4100).
  - One license of a project I/O license is equivalent to 100 logical I/O points. The number of owned project I/O licenses is the displayed number of provided logical I/O points divided by 100.
- Station
  Displays the SCSs subject to I/O metered licensing in the license project.
- License
  Displays the project I/O license used for each SCS.
- Number of logical I/O
  Displays the number of logical I/O points for each SCS.

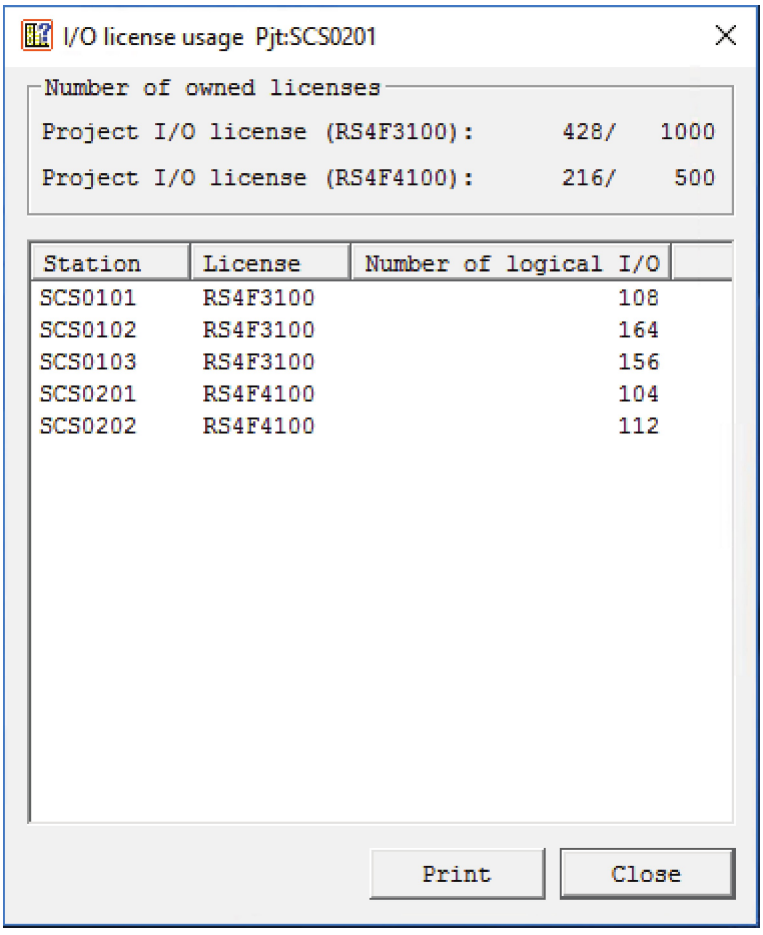


Figure F1-3 I/O license usage dialog box

Counting the logical I/O points

The items subject to the count of the logical I/O points are safety I/O (AI, AO, DI, DO) and the communication I/O of subsystem communication modules and fire and gas communication modules.

Logical I/O points are counted in the following manner. Decimal values of all of the totaled logical I/O points are rounded down.

For AIO/DIO modules, one terminal corresponds to one logical I/O point.

For subsystem communication modules, the number of data points multiplied by 0.25 corresponds to one logical I/O point. The number of data points is counted in the following manner in accordance with the data type. However, data is counted when the data has been defined with Communication I/O Builder and the communication module has also been defined.

- With 32-bit analog data, two words are counted as one point of data.
- With 16-bit analog data, one word is counted as one point of data.
- With digital data, one word is counted as 16 points of data.
- With SLSEVENT data, 24 words are counted as 24 points of data.

For fire and gas communication modules, the number of data points multiplied by 0.25 corresponds to one logical I/O point. The number of data points is counted in the following manner. However, data is counted when the data has been defined with Safety Communication I/O Editor and the communication module has also been defined.

The security information contained in the communication definitions of PROFINET and PROFIsafe is not wired as signals. Therefore, the security information is not subject to the count of logical I/O points.

- With unsigned8, two words are counted as one point of data. 1 x 0.25 = 0.25
- With float32, two words are counted as one point of data. 1 x 0.25 = 0.25
- With unsigned16, two words are counted as one point of data. 1 x 0.25 = 0.25
- With unsigned32, two words are counted as one point of data. 1 x 0.25 = 0.25

Example:

GS01_SAFE_RS is configured of unsigned8 (2 words), float32 (2 words), and security information (4 words). Because security information is not counted, the data of unsigned8 (2 words) and float32 (2 words) is counted as the number of logical I/O points.

Total number of logical I/O points for GS01_SAFE_RS = 0.25 + 0.25 = 0.5

Example:

DIAG_STATUS is configured of unsigned32 (2 words).

Total number of logical I/O points for DIAG_STATUS = 0.25

Example:

GW_STATUS, BBR_STATUS, and BATTERY_LIFE are each configured of unsigned16 (2 words).

Total number of logical I/O points for GW_STATUS, BBR_STATUS, and BATTERY_LIFE each = 0.25

The SCSs for which the logical I/O points are counted are SCSP1, SCSP2, SCSP3, SCSL2, and SCSU1.

Logical I/O points are counted in the following conditions.

- All SCS projects included in all RS projects registered with the same AD Project are subject to the count
- All SCSs registered with the same AD Project are registered to the same license project

- The project I/O license in possession is properly reflected onto the license project

These conditions properly being reflected, the SCS being registered with the license project and the RS project, and the RS project being registered with the AD project are prerequisites.

Information displayed in the case of CENTUM integration structure or CI Server integration structure

On the CENTUM Integration tab or CI Server Integration tab, the usages of the tagged variables will be displayed by types.

If integration with CENTUM or CI Server is not established, the usages will be displayed with 0s.

Table F1-3 Items on CENTUM Integration tab

Item			Remarks
Station Common Tag	IO_BOOL		
	BOOL Tag	BOOL	
		ECW_B	
		ECWR_B	Displayed only for SCSU1.
	REAL, INT Tag	DINT	
		ECW_I	
		ECWR_I	Displayed only for SCSU1.
		ECW_R	
		ECWR_R	Displayed only for SCSU1.
		IO_REAL	
		REAL	
	SCI, SCO Tag	SCI_B	
		SCI_I	
		SCI_R	
		SCO_B	
		SCO_I	
		SCO_R	
	PNI, PSI Tag	PNI_I	Displayed only for SCSP3.
		PNI_R	
		PSI_I	
		PSI_R	

Continues on the next page

Table F1-3 Items on CENTUM Integration tab (Table continued)

Item			Remarks
Area Tag	Annunciator Tag	ANN	
		ANN_FUP	
	Mapping Block Tag	ANLG_S	
		ANLGI	
		HSDTR	
		GASDTR	
		GOV_B	Not displayed in CI Server integration structure.
		GOV_IB	
		OVR_B	
		OVR_I	
		OVR_R	
		OVR_IB	
		OVR_IR	
		MOA	
		MOB_11	
		MOB_21	
		MOB_RS	
		PASSWD	
		VEL	
	Mapping Block Tag 2	AGA_3	Displayed only for SCSU1.
		AGA_7	
		AGA_R	

F2. Self Document

This chapter describes the Self Document Function.

Outline of Self Document function

Self Document is a function of printing applications as documents.

Self Document enables the following things.

Selecting print data

Source files of work databases in an SCS project can be printed. All contents of the definitions or any parts can be selected.

The following table shows an outline of data which can be printed.

Table F2-1 Data to be printed

Data to be printed	Details of Definition
Cover	
Table of Contents	
SCS project information(*1)	Data defined with SCS Manager (Project/Configuration/Resource/Properties of each project)
SCS constant data	Data defined with SCS Constants Builder
I/O parameter data	Data defined with I/O Parameter Builder or AD Organizer
Subsystem communication I/O information (*2)	Data defined with Communication I/O Builder
SCS Link Transmission data	Data defined with SCS Link Transmission Builder
Global variable data	Data defined with SCS Manager (Global variable data)
Binding data	Data defined with SCS Manager (Binding data)
Modbus address information(*3)	Data defined with Modbus Address Builder
DNP3 communication definition information (*4)	Data defined with DNP3 Communication Builder
Tag name information (*5)	Data defined with Tag Name Builder
Alarm priority information(*5)	Data defined with Alarm Priority Builder
Alarm processing table information(*5)	Data defined with Alarm Processing Table Builder
POU data	• Data defined with SCS Manager • Data defined with Multi-Language Editor

*1: It includes the data concerning the CENTUM connection function.
*2: This is the data concerning the subsystem communication.
*3: This is the data concerning the open interface.
*4: Printable only when the version of SCSU1 is R3.02.20 or later.
*5: This is the data concerning the CENTUM connection function.

Customizing what to print

The content to print can be customized as follows:

- Cover and contents pages can be created.
- Headers and footers can be created.
- Page numbers can be included.
- Font types can be specified.

- Paper orientation (landscape or portrait) for FBD and LD can be specified.

Confirming preview

Printing images can be confirmed.

Selecting printer

A printer directly connected to SENG and connected via networks can be used.

Precautions for using self documents

Save files which are being edited before printing the application.

Self-documentation

Self-documentation is a function that allows printing applications out as documents. Use Document Generator to print documents.

TIP

In ProSafe-RS R2.02, self-documentation related behavior has been changed. If compatibility is important, you can choose the behavior before R2.02. In this document, the behavior before R2.02 is called "backward-compatible mode" and described separately.

Purposes of self-documentation

In order to compare the application logic prior to modification and the application logic after the modification, the applications can be printed out with self-documentation. The consistency between the contents displayed on the windows and the contents in the printouts can also be confirmed. The self-documentation function is independent of SCS Manager and each builder; it is thus possible to double-check that the applications have been created as intended.

By comparing the printout prior modification and the printout after modification, the result of the modification can be checked to confirm that the modification is properly performed.

Printing objects

Self-documentation prints out the source files of the work database in an SCS project. It is possible to select all the definitions or any part of them.

The printed objects are shown below.

- SCS project information (*1)
- SCS constants
- I/O parameters
- Communication I/O (*2)
- SCS Link Transmission
- Modbus address (*3)
- DNP3 communication
- Tag name (*4)
- Alarm priority (*4)
- Alarm processing table (*4)
- Variables cross reference index (*5)
- POU

*1: Including information related to integration with CENTUM

*2: Information related to connection with subsystems
*3: Information related to Modbus slave communication
*4: Information related to integration with CENTUM
*5: Not printed in backward-compatible mode

Customizing print settings

The contents that are printed by using the Self-documentation function can be customized for each SCS project. The customization function of R2.02 or later is different from that of a revision before R2.02.

IMPORTANT

The most preferable paper setting for printing the self-documentations is A3 size paper with landscape orientation. Therefore, you need to set the paper size to A3 and change the orientation to Landscape.

The printed information can be customized as follows.

- A cover page can be added
- A header or footer can be printed
- A page number can be printed
- Margin setting
- Font can be specified
- The printing orientation of the FBD and the LD (portrait or landscape) can be specified (*1)

*1: If the printer settings are already the A3 size paper with landscape orientation, these settings are not necessary.

Checking print preview

It is possible to check the printed image in advance.

Print target printer

It is possible to print out to a printer directly connected to the SENG or a printer connected via a network.

Relationship with SCS Manager and Builders

The relationship between self-documentation function and engineering functions (SCS Manager and builders) is illustrated below.

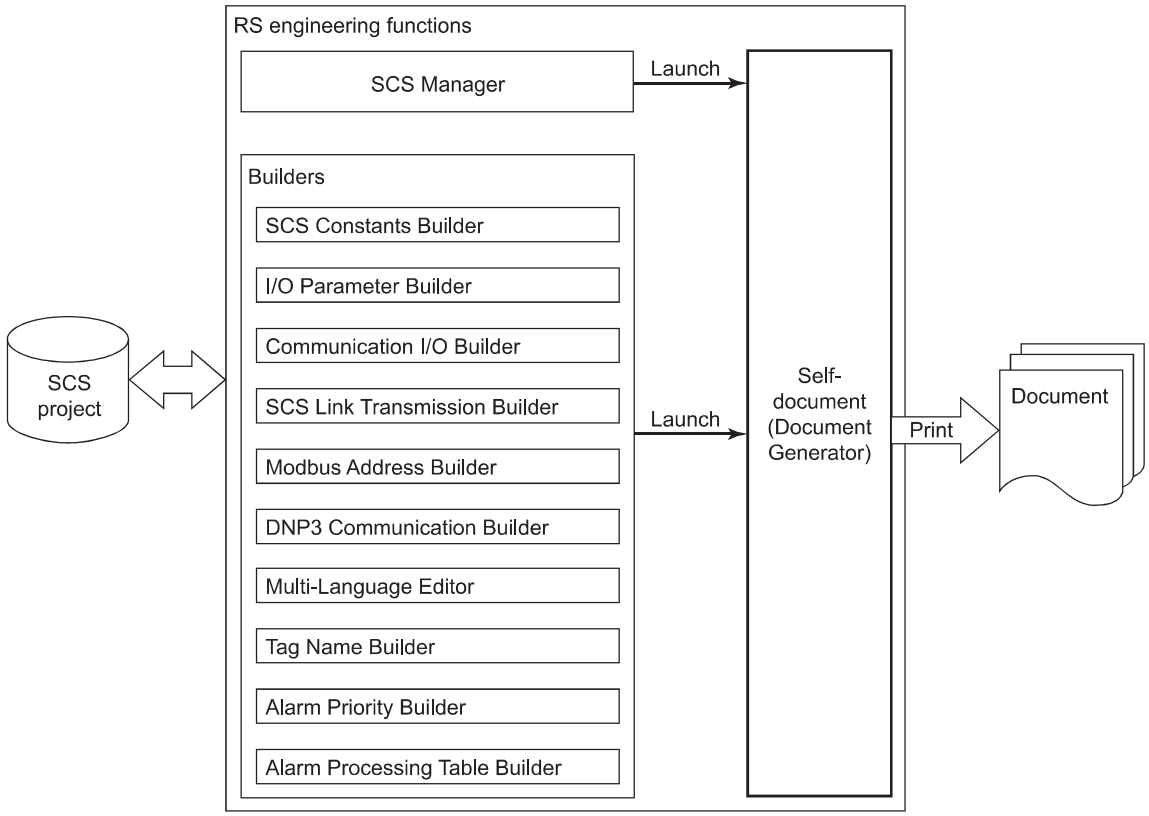


Figure F2-1 Relationship Between the Self-documentation Function and Engineering Functions

The self-documentation function is launched from SCS Manager or from any of the builders.

It allows printing definitions of SCS projects edited and saved in SCS Manager or each builder as documents.

TIP Definitions of CENTUM projects should be printed out with the self-documentation function of CENTUM.

Selecting printing mode

You can select the mode of printing by selecting the [Enhanced printing style] check box in the Customize dialog box, which is opened from the [Option] menu of SCS Manager. If the check box is cleared, self-documentation runs in backward-compatible mode and behaves the same as before R2.02.

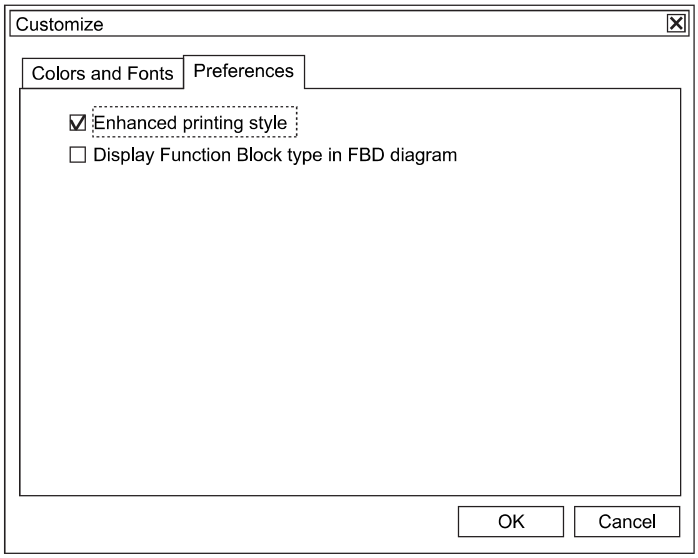


Figure F2-2 Customize dialog box

F2.1 Document Generator

Document Generator is the user interface of the self-documentation tool.

How to launch Document Generator

Document Generator can be launched by either one of the following operations.

- From the SCS Manager menu bar, select [File] > [Print], or click the "Print" button on the toolbar.
- From the menu bar of each builder, select [File] > [Print], or click the "Print" button on the toolbar.

Document Generator window structure



Figure F2.1-1 Document Generator window

Tabs

The window is composed of the following three tabs.

- "Table" tab: Select printing target

- "Options" tab: Customize print settings
- "Preview" tab: Preview printed information

If you click [Print] button in the Document Generator window, the Print dialog box appears. Select a printer and specify page settings such as paper size in the Print dialog box; then click [OK] button to start printing.

On Print dialog box, the range of pages to be printed can be set on [Page Range].

The relationship between the displayed tab and the specification method of page ranges that can be specified is shown below.

Table F2.1-1 Relationship between tabs and page ranges that can be specified

Tabs	[All]	[Current page]	[Pages] (*1)	[Sections] (*2)
Table	Specification allowed		Specification allowed	Specification allowed
Options	Specification allowed		Specification allowed	Specification allowed
Preview	Specification allowed	Specification allowed	Specification allowed	Specification allowed

*1: The printout page range can be specified with hyphen (-) or the pages can be separated by commas (,).
*2: The printout section range can be specified with hyphen (-) or the sections can be separated by commas (,).

SEE ALSO For more information about details of the "Table" tab sheet, refer to:

F2.2, “Selection of printing targets” on page F2-9

For more information about details of the "Options" tab sheet, refer to:

F2.3, “Customizing print settings” on page F2-14

For more information about details of the "Preview" tab sheet, refer to:

F2.6, “Confirmation by print preview” on page F2-34

Procedure of printing operations

The procedure of printing operations when using Document Generator is explained below.

1. Specify the printing targets in the "Table" tab.
2. Customize the print settings in the "Options" tab.
3. Click [Page Setup] and make printer settings in the Page Setup dialog box.
4. Display a print preview and check the printed information in the "Preview" tab.
5. Click [Print] button to print.

Page Setup dialog box

When you print using Document Generator, you can make printer settings in the Page Setup dialog box started from [Page Setup] on the [File] menu of SCS Manager. However, you cannot use the Page Setup dialog box in backward-compatible mode. The settings you have made in the Page Setup dialog box are reflected in the initial settings of Print dialog box of Document Generator. You can preview the image of the printout based on the settings of the Page Setup dialog box. Therefore, if you specify the printer usually used for printing in the Page Setup dialog box beforehand, the preview and printed results match. The settings in the Page Setup dialog box can be made for each computer. However, in the Page Setup dialog box, you cannot set Page Range.

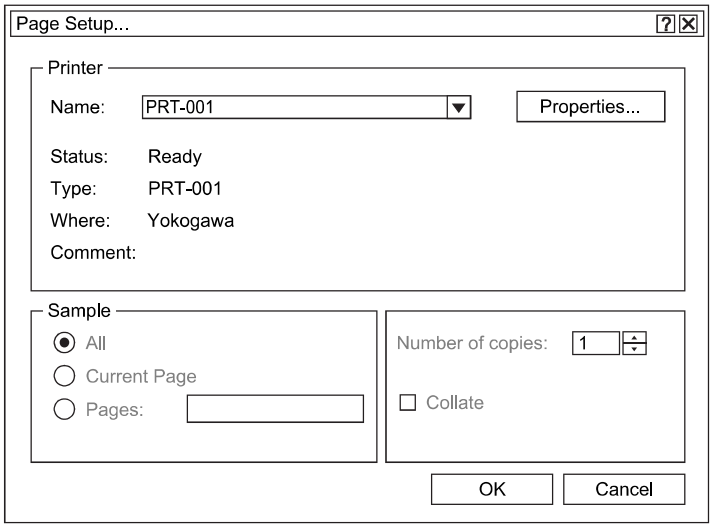


Figure F2.1-2 Page Setup dialog box

F2.2 Selection of printing targets

Select the printing targets in the "Table" tab of Document Generator.

Table tab



Figure F2.2-1 Table tab of Document Generator

Selecting printing targets in the Table tab

In the "Table" tab, you can select the definition items to be printed by Document Generator. Click the +/- buttons placed at the left edge of each item displayed in the tree view to display definition items and select the check boxes next to each definition you wish to print. For definition items that are selected in their check boxes, their data in the following table are printed.

Table F2.2-1 Printing objects

Chapter/ section Number (*1)	Definition item name in tree (*2)	Printed data	Remarks
	Cover Page	Cover page	-

Continues on the next page

Table F2.2-1 Printing objects (Table continued)

Chapter/ section Number (*1)	Definition item name in tree (*2)	Printed data	Remarks
	Table of contents	Table of contents	-
1	(Project name)	SCS project name	-
1.X	Project description	Comment for SCS project	-
1.X	Defined words	Defined words	-
2	(Configuration name)	Configuration name and comment	-
2.X	Description	Description for configuration	-
2.X	SCS project information	SCS project information	The CENTUM project top folder is printed when CENTUM is connected to the system. For a library project, only the version number is printed.
2.X	SCS constants	SCS constant definition	(*3)
3	(Resource name)	Resource name and comment	-
3.X	Description and Properties	Description for resource	-
3.X	Global Variables	List of global variables	-
3.X	I/O Modules	Node and input/output module information	(*3)
3.X	I/O Parameters	Input/output module information (wiring information and parameters)	(*3)
3.X	Comm. I/O definition	Subsystem communication I/Os	(*3)
3.X	Comm. I/O wiring	Subsystem communication I/O wirings	(*3)
3.X	Safety Subsystem Comm. I/O Definition	Fire and gas communication definition information	(*3)
3.X	Safety Subsystem Comm. I/O Wiring	Fire and gas communication wiring information	(*3)
3.X	Modbus address (Coil)	Modbus address information	(*3)
3.X	Modbus address (Input relay)		
3.X	Modbus address (Input registers)		
3.X	Modbus address (Holding registers)		

Continues on the next page

Table F2.2-1 Printing objects (Table continued)

Chapter/ section Number (*1)	Definition item name in tree (*2)	Printed data	Remarks
3.X	DNP3 communication (Parameters)	DNP3 communication	It can be printed for the SCS projects of SCSU1 that are created by the software version R3.02.20 or later.
3.X	DNP3 communication (Binary Input)		
3.X	DNP3 communication (Binary Output)		
3.X	DNP3 communication (Binary Counter)		
3.X	DNP3 communication (Analog Input)		
3.X	DNP3 communication (Analog Output)		
3.X	SCS Link Transmission	SCS Link Transmission definition	(*3)
3.X	SCS Link Transmission Wiring	SCS Link Transmission data wirings	(*3)
3.X	Detailed binding	Binding information	(*3)
3.X	Tag name definition (BOOL/ ECW_B)	Tag name definition	(*3) It can only be printed for a system with CENTUM integration structure. (*4)
3.X	Tag name definition (DINT/ REAL/ECW_I/ECW_R)		
3.X	Tag name definition (ANLGI/ ANLG_S)		
3.X	Tag name definition (VEL)		
3.X	Tag name definition (ANN)		
3.X	Tag name definition (IO_REAL)		
3.X	Tag name definition (IO_BOOL)		
3.X	Tag name definition (GOV_B/ GOV_IB/OVR_B/OVR_IB)		
3.X	Tag name definition (OVR_I/ OVR_R/OVR_IR)		
3.X	Tag name definition (PASSWD)		
3.X	Tag name definition (SCI_B/ SCO_B)		
3.X	Tag name definition (SCI_I/ SCO_I/ SCI_R/SCO_R)		
3.X	Tag name definition (MOB_11/ MOB_21)		
3.X	Tag name definition (MOB_RS)		
3.X	Tag name definition (MOA)		
3.X	Alarm priority	Alarm priority	
3.X	Alarm processing table	Alarm processing table	
3.X	Resource content	POU list (*5)	-

Continues on the next page

Table F2.2-1 Printing objects (Table continued)

Chapter/ section Number (*1)	Definition item name in tree (*2)	Printed data	Remarks
3.X	Local Variables + Parameters	List of local variables and parameters	-
4	POU	(Title only)	-
4.X	(POU)	POU name	One POU corresponds to one section.
5	Variables cross reference index	Variables cross reference index (Titles only)	(*3)
5.X	Hardware I/O	I/O variables cross reference index	(*3)
5.X	Global Variables	Global variables cross reference index	(*3)
5.X	Tag names	Tagged variables cross reference index	(*3)

*1: Chapter and section numbers vary depending on the selected printing objects. If the item selected as printing object contains no content, nothing is printed. X means a serial number starting at 1. The start page for print can be changed.
*2: Definition item names in tree are printed as the title character strings of chapters and sections (except for the cover page).
*3: For library project, the tree view is not displayed. Moreover, the Print command is not valid.
*4: Displayed in the tree view if the PC has a license for CENTUM VP Integration Engineering Package.
*5: Description of each POU is also printed.

Outputting Variables Cross Reference Index

To print variables cross reference information, click the [Table] tab in Document Generator, and select [Variable cross reference index] or select from among the individual items of [Hardware I/O], [Global Variables], [Tag Names] that are shown under [Variable cross reference index].

In variables cross reference index, information on which variables are used by which POU is listed. The following information can be output.

Table F2.2-2 Information output as variables cross reference index

Definition item name in tree	Global variables (instance)	Local variables	FB parameters
Hardware I/O (I/O variables in IO_BOOL and IO_REAL)	Output	Output	Not output
Global variables (in BOOL/DINT/REAL)	Output	Not output	Not output
Tag Names (*1)	Output	Output	Output

*1: All the variables, FB instances, and parameters to which a tag name is assigned are output. However, ANNs are output even if tag names are not assigned.

Each report contains the following data.

- Name:
  For parameters, name is output with the FB instance name. For example, "FB1.Param." If the scope of a variable is set to Local, name is output with the POU name. For example, "Var1@POU" is output.
- Type:
  Type name such as ANN and BOOL is output.
- Direction:
  Input, Output or Internal is output.
- Tag Name:
  For ANN, %AN element name is also output.

- Sheet Number:
  Sheet number is output in the format "POU name - page number."

TIP

No matter whether you have selected POU as the data to be printed or not, cross reference information is printed for all POUs. Regardless of the actual setting of [New page for each item] in the [Options] tab of Document Generator, documents are printed with a page break inserted at the end of each POU.

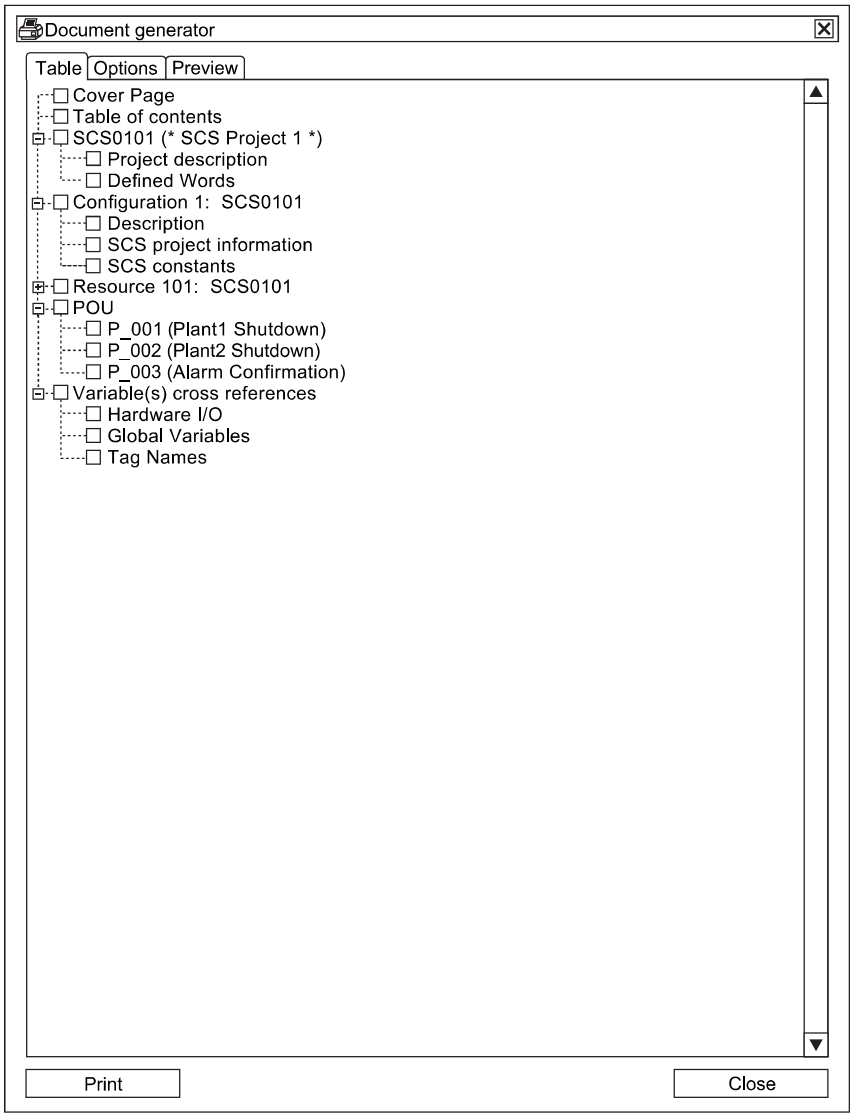


Figure F2.2-2 Variable Cross Reference Index window

F2.3 Customizing print settings

You can customize the information to be printed in the Options tab of Document Generator.

F2.3.1 Customizable print settings

To customize, click a button in each group box in the Options tab of Document Generator.

Options tab

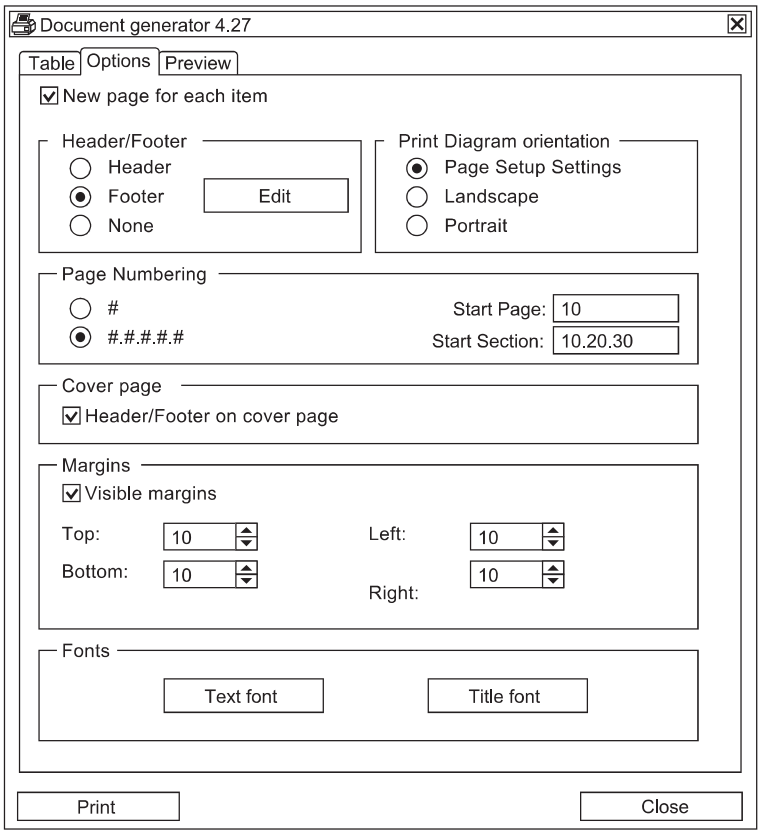


Figure F2.3.1-1 Options tab page

The components of the tab are explained in the following sections.

New page for each item

Select this check box to start a new page for each printed item. If [Landscape] is selected at "Print Diagram orientation", FBD and LD begin on a new page even if the [New page for each item] check box is not selected.

IMPORTANT

If you print after you change print settings in either the Options tab in Document Generator or the Print dialog box shown when you click the Print button in Document Generator, page breaks may be inserted in places different from those that you see on the screen.

Print diagram orientation

Select one of the three options, and the documents will be printed as specified.

- Page Setup Settings
  FBD and LD are also printed according to the settings in the Page Setup dialog box or Print dialog box.
- Landscape

FBD and LD are printed in landscape orientation regardless of the settings in the Page Setup dialog box or Print dialog box. Other print items are printed according to the settings in the Page Setup dialog box or Print dialog box.

- Portrait
  FBD and LD are printed in portrait orientation regardless of the settings in the Page Setup dialog box or Print dialog box. Other print items are printed according to the settings in the Page Setup dialog box or Print dialog box.

Header/Footer

You can make settings for a header or footer. You can select to print a header (at the top of the page) or a footer (at the bottom of the page) or not to print any of them. Click [Edit] button and the dialog box for editing Header/Footer appears.

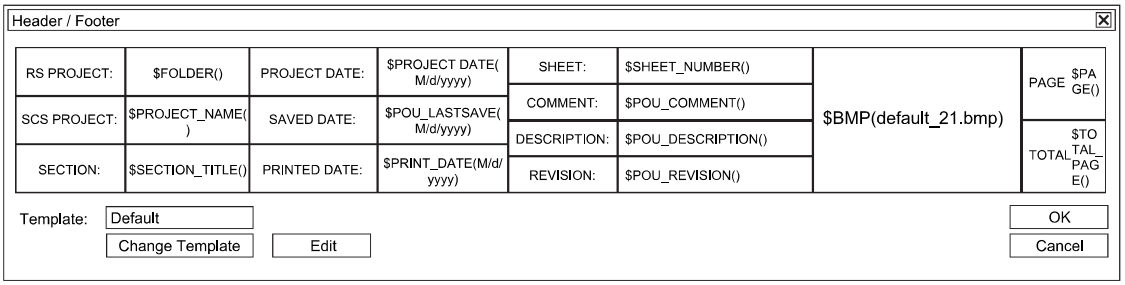


Figure F2.3.1-2 Dialog Box for editing Header/Footer

In the dialog box for editing Header/Footer, you can customize the following.

- Select a Header/Footer template.
- Change print properties of a Header/Footer template.

SEE ALSO For more information about details on customizing the header/footer, refer to:

F2.3.2, “Editing header and footer” on page F2-19

Page numbering

Specify the format of the page numbers printed in the header or footer, and the page number for the first page.
Use either of the following page number formats.

- [#]
  Page numbers are printed using the format of "Page 'page number'" (serial number). Serial numbers are assigned to pages starting from the first page. Specify the page number from which printing is to be started by entering it in [Start Page:].
- [#.#.#.#.#]
  Page numbers are printed using the format of "Page 'section/chapter number' - 'page number'" (section format). Serial numbers are assigned to pages starting from the first page for each chapter/section. Specify the section number from which printing is to be started by entering it in [Start Section:]. Note that the cover page and the table of contents are always numbered from page 1 (i).
  - The page numbers for the cover page and table of contents are printed using Roman numerals (i, ii, iii, iv, ...).
  - Each chapter after that (project data, configuration data, resource data, POU data, variable cross reference index data) is numbered in the format "Chapter- page number" or "Chapter. Section- page number."

TIP

If you want to reprint a part of the project so as to replace the old printouts after the contents of the whole SCS project were printed out, follow the procedure below:

1. In the Table tab, choose the items to be printed.
2. In the Options tab, choose [#.#.#.#.#.] at Page Numbering.
3. In [Start Section], specify the chapter and section numbers for the items you want to reprint.
4. Click [Print]. The Print dialog box appears.
5. In the Print dialog box, select [All] for [Page Range:]. Then only the specified part of the project will be printed out.

Cover page

Specify the format of the cover page.
If you check the [Header/Footer on cover page], header or footer is printed on the cover page in the format specified in the [Header/Footer] section.

Margins

Specify the printing margins of each page. The printing margins are the offsets at the top/bottom/left/right sides of the page from the perimeter of the maximum printable area.

- "Visible Margins"
  Specify whether or not to print the printing margin frame. If you select the check box, a frame showing the printing margins is printed on each page.
- "Top", "Bottom", "Left", "Right"
  Specify the margin width for the top, button, left and right margin in units of mm, respectively.

Fonts

Specify the font used in printing. The specified font is used for texts except for those shown in FBD and LD windows.

- [Text font] button
  Click the [Text font] button to show the Text Font dialog box. The font selected in this dialog box is used for texts except for those shown in FBD and LD windows (including table of contents and chapter titles and section titles).
- [Title font] button
  Click the [Title font] button to show the Title Font dialog box. The font selected in this dialog box is used for the cover page.

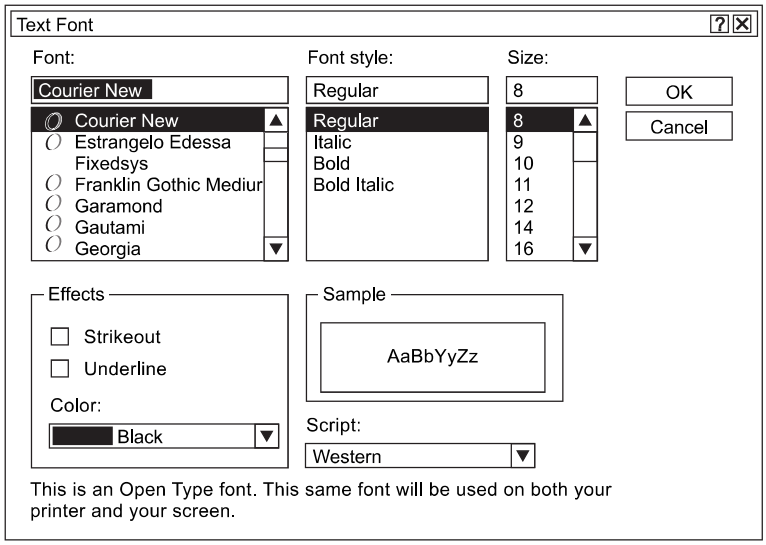


Figure F2.3.1-3 Text Font dialog box

[Font style], [Effects] and [Script] settings are invalid.

IMPORTANT

The self-documentation function prints data in the files saved by SCS Manager and builders. For this reason, if you attempt to save files while the self-documentation is running, incorrect information may be printed or the printing process may fail. In such cases, run the self-documentation again after completing saving the files.

F2.3.2 Editing header and footer

To customize Header/Footer, start the Header/Footer dialog box by clicking the [Edit] button in the [Header/Footer] group box in the [Options] tab in Document Generator.

Selecting a Header/Footer template

The following 8 types of Header/Footer templates are provided. You can select the one you like.

Table F2.3.2-1 Template list

Templates	Remarks
Default	Default template
Template_1	-
Template_2	-
Template_3	-
Template_4	-
Template_5	-
Template_A	Equivalent to Format A in backward-compatible mode
Template_B	Equivalent to Format B in backward-compatible mode

Follow the steps below to select a Header/Footer template.

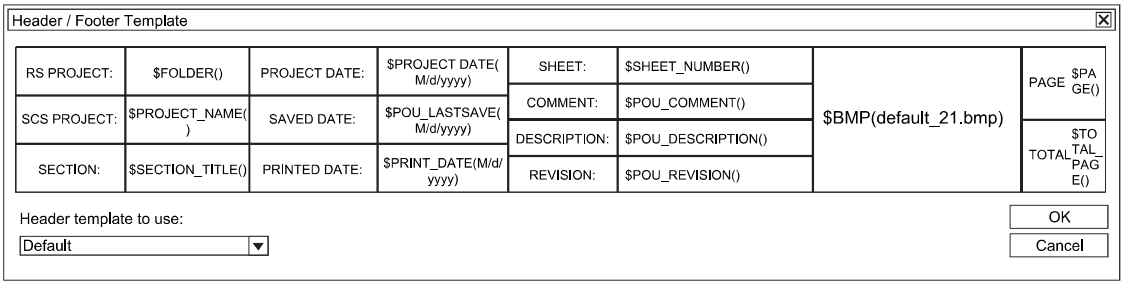


Figure F2.3.2-1 Template Selection dialog box

1. In the Header/Footer dialog box, click the [Change Template] button to open the Template selection dialog box.
2. In the list box in the Template selection dialog box, select a template you want to use. A preview of the selected template appears.
3. In the Template selection dialog box, click the [OK] button and the selected template is applied.
   Click [Cancel] to cancel your selection and the Template selection dialog box closes.

   Name of the selected template appears in the Header/Footer dialog box, and a preview of the template is shown.
4. In Header/Footer dialog box, click the [OK] button and the Header/Footer of the selected template is used in printing.
   If you click the [Cancel] button, Header/Footer is not changed. The [OK] button in the Header/Footer dialog box becomes valid only after you click the [OK] button in the Template selection dialog box in step 3.

Editing Header/Footer properties

To edit Header/Footer print properties, open the Change Print Items dialog box and follow the steps below.

1. In the Header/Footer dialog box, click the [Edit] button to show the Change Print Items dialog box.
2. In the Change Print Items dialog box, edit Header/Footer properties.
3. Click the [OK] button in the Change Print Items dialog box, and the changes you make in the dialog box are applied.
   If you want to cancel the changes, click the [Cancel] button.

   Result of your editing is shown in a preview in the Header/Footer dialog box. In the area where nothing is to be printed, the area number is shown.
4. In the Header/Footer dialog box, click the [OK] button, and the edited Header/Footer are used in printing.
   If you click the [Cancel] button, Header/Footer is not changed. The [OK] button in the Header/Footer dialog box becomes valid only after you click the [OK] button in the Change Print Items dialog box in step 3.

IMPORTANT

If you re-select a template after changing Header/Footer print properties, the changes are undone.

Change Print Items dialog box

To change the Header/Footer print properties, use the Change Print Items dialog box. One of the following is printable in the template Header/Footer area.

- Macro
- Fixed character strings (blank strings are allowed)
- Combination of macro and fixed character strings
- Bitmaps

If character strings are printed, you can specify font size (4 point to 72 point) of the character strings. Font is fixed to the one specified in [Title font] in the Options tab in Document Generator.

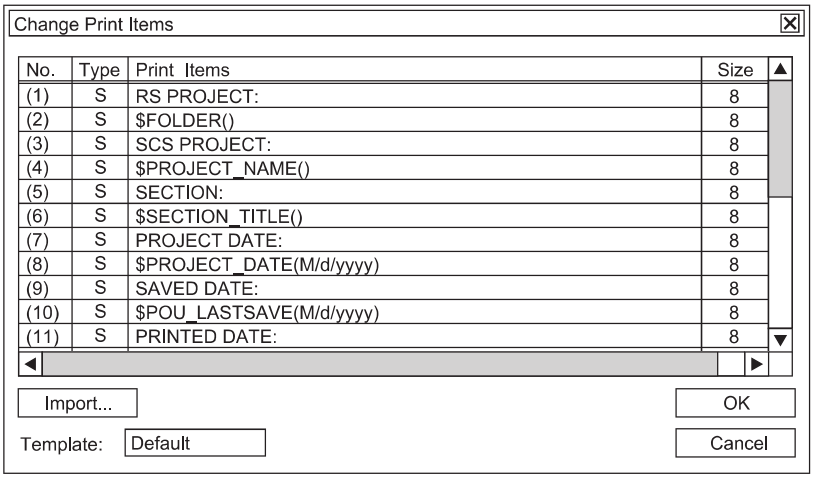


Figure F2.3.2-2 Change Print Items dialog box

The following section describes components of the Change Print Items dialog box.

No.

Shows the area number for a print item in a template. If no print item is specified, this number is shown in a preview.

Type

Shows the type of a print item.

- S: character string (Macro, fixed character strings, or combination of both)
- B: Bitmap

Print item

Specify the details for a print item. Settings are different depending on whether the "type" is S (character string) or B (bitmap).
When "type" is S (string): Displays the character string to be printed (macro, fixed string, or a combination of these).

- Click on a line with the left-button of your mouse and you can edit the character string in it.
- Select a line and right-click your mouse, and the following pop-up menu appears.

  Cut : cuts the selected character string.

  Copy : copies the selected character string.

  Paste : pastes the cut or copied character string.

  Delete : deletes the selected character string.

  If you select $FOLDER( ) or one of the commands listed below it, the corresponding macro is inserted at the point where the mouse cursor is blinking. After inserting, you can edit the character string.

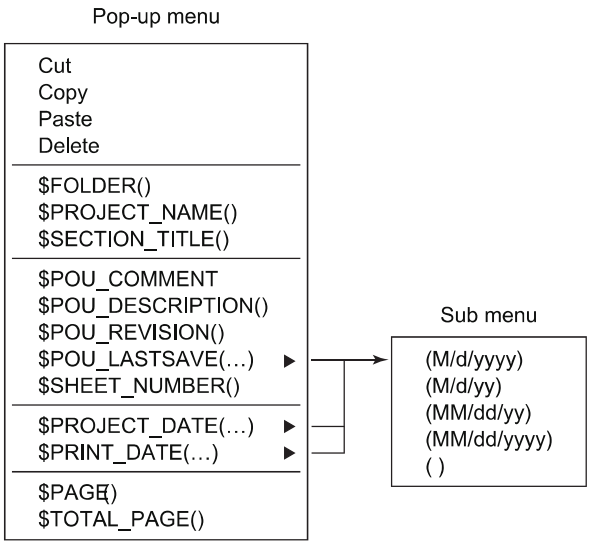


Figure F2.3.2-3 Pop-up menu and sub menu

When "type" is B (bitmap): Bitmap file name. Specify a .bmp file under the following folder.

`{Project folder}\YOKOGAWA_SCS\SELDOC\`

- Click a file name with the left button on your mouse, and you can edit it.
- Left-click the mouse and click the […] button that appears, and a file selection dialog box appears. Select a file.

Size

Font size (point) of character strings for an item of Type S (character string). Type an integer from 4 to 72 or select a size from the combo box.

Template

The name of the currently selected template is shown.

Editing Header/Footer

You can edit the Header/Footer of the selected template. The items that can be printed in the Header/Footer are macro (character string), fixed character strings, and a combination of macro and fixed character strings, and bitmap.

For example, if you specify "$PROJECT_NAME()," the actual SCS project name (or library name) is printed.

If you specify the combination of a fixed character string "Page" and macro "$PAGE" by entering "Page$PAGE()," page number will be printed in the format such as "Page 4.1-1."

If you specify one of the macros listed below or one of these macros combined with a fixed character string, the printing will come out only on the POU source pages. On the other pages, nothing is printed.

"$POU_COMMENT( )", "$POU_DESCRIPTION( )", "$POU_REVISION( )", "$POU_LASTSAVE(format)", "$SHEET_NUMBER( )"

$POU_COMMENT( )

Comment of the POU shown in the page

Example:

First Comment

$POU_DESCRIPTION( )

Description of POU shown in the page

Example:

First description

$POU_REVISION( )

Revision comment of the POU shown in the page

POU revision comment is entered and displayed in the POU Properties dialog box. The entered comment is printed as the POU revision comment in the position where this macro is specified.

Example:

First Revision

$POU_LASTSAVE(format)

Date when the shown POU is last saved or imported. Same as the "Date Modified" shown in Windows Explorer. You can specify the output format of the date by entering the format in the parenthesis of this macro as shown below.

- The following alphabets in the format stand for Year/Month/date.
- Characters other than the alphabets that stand for Year/Month/date are output as they are.
- If you want to output the alphabets that stand for Year/Month/date, enclose them with single quotation marks (').

Table F2.3.2-2 Rules for Date Format Specification

d	date
dd	date. For one digit number, 0 is filled in the tenths place.
M	Month (numeral)
MM	Month (numeral). For one digit number, 0 is filled in the tenths place.
MMM	Month (abbreviated character string). Example: Jan
MMMM	Month (character string). Example: January
y	year (last two digits). The zero for the tens place is not output.
yy	year (last two digits). The zero for the tens place is output.
yyyy	Year (western calendar)

Example format
$POU_LASTSAVE(MMM-d) Apr-6

$SHEET_NUMBER( )

Sheet number. It consists of POU name and POU page number ("POU name - page number"). If a diagram is printed over two pages or more, the first page has the page number 1, the second page, 2 and so on.

Example:

POU_A-1

$PROJECT_DATE(format)

Project date.

Project date is entered and displayed in the Project Properties dialog box. The entered value is printed in the position where this macro is specified as the project date. Like the $POU_LASTSAVE, you can specify the format.

- **$PRINT_DATE(format)**

Date of printing. The date when the document is printed. Like the $POU_LASTSAVE, you can specify the format.

- **$PAGE( )**

Page number or page number with section number. Page numbers are printed according to the setting of [Page Numbering] in Document Generator.

- If [#] (serial number format) is specified for [Page Numbering], serial number is used for page number.
  Example:
  7
- If [#.#.#.#.#.#] (section format) is specified for [Page Numbering], the page number is a combination of section number and page number within the section.
  Example:
  4.1-1

- **$TOTAL_PAGE( )**

Total number of pages to be printed. Same as the total number of pages that is printed when [#/ total number of pages] is selected for [Page Numbering] in Document Generator in backward-compatible mode (that is, [Enhanced printing style] in the Customize dialog box is set to OFF).

Example:

23

- **$PROJECT_NAME( )**

SCS project name or library name

Example:

SCS0101 or LIBRARY1

- **$FOLDER( )**

Folder name (=RS Project name) where the project is stored.

Example:

MYRSPJT

- **$SECTION_TITLE( )**

The character string "Project" for a chapter on Project. The character string "Configuration" for a chapter on configuration. The character string "Resource" for a section on Resource. The character string "POU" for a section on POU.

Example:

Configuration

Importing Header/Footer from another project

In the Change Print Items dialog box, the Header/Footer of another project can be imported. You can use the same Header/Footer as that used in another project in a new project by using Import function.

1. Select in advance, the same template as the Header/Footer of another project you want to import.
2. Click the [Import…] button.
   Folder selection dialog box appears.
3. Select SCS project or library folder, and click the [OK] button.
   The print properties of the project are reflected to the selected template of the new project. If bitmaps are included in the Header/Footer template of the selected project, the bitmap file is copied in the predefined folder of the new project (`{Project folder}\YOKOGAWA_SCS\SELDOC\`)

IMPORTANT

- If the Header/Footer template of the selected project does not exist or the template in the new project is different, a message box appears and import is not executed. If the template of the new project differs from that of the selected project, the name of the template specified in the project the system failed to import is shown, select the same template for the new project and import again.
- If a bitmap file of the same name already exists in the folder of the new project (`{Project folder}\YOKOGAWA_SCS\SELDOC\`), a dialog box appears asking you if it is all right to overwrite the bitmap file. If you click the [OK] button for all bitmap files to be imported, the import proceeds. If you click the [Cancel] button for any of them, import is not executed.

F2.4 Selection of printing targets (Backward-compatible mode)

Select the printing targets in the "Table" tab of Document Generator.

Table tab

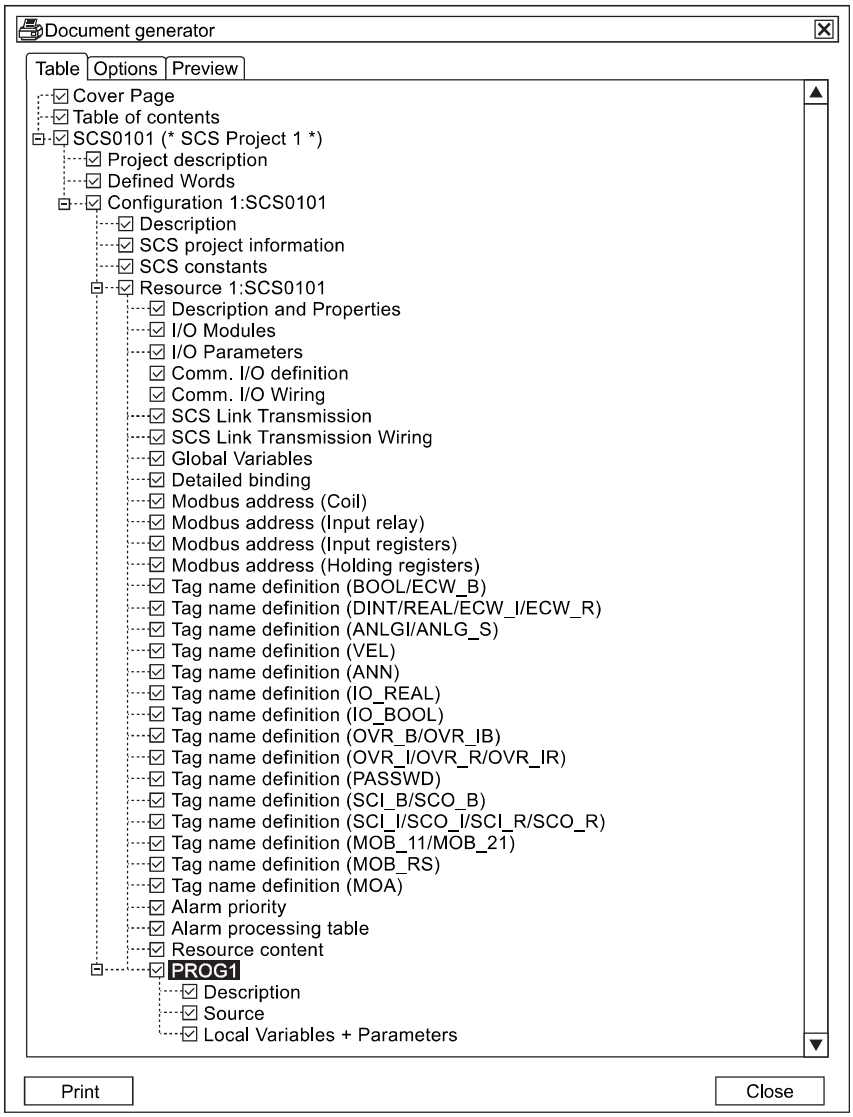


Figure F2.4-1 Table tab of Document Generator

Selecting printing targets in the Table tab

In the "Table" tab, you can select the definition items to be printed by Document Generator. Click the +/- buttons placed at the left edge of each item displayed in the tree view to display definition items and select the check boxes next to each definition you wish to print. For definition items that are selected in their check boxes, their data in the following table are printed.

Table F2.4-1 Printing objects (for compatible mode)

Chapter/ section Number (*1)	Definition item name in tree (*2)	Printed data	Remarks
	Cover Page	Cover page	-
	Table of contents	Table of contents	-
1	(Project name)	SCS project name	-
1.1	Project description	Comment for SCS project	-
1.2	Defined words	Defined words	-
1.3	(Configuration name)	Configuration name and comment	-
1.3.1	Description	Description for configuration	-
1.3.2	SCS project information	SCS project information	The CENTUM project top folder is printed when CENTUM is connected to the system. For a library project, only the version number is printed.
1.3.3	SCS constants	SCS constant definition	(*3)
1.3.4	(Resource name)	Resource name and comment	-
1.3.4.X	Description and Properties	Description for resource	-
1.3.4.X	I/O Modules	Node and input/output module information	(*3)
1.3.4.X	I/O Parameters	Input/output module information (wiring information and parameters)	(*3)
1.3.4.X	Comm. I/O definition	Subsystem communication I/Os	(*3)
1.3.4.X	Comm. I/O wiring	Subsystem communication I/O wirings	(*3)
1.3.4.X	Fire and gas communication definition	Fire and gas communication definition information	(*3)
1.3.4.X	Fire and gas communication wiring	Fire and gas communication wiring information	(*3)
1.3.4.X	SCS Link Transmission	SCS Link Transmission definition	(*3)
1.3.4.X	SCS Link Transmission Wiring	SCS Link Transmission data wirings	(*3)
1.3.4.X	Global Variables	List of global variables	
1.3.4.X	Detailed binding	Binding information	(*3)
1.3.4.X	Modbus address (Coil)	Modbus address information	(*3)
1.3.4.X	Modbus address (Input relay)		
1.3.4.X	Modbus address (Input registers)		
1.3.4.X	Modbus address (Holding registers)		

Continues on the next page

Table F2.4-1 Printing objects (for compatible mode) (Table continued)

Chapter/ section Number (*1)	Definition item name in tree (*2)	Printed data	Remarks
1.3.4.X	DNP3 communication (Parameters)	DNP3 communication	It can be printed for the SCS projects of SCSU1 that are created by the software version R3.02.20 or later.
1.3.4.X	DNP3 communication (Binary Input)		
1.3.4.X	DNP3 communication (Binary Output)		
1.3.4.X	DNP3 communication (Binary Counter)		
1.3.4.X	DNP3 communication (Analog Input)		
1.3.4.X	DNP3 communication (Analog Output)		
1.3.4.X	Tag name definition (BOOL/ ECW_B)	Tag name definition	(*3) It can only be printed for a system with CENTUM integration structure. (*4)
1.3.4.X	Tag name definition (DINT/ REAL/ECW_I/ECW_R)		
1.3.4.X	Tag name definition (ANLGI/ ANLG_S)		
1.3.4.X	Tag name definition (VEL)		
1.3.4.X	Tag name definition (ANN)		
1.3.4.X	Tag name definition (IO_REAL)		
1.3.4.X	Tag name definition (IO_BOOL)		
1.3.4.X	Tag name definition (GOV_B/ GOV_IB/OVR_B/OVR_IB)		
1.3.4.X	Tag name definition (OVR_I/ OVR_R/OVR_IR)		
1.3.4.X	Tag name definition (PASSWD)		
1.3.4.X	Tag name definition (SCI_B/ SCO_B)		
1.3.4.X	Tag name definition (SCI_I/ SCO_I/ SCI_R/SCO_R)		
1.3.4.X	Tag name definition (MOB_11/ MOB_21)		
1.3.4.X	Tag name definition (MOB_RS)		
1.3.4.X	Tag name definition (MOA)		
1.3.4.X	Alarm priority	Alarm priority	(*3) It can be printed only for a system with CENTUM integration structure. (*4)
1.3.4.X	Alarm processing table	Alarm processing table	
1.3.4.X	Resource content	POU list	-
1.3.4.X	(POU)	POU name	One POU corresponds to one item.
1.3.4.X.X	Description	Description for POU	-

Continues on the next page

Table F2.4-1 Printing objects (for compatible mode) (Table continued)

Chapter/ section Number (*1)	Definition item name in tree (*2)	Printed data	Remarks
1.3.4.X.X	Source	FBD/LD/ST	-
1.3.4.X.X	Local Variables + Parameters	List of local variables and parameters	-

*1: Chapter and section numbers vary depending on the selected printing objects. If the item selected as printing object contains no content, nothing is printed. X means a serial number starting at 1. The start page for print can be changed.
*2: Definition item names in tree are printed as the title character strings of chapters and sections (except for the cover page).
*3: For library project, the tree view is not displayed. Moreover, the Print command is not valid.
*4: Not displayed in the tree view if the PC does not have a license for CENTUM VP Integration Engineering Package.

SEE ALSO For more information about the method for changing the start page for print, refer to:

"● Page numbering" on page F2-32

F2.5 Customizing print settings (backward-compatible mode)

You can customize the information to be printed in the Options tab of Document Generator.

In ProSafe-RS R2.02, self-documentation related behavior has been changed. If compatibility is important, you can choose the behavior in before R2.02. In this document, the behavior in before R2.02 is called "backward-compatible mode."

Options tab

This section explains how to customize printing in backwards-compatible mode.

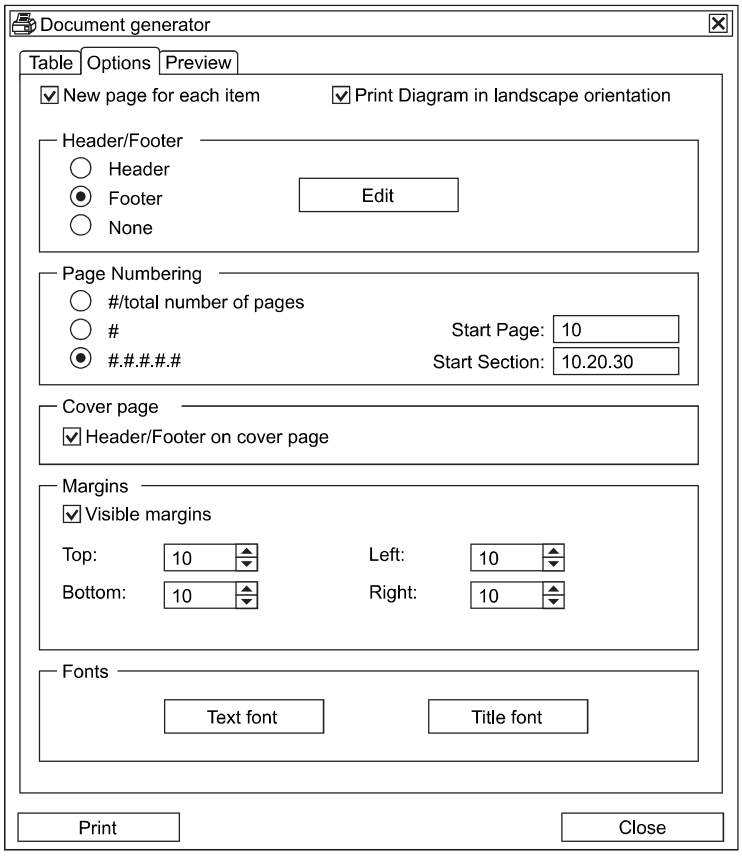


Figure F2.5-1 Options tab of Document Generator

The components of the tab are explained in the following sections.

New page for each item

Select this check box to start a new page for each printed item. If the [Print Diagram in landscape orientation] check box is selected, the FBD and the LD begin on a new page even if the [New page for each item] check box is not selected.

Print diagram in landscape orientation

If you select this check box, the FBD and the LD are printed in horizontal (landscape) orientation regardless of the default setting of the printer and specification in the Print dialog box. Other printing items follow the default settings of the printer and specifications in the Print dialog box.

Header/Footer

You can make settings for a header or footer. Select to print either the header (at the top of the page) or footer (at the bottom of the page) or not to print both. Click [Edit] button. The following dialog box appears, where you can edit the header or footer.

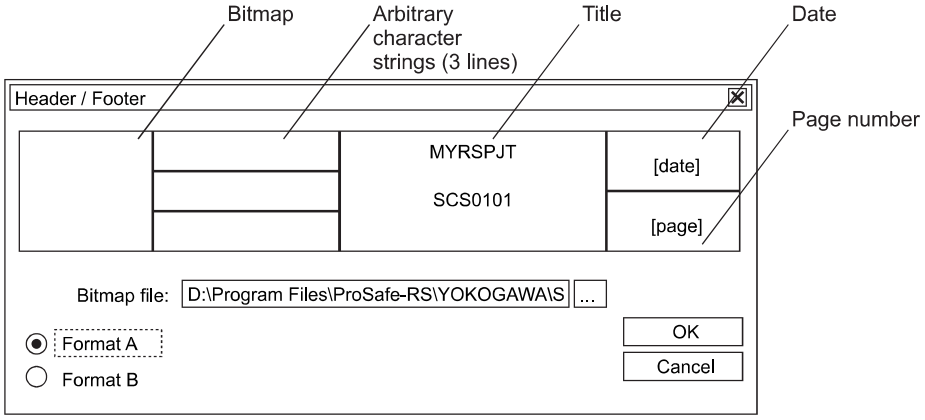


Figure F2.5-2 Header/Footer dialog box (Format A)

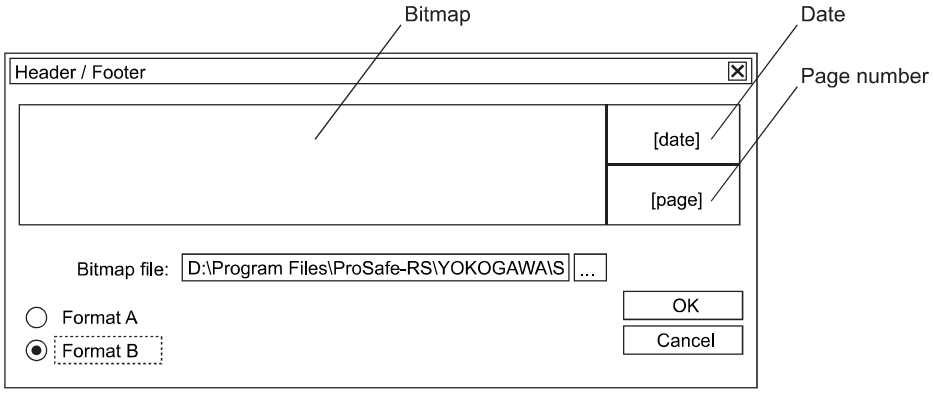


Figure F2.5-3 Header/Footer dialog box (Format B)

In the Header/Footer dialog box, check the header or footer and click [OK] button. Set the specified header or footer to be printed on each page.

There are two types of formats for the header or footer. Specify either [Format A] or [Format B].

Specify the printed items as shown below.

- Bitmap (formats A and B)
  Specify the path name of the bitmap file you want to use in the [Bitmap file:] field. It is also possible to click [...] button to select a path name using the "Open" dialog box.
- Arbitrary character strings (only for format A)
  It is possible to enter a character string directly in each of the three lines. The character strings entered are printed in the header or footer.
- Title (only for format A)
  This is the same character string as the title string. The following information is printed. These strings are also printed on the cover page.

  First line: Cannot be edited (RS project name)

  Second line: Can be edited (default: SCS project name)

  Third line: Can be edited (default: explanation of the project)
- Date (formats A and B)

The date on which the printing was done is printed out. The date format follows the default format of the locale selected in "Regional Options" of the Windows.

- Page numbers (formats A and B)
  The page numbers are printed. The format of page numbers used is the format selected in the "Options" tab.

Page numbering

Specify the format of the page numbers printed in the header or footer, and the page number for the first page.
Use either of the following page number formats.

- [# / total number of pages]
  Page numbers are printed using the format of "page number/total number of pages" (serial number along with the total number of pages). Serial numbers are assigned to pages starting from the first page.
- [#]
  Page numbers are printed using the format of "Page 'page number'" (serial number). Serial numbers are assigned to pages starting from the first page. Specify the page number from which printing is to be started by entering it in [Start Page:].
- [#.#.#.#.#]
  Page numbers are printed using the format of "chapter number.section number.page number" (section format). Serial numbers are assigned to pages starting from the first page for each chapter/section. Specify the section number from which printing is to be started by entering it in [Start Section:]. Note that the cover page and the table of contents are always numbered from page 1 (i).
  - The page numbers for the cover page and table of contents are printed using Roman numerals (i, ii, iii, iv, ...).
  - The project information is printed using the "9.9" format.
  - The configuration information is printed using the "9.9.9" format.
  - The resource information is printed using the "9.9.9.9" format.
  - The POU information is printed using the "9.9.9.9.9" format.
  - The information in lower hierarchy than POU is printed using the "9.9.9.9.9.9" format.

TIP

If you want to reprint a part of the project so as to replace the old printouts after the contents of the whole SCS project were printed out, follow the procedure below:

1. In the Table tab, choose the items to be printed.
2. In the Options tab, choose [#.#.#.#.#.] at Page Numbering.
3. In [Start Section], specify the chapter and section numbers for the items you want to reprint.
4. Click [Print]. The Print dialog box appears.
5. In the Print dialog box, select [All] for [Page Range:]. Then only the specified part of the project will be printed out.

Cover page

Specify the format of the cover page.
If you check the [Header/Footer on cover page], header or footer is printed on the cover page in the format specified in the [Header/Footer] section.

Margins

Specify the printing margins of each page. The printing margins are the offsets at the top/bottom/left/right sides of the page from the perimeter of the maximum printable area.

- "Visible Margins"
  Specify whether or not to print the printing margin frame. If you select the check box, a frame showing the printing margins is printed on each page.
- "Top", "Bottom", "Left", "Right"
  Specify the margin width for the top, button, left and right margin in units of mm, respectively.

Fonts

Specify the font used in printing. The font specification applies to text used for information displayed except for the FBD, the LD and the ST of Multi-Language Editor.

- "Text font"
  Click [Text font] button to display the Text font dialog box. The font selected in this dialog box is used as the font for the table of contents and titles of chapters and sections.
- "Title font"
  Click [Title font] button to display the Title font dialog box. The font selected in this dialog box is used as the font for the cover page.

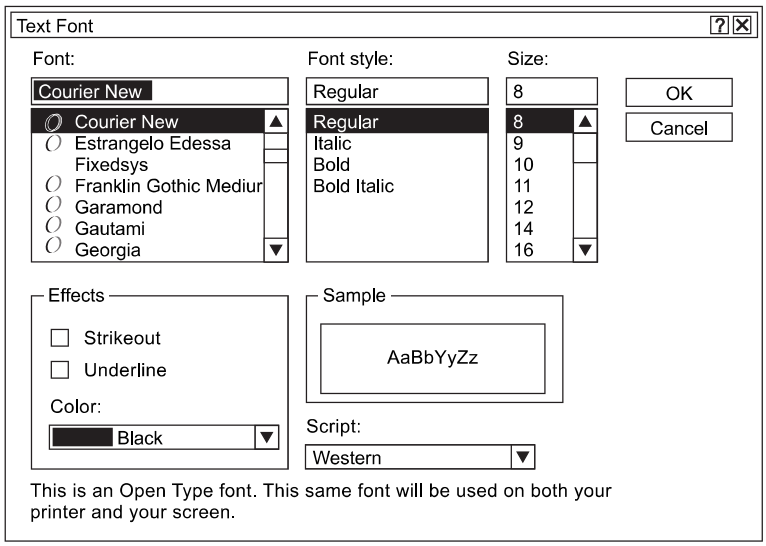


Figure F2.5-4 Text Font dialog box

TIP

[Font style], [Effects] and [Script] settings are invalid.

IMPORTANT

The self-documentation function prints data in the files saved by SCS Manager and builders. For this reason, if you attempt to save files while the self-documentation is running, incorrect information may be printed or the printing process may fail. In such cases, run the self-documentation again after completing saving the files.

F2.6 Confirmation by print preview

A preview of the information to be printed can be displayed in the "Preview" tab of Document Generator. All the pages selected as printing targets in the "Table" tab are displayed in the "Preview" tab reflecting the result of customization in the "Options" tab. Each page of the printing results can be displayed by scrolling through the pages.

TIP

When you print using Document Generator, you can make print settings in the Page Setup dialog box started from File menu in SCS Manager. However, you cannot use the Page Setup dialog box in backward-compatible mode. A preview is shown with the printer settings made here. Therefore, if you specify the printer usually used for printing in the Page Setup dialog box beforehand, the preview and printed results match. The settings in the Page Setup dialog box can be made for each computer. However, in the Page Setup dialog box, you cannot set Page Range.

F3. Database Validity Check Tool

Database Validity Check Tool checks the mutual validity of the work database, the master database and the SCS database in the SCS. It checks whether or not the generation time and CRC (Cyclic Redundancy Checksum) of the databases match.

This chapter explains the window functions and operations of Database Validity Check Tool.

Relationship among Inter-database checks

The figure below illustrates the relationship of mutual validation of the work database, the master database and the SCS database within an SCS.

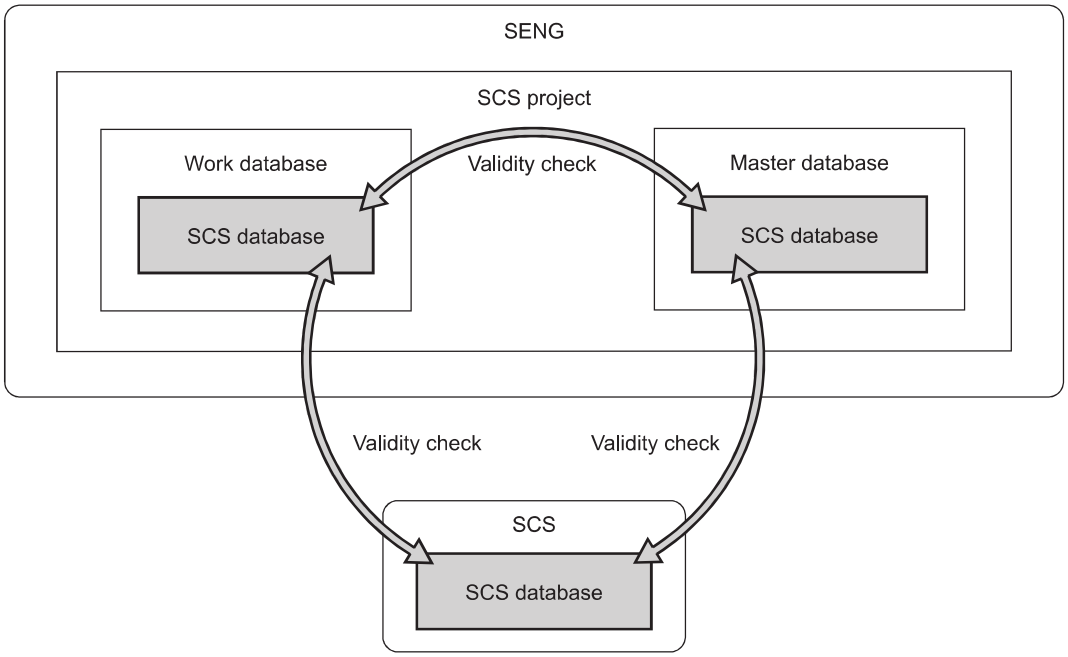


Figure F3-1 Inter-database check

The generation time and CRC information are acquired for each of the following databases from the work database, the master database and the SCS database within an SCS:

- POU DB
- Variable DB
- System DB (database for safety system)
- Integration DB (database for connecting CENTUM and external devices)

TIP The source files of the work database and the source files of the master database are not compared.

Repair database

If an online change download is interrupted or discontinued, database mismatch often occurs between SCS and SENG. While the database does not match between SCS and SENG, online change download attempts fail.

The database repairing function makes the database match between SCS and SENG, enabling you to run the discontinued online change download again.

Database Validity Check Tool of R3.02.10 or later provides the database repairing function. You can use the database repairing function only when the database does not match between SCS and SENG.

An example case of database repair is as follows:

1. If a communication error occurs during offline download or online change download, the master database on the SENG may fail to be updated although the database on the SCS is updated. As a result, the database does not match between the SCS and SENG after the communication error and online change download is discontinued. With non-matching databases between SCS and SENG, online change download attempts fail.
2. The database repairing function overwrites the master database with the contents of the work database to match the database between SCS and SENG. When the master database is repaired successfully, the display in the Check Result List is refreshed.

TIP

Until the master database is repaired, the SCS project remains read only and cannot be edited or built. Restoration of the master database and master database offline download are also disabled.

3. After the master database is repaired, you can run the interrupted online change download and master database offline download again. You can read/write, edit, and build the SCS project. You can also use the Master Database Restoring Function.

SEE ALSO

For more information about Master database off-line download, refer to:

I4.4, “Master database offline download” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about Master Database Restoring function, refer to:

F4., “Master Database Restoring Function” on page F4-1

Launching Database Validity Check Tool

1. Choose [Engineering] from [Tools] menu of SCS Manager.
   The Engineering Launcher menu appears.
2. Select [Database Validity Check] from the Engineering launcher menu.
   Database Validity Check Tool launches and the Database Validity Check Tool window appears.

Database Validity Check Tool window structure

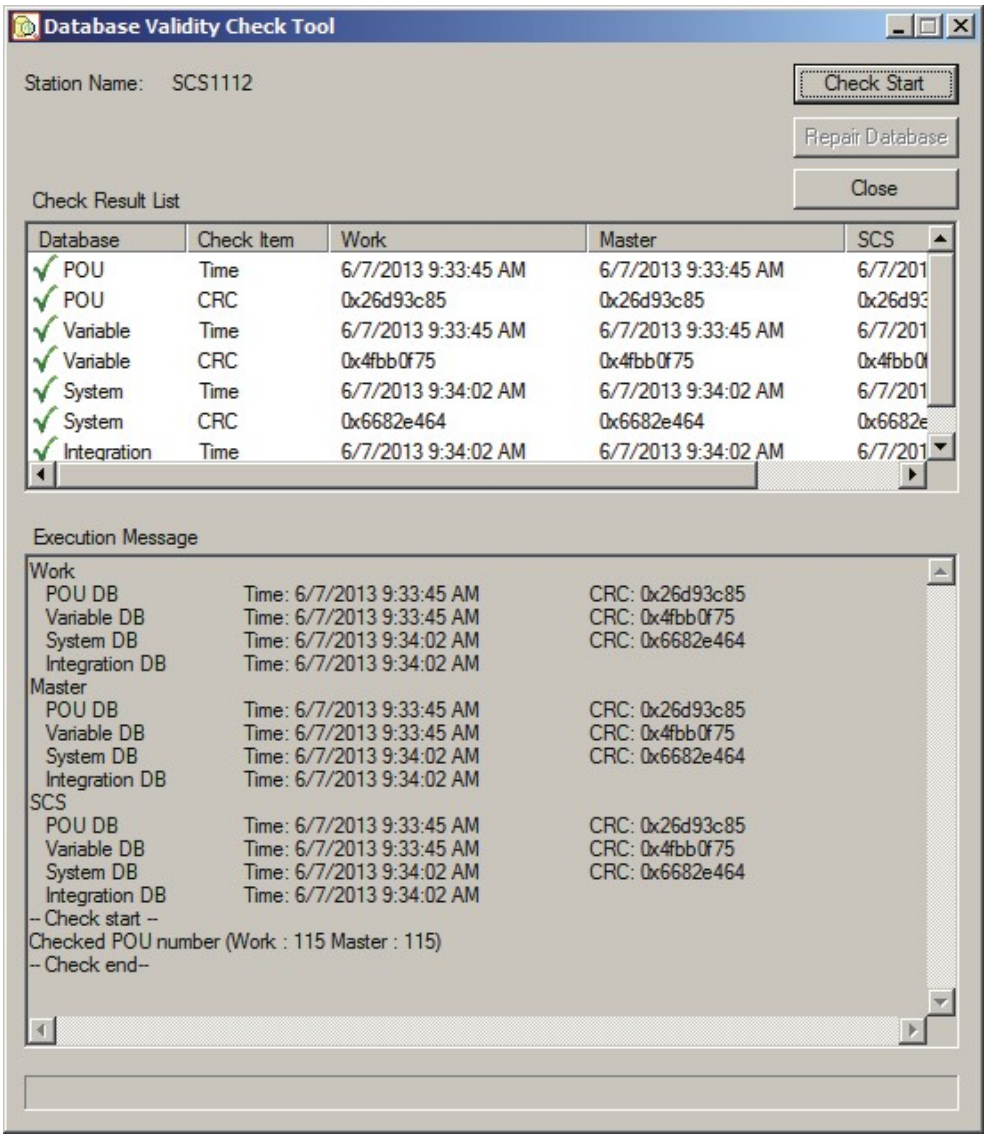


Figure F3-2 Database Validity Check Tool window

The components of the window are explained in the following sections.

Station name

The station name of the SCS in question is displayed.

Check result list

The results of checking the database validity are displayed in a list.

Items displayed in the check result list are explained below.

Table F3-1 Items displayed in check result list

Item name	Display
Database	Displays an icon indicating the results of checking the database validity along with the database name (POU DB, Variable DB, System DB, Integration DB)

Continues on the next page

Table F3-1 Items displayed in check result list (Table continued)

Item name	Display
Check Item	Displays whether the validity is checked based on the generation time or CRC
Work	Displays the generation time and CRC of the work database
Master	Displays the generation time and CRC of the master database. The master database is generated and the master information is displayed when you download the work database to the SCS.
SCS	Displays the generation time and CRC of the SCS database within the SCS. Displayed when the SCS is connected.

Types of icons

The following three colors are used for the icons displayed in the [Database] column, depending on whether the SCS database matches the work database and master database or not.

Table F3-2 Types of icons

Icon (color)	Description
(green)	The work database, the master database and the SCS database all match.
(blue)	The contents of the work database, the master database and the SCS database all match.
(yellow)	The work database and the master database do not match. This result occurs if you performed a build operation to generate the work database but have not performed download. When required, you can perform online change download or offline download to download the work database to the SCS. If you want discard the work database, you can use Master Database Restoring Function to duplicate the master database into the work database.
(red)	The master database and the SCS database do not match. Online change download cannot be performed. Perform either offline download or master database offline download to update the SCS database so that it matches with the master database.

IMPORTANT

The Variable DB is not downloaded to SCS if an On-line change download is performed with an application for which the definition details of its variables have not been changed. For this reason, the time of the Variable DB of the Work database and the CRC are not reflected onto the SCS. If this happens, the icon indicating the check result is shown in blue and the following message appears.

Example:

```
The content of the definition is corresponding though the time and CRC of V
ariable DB is not corresponding between work and master.
```

SEE ALSO

For more information about Offline download, refer to:

C7., “Offline download to the target SCS” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about Online change download, refer to:

E1.1, “Online change download” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about Master database off-line download, refer to:

I4.4, “Master database offline download” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about Master Database Restoring function, refer to:

F4., “Master Database Restoring Function” on page F4-1

Checking database validity

- Click the [Check Start] button in the Database Validity Check Tool window.
  Database validity check starts.

  During the check, the progress is displayed in the progress bar at the bottom of the window.

Execution messages

Execution messages generated during checking are displayed.

The information shown in the execution message area can be copied and used as information for reports.

There are following three types of operation messages.

- Error messages notifying processing errors
- Information acquired during checking
- Checking result

Example of error messages notifying processing errors and action to take

If you start database validity check while the target SCS project is being built or downloaded, an error message like the one shown in the following figure is displayed. Wait until the build or downloading is completed and start the check again.

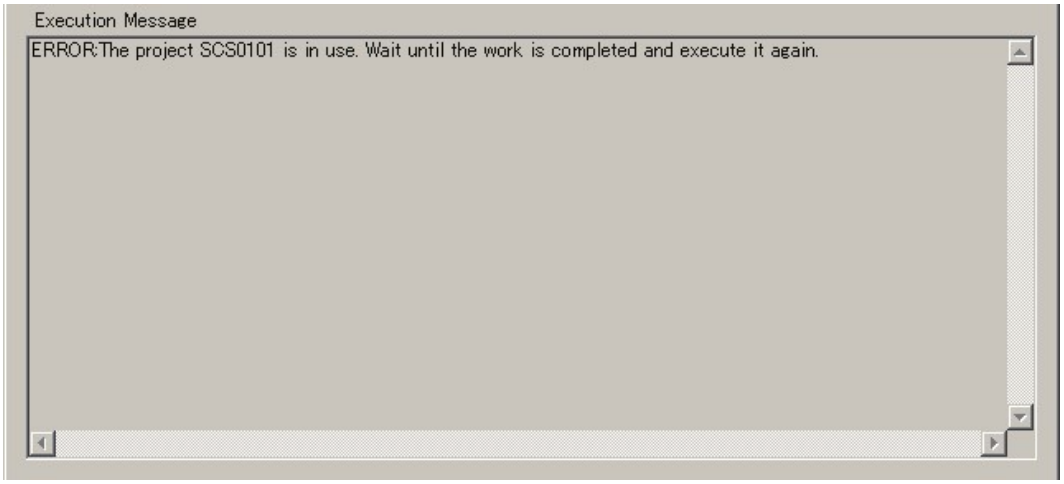


Figure F3-3 Example of error messages

Example of information acquired during checking

The generation time and CRC information are displayed for the work database, the master database and the SCS database within the SCS.

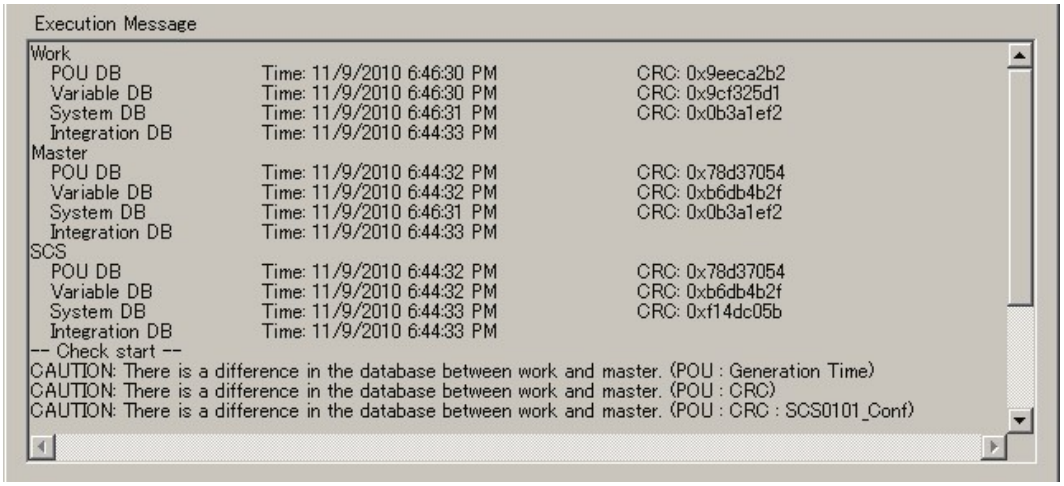


Figure F3-4 Example of information acquired during checking

Example of checking result and displayed contents

The result after comparing the SCS database in SCS, the work database and the master database will be displayed.

- Comparing the generation time and CRC of the databases.
- If CRC discrepancies are found among the POUs of databases, the POU name and the resource configuration file name (<SCSProjectName>_Conf) will be displayed.
- "IMPORTANT" indicates the discrepancy between the SCS settings in SCS and in the master database corresponding to the red icons in the check result list.
- "CAUTION" indicates the discrepancy between the SCS settings in work database and in the master database corresponding to the yellow icons in the check result list.
- Indicates the number of compared POUs.

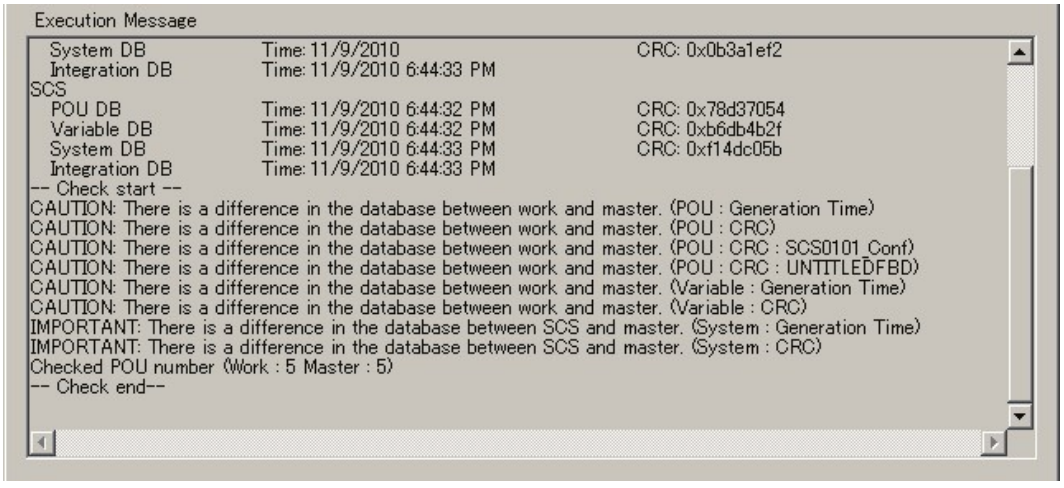


Figure F3-5 Example of checking result

Repairing the database that does not match

- Click the [Repair Database] button in the Database Validity Check Tool window.
  The master database is overwritten with the contents of the work database. "Check Result List" indicates that the master database and the SCS database match.

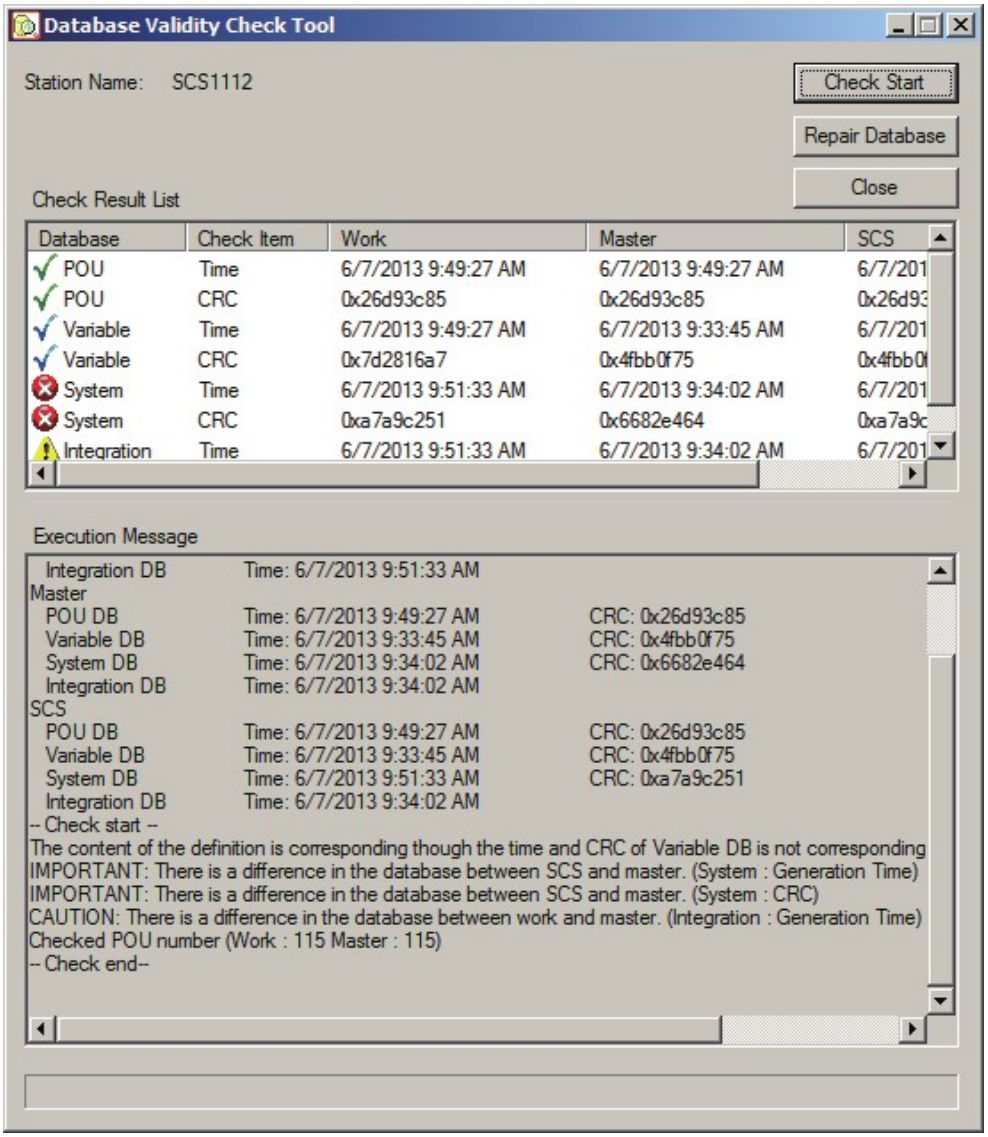


Figure F3-6 Database Validity Check Tool window

Exiting Database Validity Check Tool

- Click the [Close] button in the Database Validity Check Tool window.
  The button is disabled during checking.

  The Database Validity Check Tool is exited.

F4. Master Database Restoring Function

Master Database Restoring function is a tool to restore the edited SCS project to the last downloaded state. This function may be used mainly in cases when an edit, for which an On-line change download cannot be performed, is made by mistake to an SCS project. If an edit, for which an On-line change download cannot be performed, has been made, using this tool restores the SCS project to its most recently downloaded state. As a result, you can continue to perform the online change from the application in its most recently downloaded state.

This section explains the operations involved in restoring the master database.

TIP

In the case of an SCS project selecting I/O list engineering with version R4.03.00 or earlier, after restoring the Master Database using the Master Database Restoring function, restore the safety I/O list and IOM information in AD Organizer to the contents labeled at the time of the previous download.

How to start the tool and differences in behavior

You can start Master Database Restoring Function Tool from the start menu or from AD Organizer.

If you start this tool from AD Organizer and perform restoration of an SCS project, the data of I/O list engineering will also be restored automatically. If you start the tool from the Start menu, the data of I/O list engineering will not be restored automatically.

When you start this tool from the Start menu, the following message appears:

> When this tool is started from the Windows Start Menu, the I/O List Engineering data recovery to AD Suite is not performed automatically. To automatically restore I/O List Engineering data to AD Suite, please specify the SCS station node on System Structure Navigator in AD Organizer and launch this tool from context menu.

In order to link the SCS project backup/restoration function with the I/O list engineered data, access rights that allow execution of SCS import in AD Organizer is required.

Follow these steps to start the tool from AD Organizer:

1. Start AD Organizer.
2. Select the SCS project of your choice in the System Structure Navigator, and from the context menu, select [Master DB Restoring Function Tool].
   The window of the Master DB Restoring Function Tool appears.

SEE ALSO

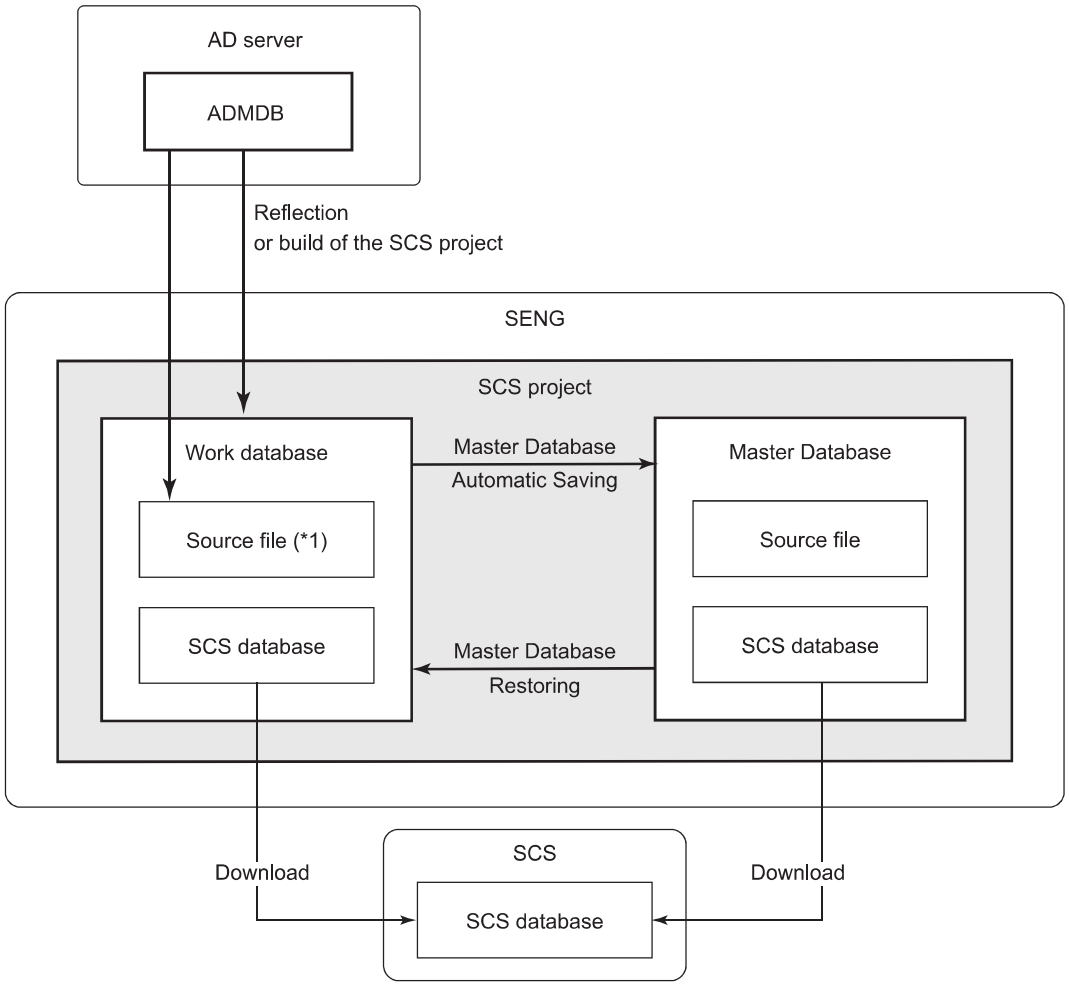
For more information about access rights in I/O list engineering, refer to:

C1.2.2, “Controlling access to AD projects” on page C1-30

Overview of Master Database Restoring Function

The engineering data required for operating ProSafe-RS is stored as the work database of an SCS project in the SENG, and the SCS database within this work database is subsequently downloaded to the SCS by user operation. Once downloaded, the work database is stored as the master database.

The information of an SCS project includes the work database in the SENG, the master database in the same SENG and the SCS database within the SCS. Immediately after downloading, the two source files and three SCS databases contain the same data; that is, the source files and SCS databases are consistent.



*1: The source file includes the safety I/O list and IOM information.

Figure F4-1 Database configuration

If you do not perform download after engineering (saving data created in a builder in the work database), the data in the work database and other databases will not match.

Master Database Restoring Function is a tool to discard the information in the work database and restore the work database with the information in the master database. So that the engineering data (in the work database) can match the engineering data in the master database.

Note that Database Validity Check Tool is used to check that the data in each database matches.

TIP

In addition to starting Master Database Restoring Function Tool from the Start menu, you can also start this tool from AD Organizer. However, if you start this tool from the Start menu when the master database contains I/O list engineered data, the I/O list engineered data on the AD Server will not be restored even if the restoration process is performed. If you start the tool from AD Organizer, the I/O list engineered data will also be restored automatically when you perform the restoration process.

SEE ALSO

For more information about details of the Database Validity Check Tool, refer to:

F3., “Database Validity Check Tool” on page F3-1

Work database restoration timing

It is possible to use Master Database Restoring Function to restore the data of the master database in the work database at any time. However, the SCS project that has been opened by the SCS Manager or the Multi-Language Editor cannot be restored. Likewise, when the Master Database Restoring Function is used, the SCS Manager and Multi-Language Editor cannot be used.

Restoration target file

The master database of an SCS is stored in located below the top folder of each SCS project.

It is possible to use Master Database Restoring Function to restore the work database based on all the files.

IMPORTANT

Do not add, delete or change folders and files in layers below the top folder of the SCS project using Windows Explorer.

Master Database Restoring Function window structure

By starting SCS master DB recover, the following window appears.

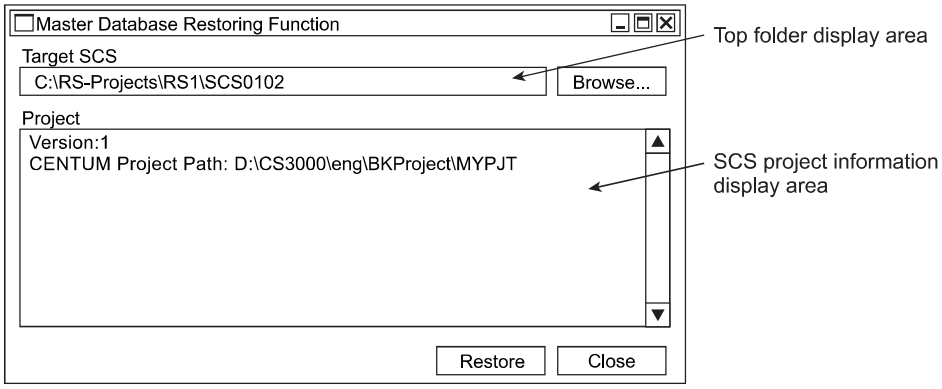


Figure F4-2 Master Database Restoring Function window

When started from AD Organizer, the display will be as follows:

- The name of the AD project subject to restoration appears on the title bar.
- The path of the target SCS project appears in the SCS project information display area, and the project becomes uneditable.
- The Browse button is disabled.

SEE ALSO For more information about how to start the Master Database Restoring Function, refer to:

"ProSafe-RS and ProSafe-RS Lite applications that can start from Start menu" in Read Me First (IM 32P01A30-01EN)

Top folder display area

The path to the top folder of the SCS project, which is the restoration destination of the master database, is displayed in this field.

To change the target project, enter the path to the desired project folder directly in the field of the top folder display area, or select a folder in the folder selection dialog box displayed by clicking [Browse] button.

However, when Master Database Restoring Function is started from AD Organizer, the top folder SCS is fixed. You cannot edit this folder path. The Browse button is disabled.

SCS Project Information display area

This area displays information about the target SCS project.

When the SCS project subject to restoration includes data of I/O list engineering, [ADS] appears in the SCS project information display area.

Example: Version:1 [ADS]

Master database restoration operation

1. Specify the path to the top folder of the SCS project, which is the restoration destination of the master database, in the top folder display area.
2. Check the information displayed in the SCS project information display area.
3. Click [Restore] button.
   The Status Display dialog box appears and the restoration process starts.

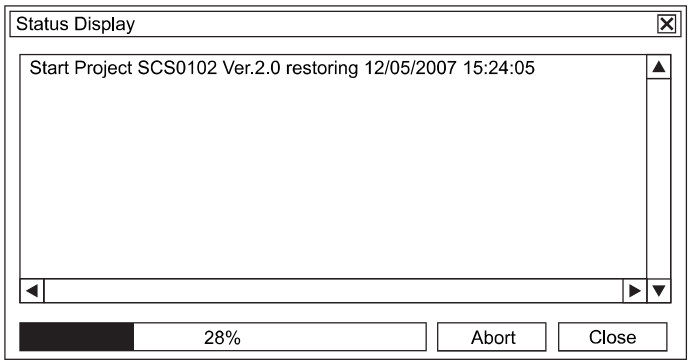


Figure F4-3 Status Display dialog box

The information displayed in the Status Display dialog box is as follows:

- Restoration start date/time
- Restoration completion date/time
- Warnings and errors
- Numbers of warnings and errors

4. Click [Close] button when Restore is completed.
   The Status Display dialog box closes.
5. Click [Close] in the Master Database Restoring Function window to end Master Database Restoring Function.

TIP

- In order to stop the restoration during the processing, click [Abort] button. The restoration processing that has been carried out so far is discarded and the work database returns to the status before the restoration processing operation.
- To select information displayed in the Status Display dialog box, select [Select All] from the pop-up menu opened by right-clicking. Select [Copy] to copy the information.

SEE ALSO For more information about precautions for restoring an SCS project that contains the safety I/O list to which the Safety I/O parameter profile is assigned by using Master Database Restoring function, refer to:

"■ Restoring SCS projects by Version Control Tool and Master Database Restoring function" in D1.5.11, "Precautions for importing and restoring SCS projects including safety I/O parameters" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Operations after restoring an SCS project by using the Master Database Restoring Function when performing I/O list engineering

This section describes the operations for an SCS project that was engineered by I/O list engineering with a revision earlier than R4.03.10. In this case, you must manually restore the details defined with the system structure navigator in AD Organizer.

TIP When downloading data to SCS with SENG R4.03.10 or later, data of I/O list engineering is included in the master database of the SCS project. When you perform the restoration process by using Master Database Restoring function started from AD Organizer, the data of I/O list engineering is also automatically restored at the same timing.

When [ADS] is displayed in the SCS project information area, it indicates that the data of I/O list engineering is included in the target SCS project.

The subjects of manual restoration are as follows:

- Safety I/O list
- Node definition
- IOM definition

After engineering by using iDefine, the following data are also restored:

- POU, variables, and tag information that were created in iDefine

IMPORTANT

The engineering data that was created by using iDefine must be restored so that it is consistent with the data that was restored by using the Master Database Restoring Function. As such, we recommend that you create a backup of the iDefine-config file when you import it to AD Organizer.

In iDefine, it is possible for multiple SCS to share one module, so it may be necessary to modify the data manually depending on the changes made.

Follow these steps to manually restore the definition details of System Structure Navigator.

1. From the context menu of the target SCS in System Structure Navigator in AD Organizer, select [Display revision history].
   The Revision History dialog box appears.
2. Select [All] and click [View].
   The Revision History window appears.
3. On the tab sheet for labels in the Revision History window, search for the label corresponding to the modified data.
   The following labels are attached to the files when a download is performed.
   `SCS project name-Download-(date)`
4. Select the label and click [Details].
   The Label Detail dialog box appears.
5. From the list in the Label Detail dialog box, search for the following files, select each file, and select [Launch Editor] from the context menu:

- I/O_definition
- Node_definition
- IOM_definition

6. Extract data from each file. Perform all of the following operations when extracting data. There is no specific order for performing these operations.
   - In order to export the data of I/O_definition, select [Export] from the sub menu of Safety I/O Editor.
   - In order to export the content of IOM Definition, select [Export] from the sub menu of IOM Definition Editor.
7. From the system structure navigator in AD Organizer, select the files under the I/O-List folder and start Safety I/O Editor.
8. Import the data of I/O_definition that was exported from Safety I/O Editor in the step 6.
9. Select the targeted SCS and start IOM Definition Editor.
   a. If the structure of nodes, IOM, ESB bus coupler module, or N-ESB bus coupler module is different from the structure that is defined in the master database, make the structure same as the one defined in the master database.
   b. By using IOM Definition Editor, import the files that were exported from IOM Definition Editor in the step 6.
10. Select the targeted SCS and select [RS Generation Manager] from the context menu. Generation Manager will start.
11. After selecting the [RS project name] and [SCS project name], click [Reflection]. The reflection process will be run.
12. Using the project comparing tool, compare the Work database created with the above steps against the Work database of the version at the origin of the check-out controlled with the Version Control Tool to check that the data of AD Organizer has been correctly restored.

F5. Version control

The Version Control Tool manages the history of changes of SCS projects and assists the user with system updating tasks. This section describes how to use the Version Control Tool.

Version Control Tool is used for the following purposes.

SEE ALSO For more information about differences in behavior depending on how to start Version Control Tool, refer to:

"■ How to start the tool and differences in behavior" on page F5-2

■ Version control of project data

Save (check-in) engineering data at a project milestone or at the end of engineering in different hard disks.

When checking in to an SCS project created with I/O list engineering, check in upon placing labels on the safety I/O list and IOM information of AD Organizer.

Labels of the following name are automatically added when checking in with the Version Control Tool.

```
SCS project name-Version
```

Version is the Version number specified by the user with the version control tool.

When checking out, return the safety I/O list and IOM information with AD Organizer based on these labels.

SEE ALSO For more information about how to set labels, refer to:

C2.8, "Setting labels" on page C2-17

■ Backing up project data

Checked-in data can be used as backup data. Checked-in project data can be checked out and restored.

■ Engineering and replacing the revised project with large-scale changes

When making large-scale changes to an SCS project, it is a good idea to perform engineering tasks on temporarily copied project data, rather than editing the active project data directly; this way, the active project data can be replaced with the new project data at the end of engineering.

F5.1 Main window of Version Control Tool

This section explains the components of the main window of Version Control Tool.

How to start the tool and differences in behavior

If a check-in folder has not been specified, the Select Checkin Folder dialog box appears automatically when the Version Control Tool is started.

You can start the Version Control Tool from the start menu or from AD Organizer.

If you start this tool from AD Organizer and perform a checkout when data of I/O list engineering is included in the SCS project, the data of I/O list engineering on the AD Server will also be restored automatically at the same timing as the checkout.

In addition, you cannot perform SCS project registration tasks for other than the SCS projects specified with AD Organizer. However, if none of the SCS projects specified in AD Organizer has been registered, you can register any SCS projects when you start the Version Control Tool.

When you start this tool from the Start menu, the following message appears:

> When this tool is started from the Windows Start Menu, the I/O List Engineering data recovery to AD Suite is not performed automatically. To automatically restore I/O List Engineering data to AD Suite, please specify the SCS station node on System Structure Navigator in AD Organizer and launch this tool from context menu.

Follow these steps to start the tool from AD Organizer:

1. Start AD Organizer.
2. Select the SCS project of your choice in the System Structure Navigator, and from the context menu, select [Version Control Tool].
   The window of the Version Control Tool appears.

SEE ALSO For more information about SCS project registration tasks, refer to:

F5.2, “Registration of SCS projects for version control” on page F5-7

Version Control Tool window

When you start Version Control Tool, the following window appears.

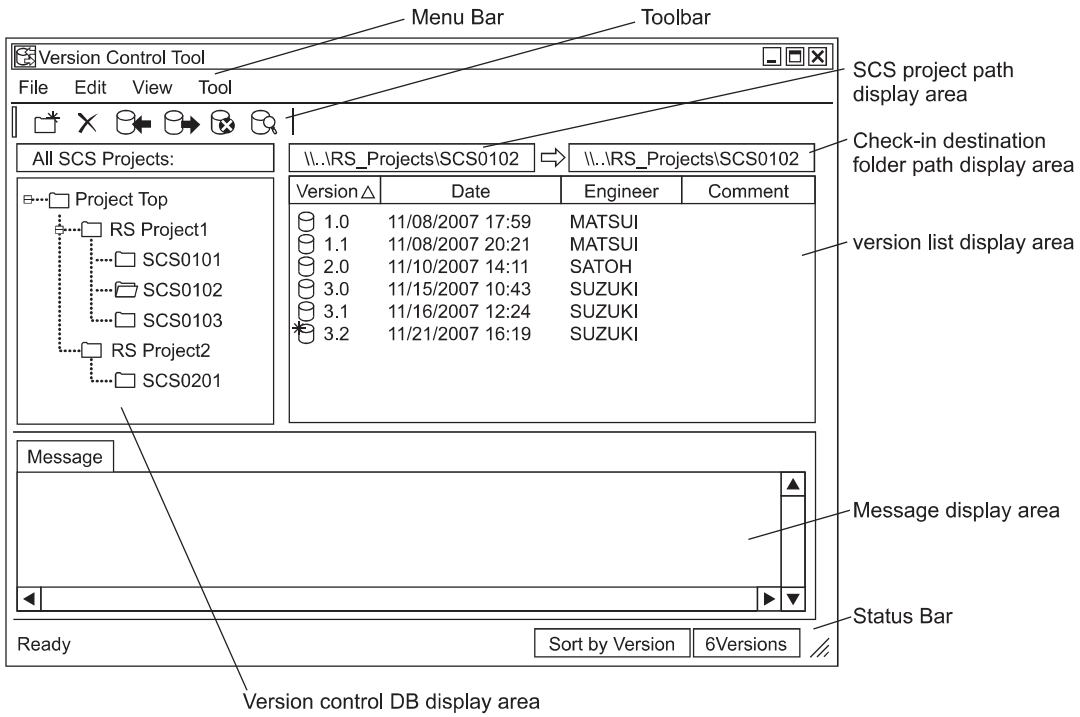


Figure F5.1-1 Version Control Tool window

When started from AD Organizer, the display will be as follows:

- The name of the AD project subject to version control appears on the title bar.
- When the applicable SCS project displayed in the version list display area includes the data of I/O list engineering, [ADS] appears to the right of the version number.

The components of the window are explained in the following sections.

Menu bar

The menu bar provides the following menus.

- File menu
- Edit menu
- View menu
- Tool menu

The menu items of each menu are explained below.

Table F5.1-1 File menu

Menu item	Description
Register Project (*1)	Starts new version control of an SCS project
Delete Version/Project (*1)	Deletes specified versions ,SCS projects or RS projects from the check-in folder
Print Preview	Displays print preview.
Print	Displays the print dialog box for printing purposes.
Exit Version Control Tool	Closes Version Control Tool

*1: Disabled when Version Control Tool is started from AD Organizer.

Table F5.1-2 Edit menu

Menu item	Description
Checkin	Checks in the selected SCS project to the specified check-in folder
Checkout	Checks out the selected version to the specified folder
Abort	Stops a check-out or check-in operation in progress
Select All	Selects all versions
Deselect All	Deselects all versions

Table F5.1-3 View menu

Menu item	Description
Detail	Displays a dialog box that displays detailed information of the selected version
Order of Display	Selects a display order for the version list display area. The selectable display orders are in order of version, date and engineer name.
Toolbar	Specifies whether or not to show the tool bar
Status Bar	Determines whether or not to display the status bar
Message Display Area	Specifies whether or not to show the message display area

Table F5.1-4 Tool menu

Menu item	Description
Change Checkin Folder	Displays a dialog box for changing the top path of the check-in folder
Change Target Project Folder (*1)	Changes the top path of an SCS project to be the target of version control. This menu item can only be selected when an SCS project is selected in the version control DB display area.
Option	Sets the operating environment of the tool and displays the option dialog box.

*1: Disabled when Version Control Tool is started from AD Organizer.

Toolbar

The toolbar provides the following buttons.

Table F5.1-5 Toolbar buttons

Button	Name	Description
	Register SCS Project	Same as [Register Project] in the [File] menu
	Delete Version/Project	Same as [Delete Version/Project] in the [File] menu
	Checkin	Same as [Checkin] in the [Edit] menu
	Checkout	Same as [Checkout] in the [Edit] menu
	Abort	Same as [Abort] in the [Edit] menu
	Detail	Same as [Detail] in the [View] menu

Version Control DB display area

The version control DB display area displays RS projects and SCS projects in the check-in folders specified by engineers in a tree structure.

The displayed folder structure is limited down to the level of SCS projects; folders in lower layers are not displayed.

When Version Control Tool is started from AD Organizer, only the applicable SCS projects are displayed.

When Version Control Tool is started from the Start menu, all SCS projects subject to control are displayed.

SCS Project Path display area

If you select an SCS project in the version control DB display area, the path to the top folder of the SCS project to be checked-in is displayed in this area.

Check-in destination folder path display area

This area displays the folder path of the check-in destination (check-in folder) for the SCS project selected in the version control DB display area.

Version list display area

This area displays a list of versions corresponding to the SCS project selected in the version control DB display area. When the applicable SCS project includes the data of I/O list engineering, [ADS] appears to the right of the version number.

You can select multiple versions.

If you double-click a version, the Detail dialog box appears and shows the detailed information about the selected version.

The following information is displayed in the version list display area:

- Version
- Date (Check-in time and date)
- Engineer
- Comment

If you click a column title other than Comment once, the list is sorted according to the selected item in the ascending order. If you click once again, the list is sorted in the descending order.

An icon indicating the version is displayed at the left edge of the list. The icon for the latest version has a different shape than other icons. Note that the latest version is judged from the check-in date, rather than the version number, and the icon is displayed accordingly.

SEE ALSO For more information about Detail dialog box, refer to:

"■ Display of information related to versions" on page F5-19

Message display area

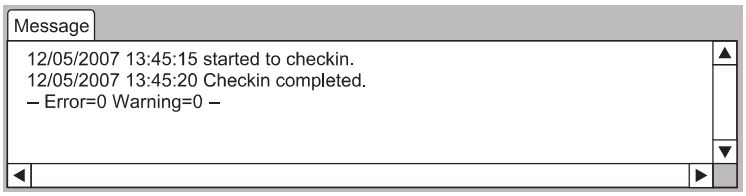


Figure F5.1-2 Message display area

The message display area displays messages generated at check-in, check-out, deletion, etc.

TIP Right click the mouse to show a pop-up menu. Choosing [Copy] from the menu may copy the messages.

Status bar

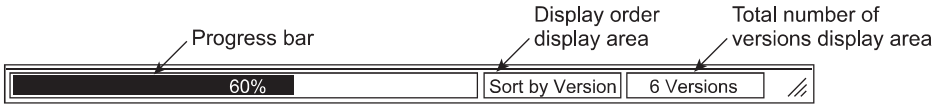


Figure F5.1-3 Status bar

The status bar contains the following display areas.

- Progress bar
  At check-in, check-out and deletion, the progress bar appears and displays the processing percentage. If the progress bar is not displayed, hints for the tool appear according to the mouse cursor position.
- Display order display area
  This area displays the display order chosen in the version list display area.
- Total number of versions display area
  This area displays the total number of displayed versions.

F5.2 Registration of SCS projects for version control

If version control is performed for an SCS project for the first time, the project must be registered. Once registered, the project is displayed and can be selected in the tree list of the version control DB display area.

When Version Control Tool is started from AD Organizer, you cannot perform SCS project registration tasks for other than the specified SCS project. However, when none of the SCS projects specified in AD Organizer has been registered, the Select SCS Project dialog box appears when you start the tool, and you can register any SCS projects.

1. In the Version Control Tool window, select [File] > [Register Project]. Alternatively, click [Register SCS Project] on the toolbar.
   The Select SCS Project dialog box appears.

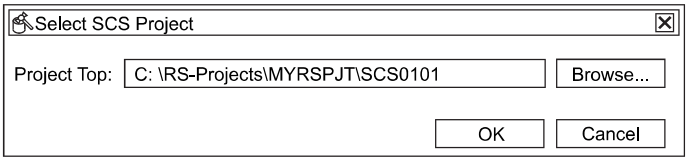


Figure F5.2-1 Select SCS Project dialog box

2. Specify the top folder of the SCS project for which you want to perform version control. In order to change the top folder, enter the path to the desired folder directly in the field or select it in the folder selection dialog box displayed by clicking [Browse] button.
3. Click [OK].
   The top folder of the SCS project is displayed in the SCS project path display area.

IMPORTANT

You can specify the top folder path to SCS project in the format for local drives, not necessarily in the Universal Naming Convention (UNC). But before you use the local drive format, you must specify "Folder sharing" as a user with administrator privilege. "Folder sharing" enables you to check-in folders to local drives.

TIP

An error dialog box appears if the specified folder does not exist, the top folder of an SCS project that is already registered for version control is specified, or a folder that is not the top folder of an SCS project is specified.

Folder sharing

When a SCS project is registered, the upper level folder of the RS project folder needs to be specified as a shared folder.
An example below shows how to specify a folder as a shared folder. In this example, the folder named RS-Projects is specified as the shared folder.



Figure F5.2-2 Example of shared folder specification

1. Open Windows Explorer, right click on RS-Projects folder and then choose [Properties] from the pop-up menu. The Properties dialog box will be displayed.
2. Display "Sharing" tab and click [Advanced Sharing].

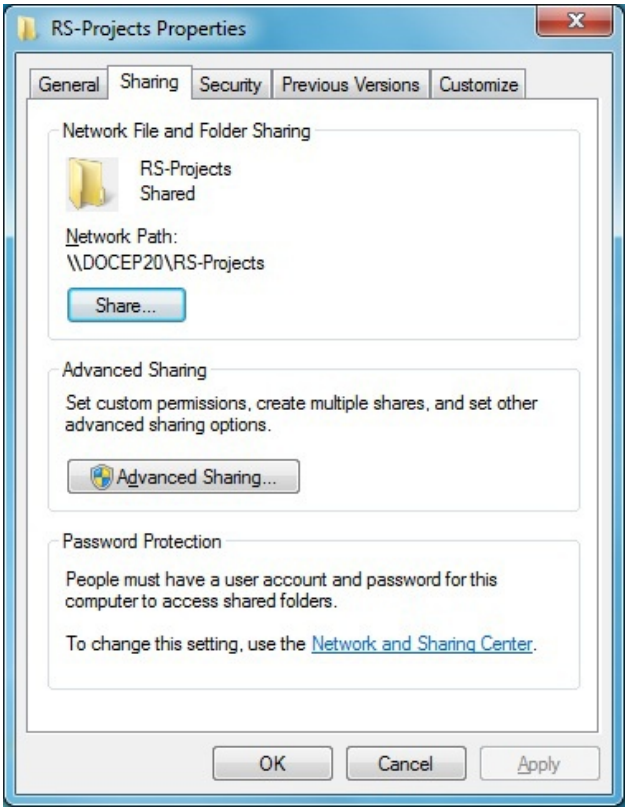


Figure F5.2-3 Sharing tab

Advanced Sharing dialog box appears.

3. Check the [Share this Folder] option and click [Permissions] button.

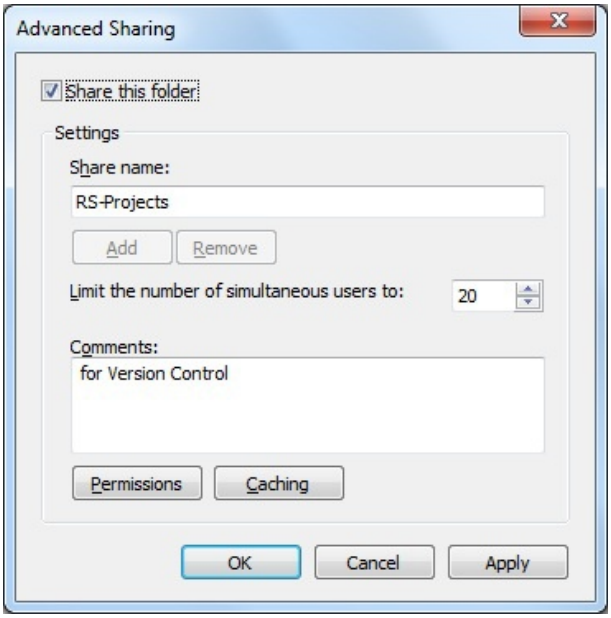


Figure F5.2-4 Advanced Sharing dialog box

Permission dialog box appears.

4. Check all the check boxes in [Allow] column of "Permissions for Everyone" and then click [OK].

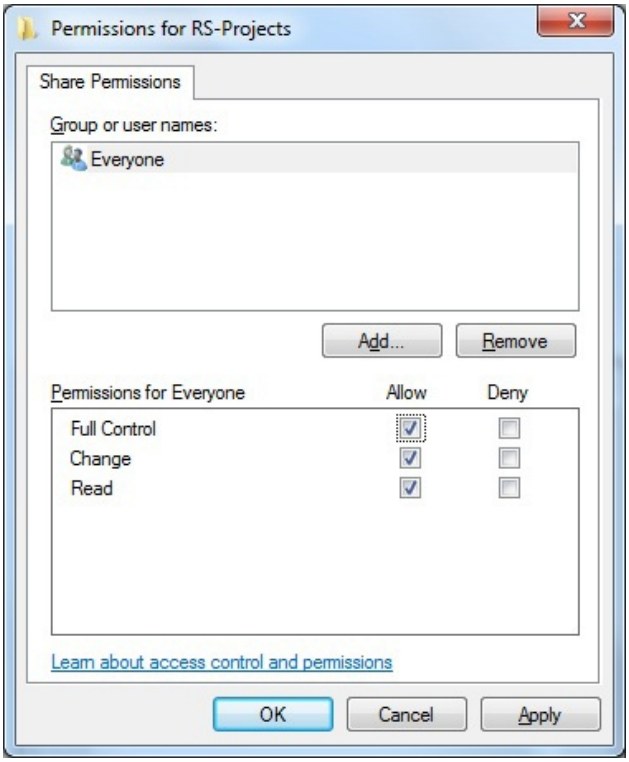


Figure F5.2-5 Permissions dialog box

RS-Projects folder becomes a shared folder.

F5.3 Checking in project data

When you check in an SCS project, the project data of the SCS project is saved in the check-in folder. At this point, a version number is assigned to the project data and the data is controlled according to this number.

Check-in timing

Project data can be checked in at any point.

However, when an SCS project to be checked in is being edited in SCS Manager, Multi-Language Editor, or any of the builders, it cannot be checked in or out with Version Control Tool. In addition, the SCS project cannot be edited with SCS Manager, Multi-Language Editor, or any of the builders while Version Control Tool is performing the check-in and check-out operation.

When the folder of the applicable SCS project includes data of I/O list engineering, the I/O list engineering data files are checked in together. The timing at which the data of I/O list engineering is registered to the SCS project is when the reflection process is implemented using RS generation manager.

Structure of check-in destination folder

The user can select any location for the top folder of the check-in destination, but the folder structure below the top folder is determined automatically.

IMPORTANT

- Do not use Windows Explorer to add, delete or modify the folders or files under the SCS project top folder, except for coping the library.
- Do not edit checked-in project data directly with SCS Manager.
- Do not operate on checked-in project data with Master Database Restoring Function.

Note that, in advance, the top folder of the check-in destination must be given a shared name "RS-Share" and its security must be strengthened by running the IT Security Tool.

SEE ALSO

For more information about strengthening security when placing the check-in destination folder on a SENG PC, refer to:

"■ Strengthening the Security of the Project Database on SENG PC" in B4.2, "Settings of Project Database Folder" in Installation Guide (IM 32P01C50-01EN)

For more information about strengthening security when placing the check-in destination folder on a file server, refer to:

"■ Strengthening the Security of Version Control Tool's Check-in Folder" in B4.2, "Settings of Project Database Folder" in Installation Guide (IM 32P01C50-01EN)

Specification of check-in destination folder

1. Start the Version Control Tool.
   If a check-in folder has not been specified, the Select Checkin Folder dialog box appears automatically.

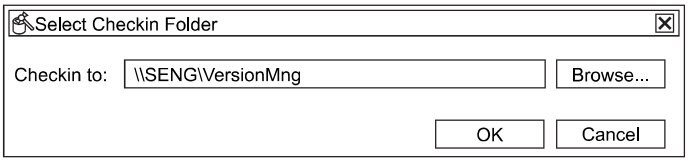


Figure F5.3-1 Select Checkin Folder dialog box

2. Specify a check-in folder.
   In order to change the check-in folder, enter the path to the desired folder directly in the field or select it in the folder selection dialog box displayed by clicking [Browse] button.

IMPORTANT

To prevent from the hardware abnormality, it is recommended to specify a folder in a disk different from the disk where SCS projects are saved.

3. Click [OK].
   The check-in folder is specified and the focus is returned to the window of the Version Control Tool.

   The structure of the specified folder is displayed in the version control DB display area.

Check-in operation

It is possible to check in project data at any point.

1. Select an SCS project to be checked-in in the version control DB display area.

TIP If the SCS project you want to check in is not displayed, register the SCS project for version control in advance following the procedure in "Registration of SCS Projects for Version Control."

2. Click [Checkin] button in the toolbar of the Version Control Tool window or select [Checkin] from the [Edit] menu;
   the Checkin dialog box appears.

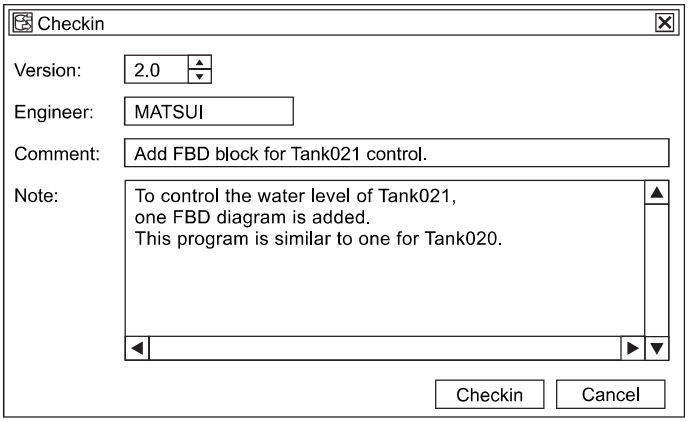


Figure F5.3-2 Checkin dialog box

3. Set version information and other items recorded in the version information file.
   The items that should be set in the Checkin dialog box are shown below.

Table F5.3-1 Setting items in the Checkin dialog box

Item displayed	Description
Version	Version number. Directly enter a number or make a selection from the spin box. The version number cannot be changed after check-in (*1)
Engineer	Enter the name of an engineer who performs check-in within 16 uppercase alphanumeric characters. An error dialog box appears if the field is left blank.
Comment	Enter any comment using up to 64 characters.
Note	Enter a more detailed description than in [Comment].

*1: If it is absolutely necessary to change the version number after check-in, delete the version you checked in and check in the data again with the correct version number. Note that the check-in date/time changes.

The rules for setting version numbers are explained below.

Table F5.3-2 Version input rules

Item	Description
Format	Up to 8 characters and 2 decimal points can be entered. A minus sign can also be specified. Example: 1, 1.0, 1.01, -1.0, -1.01, -1.10
Default value	1.0 for the first check-in. The least significant digit of the latest version is incremented for 2nd check-in and onward. Example: 2 if the latest version is 1 Example: 1.1 if the latest version is 1.0 Example: 1.02 if the latest version is 1.01 Example: 1.11 if the latest version is 1.10 Example: -2 if the latest version is -1
Input check	An error dialog box appears in the following cases. If the format is erroneous If the version number already exists If the number is smaller than the latest version number of the existing version (*1), a warning dialog box appears.

*1: In case of version numbers with minus signs, the absolute value of the input is checked, i.e., excluding the minus sign, For example, a warning dialog box appears if you enter -1 after -2.

4. Click [Checkin] button.
   The saving processing starts. At this point, a message indicating the saving status is displayed in the message display area and the saving status is shown in the progress bar.

   The following information is displayed in the message display area.

   - Check-in start date/time
   - Check-in completion date/time
   - Warnings and errors
   - Numbers of warnings and errors

TIP

During the check-in processing, [Abort] of the [Edit] menu and the [Abort] button of the toolbar are enabled; by selecting either of these, it is possible to stop the processing in the middle. If you select this menu item or button, the check-in processing is stopped and the files checked out until then are discarded.

IMPORTANT

When I/O list engineering is being performed and there is data being edited in AD Organizer, be sure to check in to the Version Control Tool after successfully completing the reflection process with Generation Manager or the build process of the SCS project.

SEE ALSO

For more information about reflection processes and SCS build processes, refer to:

D4., “Overview of RS generation” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

F5.4 Checking out project data

The checked-in project data can be retrieved (checked out) to a folder under the top folder of the SCS project or any other folder. The checked-out folders and files can be edited.

IMPORTANT

If you check out project data immediately below the SCS project top folder, the existing SCS project is cleared and the project data is replaced with the new version.

Check-out operation

Checked-in project data can be checked out at any point.

When Version Control Tool is started from the Start menu, the data of I/O list engineering on the AD Server will not be restored automatically even if you specify an SCS project having a project name with [ADS]. When Version Control Tool is started from AD Organizer, you can automatically restore the data of I/O list engineering.

1. Select the SCS project to be checked out and the version from the version control DB display area and the version list display area, respectively.
2. Click [Checkout] in the toolbar or select [Edit] > [Checkout].
   The Checkout dialog box appears.

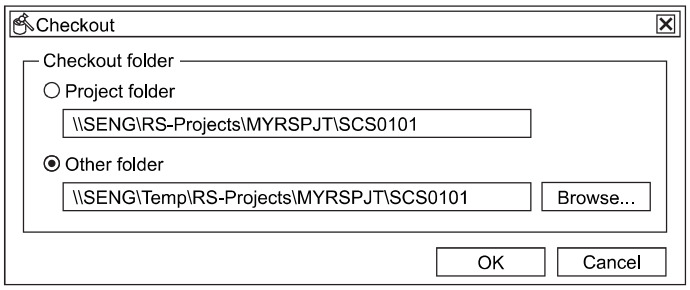


Figure F5.4-1 Checkout dialog box

   If you have started Version Control Tool from AD Organizer, only the Project folder option is enabled in the Checkout dialog box.

3. Select the location where the data should be checked out to, immediately below the top folder of the registered SCS project folder, or any other folder.
   To specify the SCS project top folder, select [Project folder]. The path name of the SCS project top folder cannot be changed.

   To specify any other folder, select [Other folder]. Enter the path to the desired folder directly or select it from the folder selection dialog box displayed by clicking [Browse] button.

IMPORTANT

If the folder for the checked-out data is UNC type, the folder should not be a shared folder. Create a new folder under the shared folder. Specify the newly created folder as the destination for check out. It is recommended to set the folder one level upper than the RS project folder as the shared folder.

   The check-out processing is different depending on whether the check-out destination is set to the SCS project top folder or any other folder. The differences in processing are explained below.

- SCS project top folder
  All the files below the specified folder are cleared before check-out processing when the user clicks [Yes] button in the confirmation dialog box.

  The structure of the folders under the SCS project top folder should match the structure of the checked-in folders. Moreover, the structure of the files after checking-out should be the same as the structure of the checked-in files.

- Other folder
  Files below the specified folder are not cleared before check-out. This causes the folder structure at the specified folder and below to be merged with the checked-in folder structure. Moreover, the file structure after check-out is also merged with the checked-in file structure; files with the same names are overwritten.

  However, if a user-defined folder is used as the SCS project folder, it behaves the same as for the SCS project top folder.

TIP

- In order to reflect the data that has been checked out onto the SCS project currently being engineered, select the directory directly under the SCS project top folder. When the engineering method is I/O list engineering, also be sure to restore the details defined with AD Organizer.
- An error dialog box appears if you specify the SCS project top folder and the specified folder does not exist.
- If you specify the project folder, it is checked that the specified folder is an SCS project folder. If it is not, an error dialog box appears.
- If you select any other folder and the specified path does not exist, a confirmation dialog box appears, asking whether or not to create it. If you click OK, a new folder is created.
  In this case, the created folder remains even if you abort check-out processing in the middle.

4. Click [OK] button.
   A confirmation dialog box appears.
5. Click [Yes] button in the confirmation dialog box.
   Check-out processing is performed and the target folder and all files below the target folder are copied to the destination. At this point, the message display area displays the check-out status. The status bar displays the progress status with the progress bar.

   The following information is displayed in the message display area.

   - Check-out start date/time
   - Check-out completion date/time
   - Warnings and errors
   - Numbers of warnings and errors

TIP

During the check-out processing, Abort in the Edit menu and Abort on the toolbar are enabled; by selecting either of these, it is possible to stop the processing in the middle. If you select this menu item or button, check-out processing is stopped and the files checked out until then are discarded.

SEE ALSO

For more information about precautions for restoring an SCS project that contains the safety I/O list to which the Safety I/O parameter profile is assigned by using Version Control Tool, refer to:

"■ Restoring SCS projects by Version Control Tool and Master Database Restoring function" in D1.5.11, "Precautions for importing and restoring SCS projects including safety I/O parameters" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Operations after checking out an SCS project by using the Version Control Tool when performing I/O list engineering

This section describes the operations for an SCS project that was engineered by I/O list engineering with a revision earlier than R4.03.10.

Once an SCS project created with I/O list engineering has been checked out by using the version control tool, it is necessary to manually restore the details defined with System Structure Navigator in AD Organizer.

TIP

When performing the check-in process with SENG R4.03.10 or later, data of I/O list engineering will be included in the SCS project checked in. When you perform the check-out process by using Version Control Tool started from AD Organizer, the data of I/O list engineering will also automatically be restored at the same timing.

When [ADS] is displayed in the SCS project information area, this indicates that the data of I/O list engineering is included in the applicable SCS project.

The subjects of manual restoration are as follows:

- Safety I/O list
- Node definition
- IOM definition

After engineering by using iDefine, the following data are also restored:

- POU, variables, and tag information that were created in iDefine

IMPORTANT

The engineering data that was created by using iDefine must be modified so that it is consistent with the data that was checked-out by using the Version Control Tool. As such, we recommend that you create a backup of the iDefine-config file.

In iDefine, it is possible for multiple SCS to share one module, so it may be necessary to modify the data manually depending on the changes made.

Follow these steps to manually restore the definition details of System Structure Navigator.

1. From the context menu of the target SCS in System Structure Navigator in AD Organizer, select [Display revision history].
   The Revision History dialog box appears.
2. Select [All] and click [View].
   The Revision History window appears.
3. On the tab sheet for labels in the Revision History window, search for the label corresponding to the modified data.
   The following labels are attached to the files when they are checked in.
   `SCS project name-Version`

   Version is the Version number specified by the user with Version Control Tool.
4. Select the label and click [Details].
   The Label Detail dialog box appears.
5. From the list in the Label Detail dialog box, search for the following files, select each file, and select [Launch Editor] from the context menu:
   - I/O_definition
   - Node_definition
   - IOM_definition

   Data form the past is displayed.
6. Extract data from each file. Perform all of the following operations when extracting data. There is no specific order for performing these operations.

- In order to export the data of I/O_definition, select [Export] from the sub menu of Safety I/O Editor.
- In order to export the content of IOM Definition, select [Export] from the sub menu of IOM Definition Editor.

7. From the system structure navigator in AD Organizer, select the files under the I/O-List folder and start Safety I/O Editor.
8. Import the data of I/O_definition that was exported from Safety I/O Editor in the step 6.
9. Select the targeted SCS and start IOM Definition Editor.
   a. If the structure of nodes, IOM, ESB bus coupler module, or N-ESB bus coupler module is different from the previous structure, make the definitions same as the previous ones.
   b. By using IOM Definition Editor, import the files that were exported from IOM Definition Editor in the step 6.
10. Select the targeted SCS and select [RS Generation Manager] from the context menu. Generation Manager will start.
11. After selecting the [RS project name] and [SCS project name], click [Reflection]. The reflection process will be run.
12. Using the project comparing tool, compare the Work database created with the above steps against the Work database of the version at the origin of the check-out controlled with the Version Control Tool to check that the data of AD Organizer has been correctly restored.

F5.5 Deleting of versions

Checked-in projects data can be deleted at any point. It is also possible to delete multiple versions at one time. Be aware, however, that the project data of a once deleted version cannot be restored.

Version deletion operation

Checked-in project data can be deleted at any point.

1. Select the target version in the version list display area.
   Multiple versions can be selected at the same time.
2. Click "Delete Version/Project" button of the toolbar or select [Delete Version/Project] from the [File] menu;
   the Version Control tool dialog box appears.

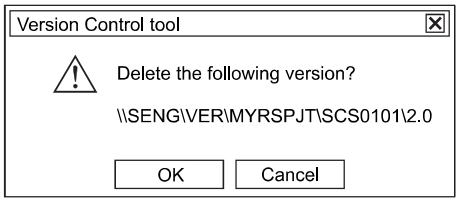


Figure F5.5-1 Version Control Tool dialog box

3. Click [OK].
   All the target folders and files below the folders are deleted. At this point, the deletion status is displayed in the message display area and the processing status is displayed in the status bar with the progress bar.

   The deleted versions are no longer displayed in the version list display area.

   The following information is displayed in the message display area.

   - Deletion start date/time
   - Deletion completion date/time
   - Warnings and errors
   - Numbers of warnings and errors

F5.6 Deleting all check-in data related to a project

Checked-in projects data stored in the version control database is deleted for each SCS project or RS project.

Check-in data project deletion

Check-in project data stored in the version control database is deleted for each SCS project or RS project.

1. Select an SCS project or RS project in the version control DB display area.
2. Click [Delete Version/Project] button in the toolbar or select [Delete Version/Project] in the [File] menu;
   the Version Control tool dialog box appears.

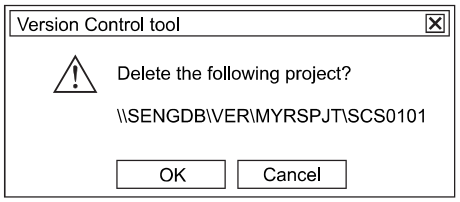


Figure F5.6-1 Version Control Tool dialog box

3. Click [OK] button.
   The deletion process is executed and the entire folder of the corresponding SCS project or RS project is deleted from the version control database. At this point, the deletion status is displayed in the message display area and the processing status is displayed in the status bar with the progress bar.

   The deleted project is no longer displayed in the version control DB display area.

   The following information is displayed in the message display area.

   - Deletion start date/time
   - Deletion completion date/time
   - Warnings and errors
   - Numbers of warnings and errors

F5.7 Viewing version information

At check-in, not only the version number, but also comments and other kinds of version information are recorded together with the data to be checked in. The version information can be viewed in the Detail dialog box.

Moreover, check-in states in the past are displayed in the version list display area. It is possible to change the sorting order and filter versions to be displayed in the version list display area.

SEE ALSO For more information about changing the sorting order in the version list display area, refer to:

"■ Version Control Tool window" on page F5-2

■ Display of information related to versions

Detailed information of the selected version is displayed in the Detail dialog box.

● Displaying the Detail dialog box

The Detail dialog box is displayed by performing either one of the following operations.

- Select [Detail] in the [View] menu.
- Select the [Detail] button in the tool bar.
- Select [Detail] in the pop-up menu displayed by clicking the right mouse button in the version list display area.
- Double-click in the version list display area.

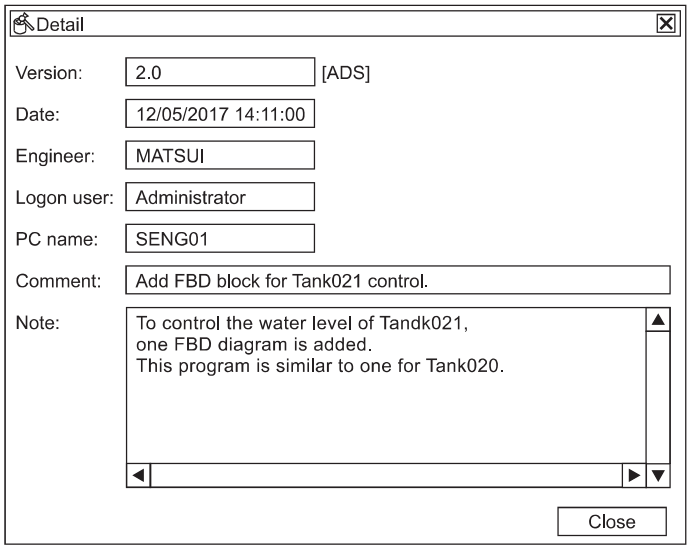


Figure F5.7-1 Detail dialog box

The Detail dialog box shows the following information items related to the selected version.

Table F5.7-1 Information displayed in the Detail dialog box

Item	Description
Version	Version number (*1)
Date	Date and time
Engineer	Engineer name
Logon user	Logon user name

Continues on the next page

Table F5.7-1 Information displayed in the Detail dialog box (Table continued)

Item	Description
PC name	PC name
Comment	Comment
Note	Description

*1: When the applicable SCS project includes the data of I/O list engineering, [ADS] appears to the right of the text box.

Filtering version list

Every time data is checked in, new check-in information is added; the version list may eventually contain too many lines. In this case, it is possible to filter the list such that versions that do not need to be viewed are not listed. The filtering settings are made in the Option dialog box.

Displaying the Option dialog box

Select [Option] from the [Tool] menu.
The Option dialog box appears.

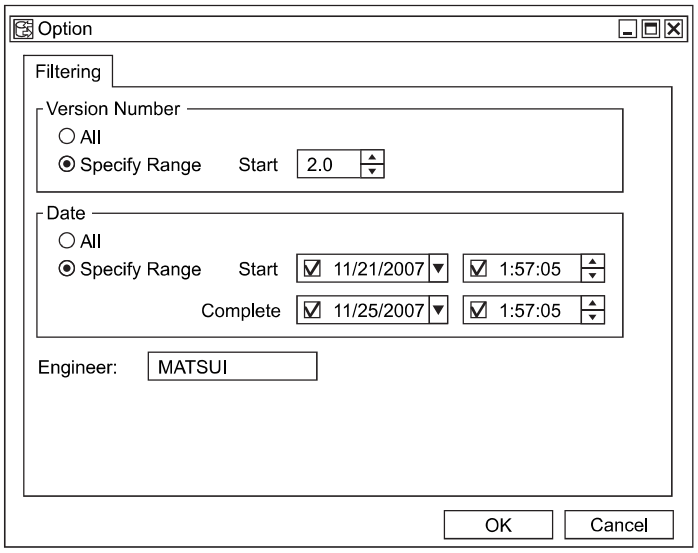


Figure F5.7-2 Option dialog box

Specification of filtering items

The following filtering items can be specified in the Option dialog box. When filtering items are set, the list only displays project data satisfying all the conditions below.

Table F5.7-2 Filtering items

Item	Description
Version Number	The specified version number and onwards can be displayed. Select a version number in the spin box or enter the version number directly.
Date	Only versions that were checked-in during a certain period can be displayed. In order to specify this item, select a period to be displayed in the calendar control and spin box or enter the period directly.
Engineer	Only versions checked in by a specific engineer can be displayed. In order to specify this item, enter an engineer name directly in the text box.

Specify filtering items and click [OK] button.

The version list display area is updated and the list is shown according to the specified filtering conditions.

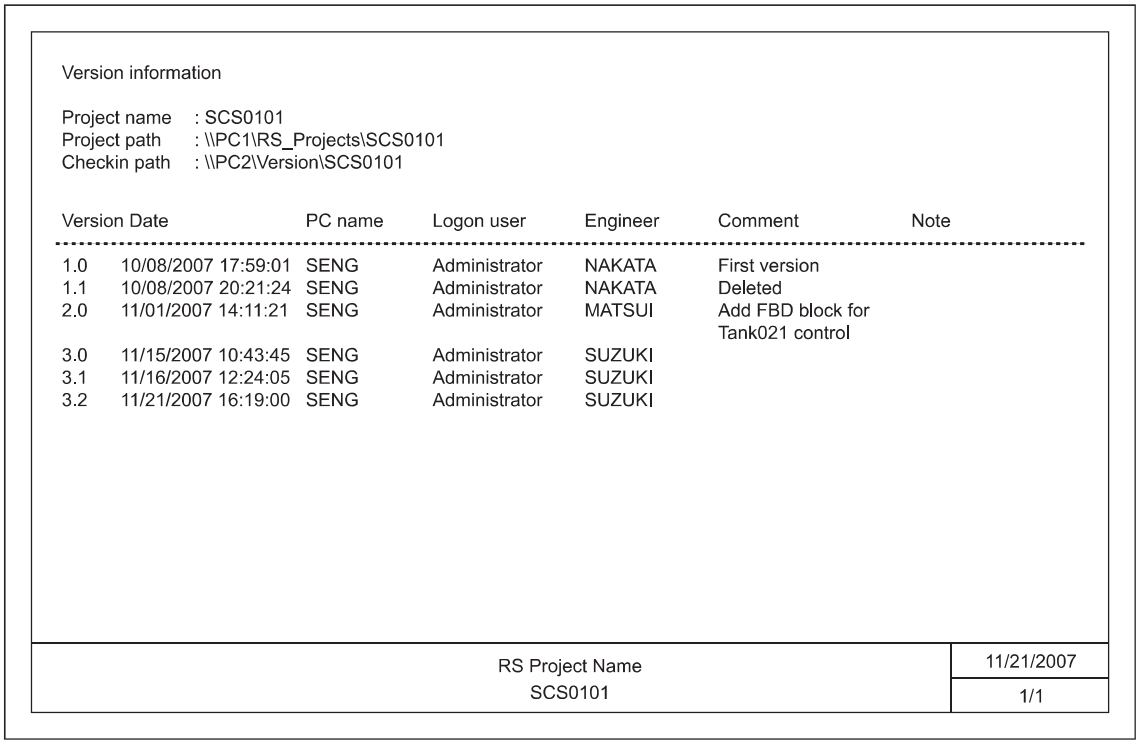
F5.8 Printing version information

It is possible to print the version information of the SCS project displayed in the version list display area.

The version list displayed in the version list display area can be sorted or filtered. The version information is printed in the landscape orientation on A3 size paper according to the display in the version list display area.

Printing example

Choose [Print] from [File] menu. The SCS Project Version Information can be printed out. A sample of printout is shown as follows:



Version information

Project name : SCS0101
Project path : \\PC1\RS_Projects\SCS0101
Checkin path : \\PC2\Version\SCS0101

Version	Date	PC name	Logon user	Engineer	Comment	Note
1.0	10/08/2007 17:59:01	SENG	Administrator	NAKATA	First version	
1.1	10/08/2007 20:21:24	SENG	Administrator	NAKATA	Deleted	
2.0	11/01/2007 14:11:21	SENG	Administrator	MATSUI	Add FBD block for Tank021 control	
3.0	11/15/2007 10:43:45	SENG	Administrator	SUZUKI		
3.1	11/16/2007 12:24:05	SENG	Administrator	SUZUKI		
3.2	11/21/2007 16:19:00	SENG	Administrator	SUZUKI		

RS Project Name
SCS0101

11/21/2007
1/1

Figure F5.8-1 Printing example

F5.9 Changing the top path of a check-in folder

If the capacity of the disk used for version control becomes insufficient or the disk crashes, secure new disk space for version control in a new disk location.

At this point, it is necessary to change the check-in path maintained in each SENG to the path of the newly set disk space. The top path of a check-in folder is changed in the Select Check-in Folder dialog box.

Changing check-in folder top path

1. Select [Change Checkin Folder] from the [Tool] menu
   The Select Checkin Folder dialog box appears.

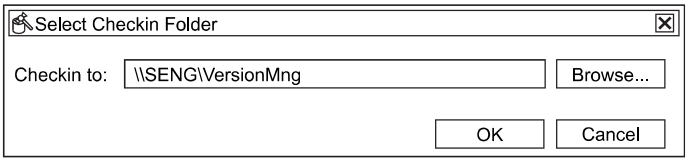


Figure F5.9-1 Select Checkin Folder dialog box

2. Specify the check-in folder.
   To change the check-in folder, enter the path to the folder directly or select it from the folder selection dialog box displayed by clicking [Browse] button.

TIP

An error dialog box appears if the specified folder does not exist.

3. Click [OK].
   The check-in folder is specified. The structure of the specified folder is displayed in the version control DB display area.

F6. Project Comparing Tool

The Project Comparing Tool is a tool for detecting, displaying and printing differences between two specified SCS projects.

F6.1 Overview of project comparison

Using the Project Comparing Tool, you can check the differences between two projects, which is useful in such a case when you have created a similar project using the data of an existing SCS project. It is recommended to print the detected differences and use them for checking at your desk. If no differences were detected, it can be considered that the two projects are the same.

Comparable project data

With the Project Comparing Tool, the data of any two SCS projects can be compared. The following three types of project data are comparable, and you can specify any combination of these project data.

- Project work database
- Project master database
- Project saved by version control tool
  (work database and master database)

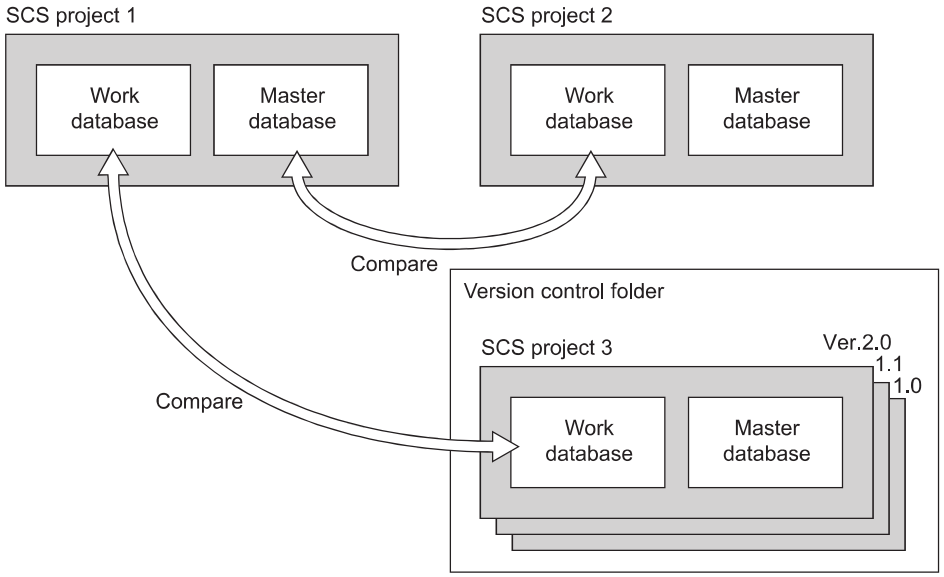


Figure F6.1-1 Comparison of project data by Project Comparing Tool

F6.2 Window configuration of Project Comparing Tool

This section describes the window configuration of the Project Comparing Tool.

The following figure shows an example of the display after project comparison is executed.

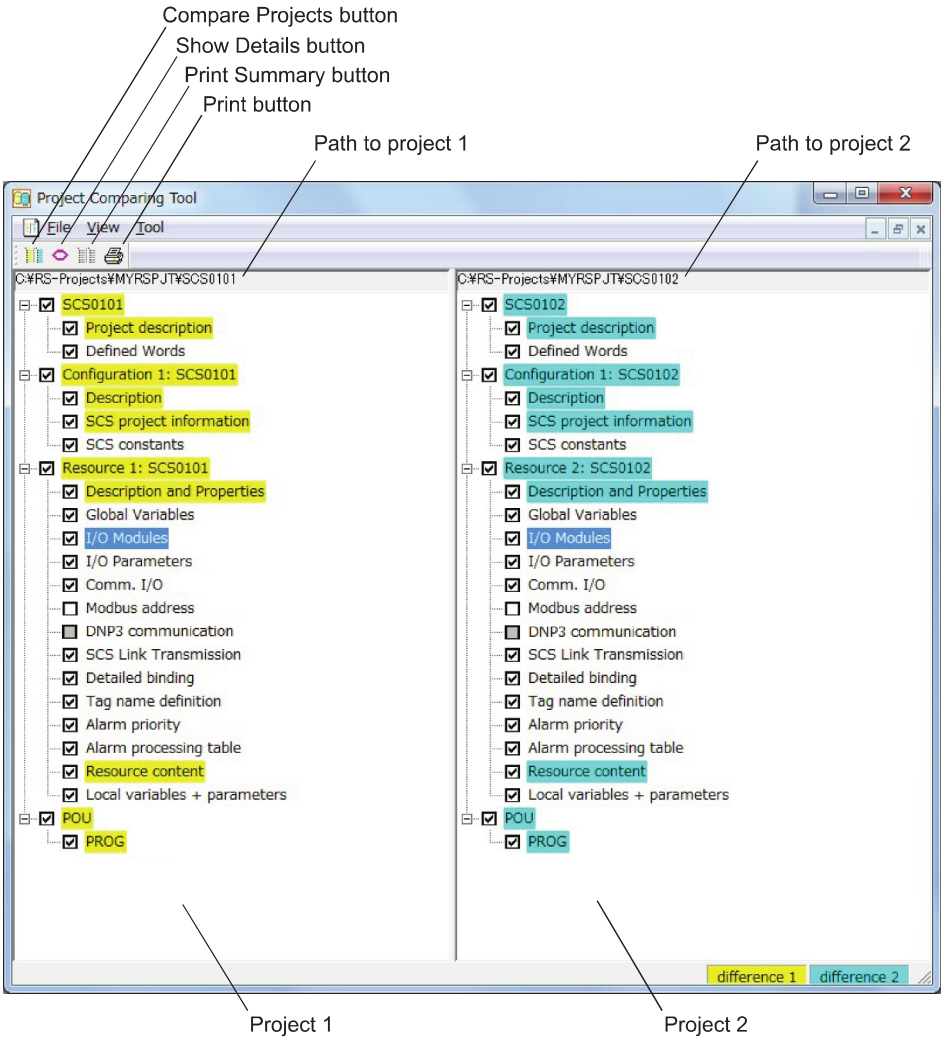


Figure F6.2-1 Window of Project Comparing Tool

When the SCS project subject to comparison includes engineering data created with AD Organizer, ADS appears to the right of the SCS project name.

SEE ALSO For more information about display example, refer to:

"■ Comparing projects" on page F6-6

■ Compared items list display

When two projects that you wish to compare are specified, the data items of each project are displayed in a tree view in the left and right panes. Above each tree, the path of the project is displayed. When comparison is executed, data of the items with their check box selected are compared, and the items where any difference was detected are marked with yellow (Project 1) and cyan (Project 2).

Also, among the items where any difference was detected, those items for which detailed information is to be displayed or printed may also be selected by check boxes.

The following table lists the data items compared by the Project Comparing Tool.

Table F6.2-1 Compared items list

Item		Remarks
Station	Project description	-
	Defined words	-
Configuration	Description	-
	SCS project information	-
	SCS constants	Items set in the SCS Constants Builder
Resource	Description and properties	-
	Global variables	Among the variables defined in the dictionary, those that are global
	I/O modules	-
	I/O parameters	Items set in the I/O Parameter Builder
	Comm. I/O	Items set in the Communication I/O Builder
	Modbus address	Items set in the Modbus Address Builder
	DNP3 communication	Items set in DNP3 Communication Builder
	SCS Link Transmission	Items set in the SCS Link Transmission Builder
	Detailed binding	-
	Tag name definition	Items set in the Tag Name Builder
	Alarm priority	Items set in the Alarm Priority Builder
	Alarm processing table	Items displayed in the Alarm Processing Table Builder
	Resource content	List of user-defined groups and POUs
	Local variables + parameters	Among the variables defined in the dictionary, local variables of the POU
POU	POU name	Logic defined in Multi-language Editor

For items other than POUs, the same items are displayed in the left and right panes.

The POU display order is as follows:

- Project 1: The order of execution.
- Project 2: The order in which matches with a POU name of Project 1 are found. However, POUs that do not exist in Project 1 are added at the end.

Menu bar

The menu bar provides the following menus

- [File] menu
- [View] menu
- [Tool] menu

The menu items of each menu are explained below.

Table F6.2-2 File menu

Menu Item	Description
Compare Projects	Start comparison of the items for which the check box is selected.
Select Projects Paths	Call the dialog box for setting the paths of SCS projects to be compared.
Print Summary	Print a summary of the comparison results.
Print	Print the detailed differences of the items for which the check box is selected.
Exit Project Comparing Tool	Close the Project Comparing Tool.

Table F6.2-3 View menu

Menu Item	Description
Toolbar	Switch between show and hide the toolbar.
Status Bar	Switch between show and hide the status bar.

Table F6.2-4 Tool menu

Menu Item	Description
Show Details	Display the detailed differences of the items for which the check box is selected.
Select Items	Call the dialog box for batch selection of check boxes.

Toolbar

The toolbar provides the following buttons.

Table F6.2-5 Toolbar buttons

Name	Description
Compare Projects	Start comparison of the items for which the check box is selected.
Show details	Display the detailed differences of the items for which the check box is selected.
Print summary	Print a summary of the comparison results.
Print	Print the detailed differences of the items for which the check box is selected.

F6.3 Comparing two SCS projects

This section describes the procedure for comparing two specified SCS projects and the procedure for printing a summary of the comparison results.

About designation of projects

To designate two SCS projects for comparison, you need to specify the path to the top folder of the SCS projects. If you want to specify the master database of the SCS project, you can specify by selecting the "Master" check box.

To specify a version-controlled project, you need to specify the path to the folder of the version number under the check-in folder. In this case as well, by selecting the "Master" check box, the master database of the specified project will be the target of comparison.

Example:

To compare the data of version number 1.3 of the SCS project SCS0101 which is saved in the check-in folder `\\SENG_DB_PC\VER\MYRSPJT`, specify the path as follows.

```
\\SENG_DB_PC\VER\MYRSPJT\SCS0101\1.3
```

SEE ALSO For more information about version-controlled project databases, refer to:

F5., “Version control” on page F5-1

Comparing projects

IMPORTANT

- Before using the Project Comparing Tool, close SCS Manager. The Project Comparing Tool and the SCS Manager cannot be used at the same time.
- An SCS project that is opened by the SCS Manager on another SENG cannot be compared.

Follow these steps to run a comparison of projects.

1. Start Project Comparing Tool.
   A dialog box for specifying the top paths of the two SCS projects to be compared appears.

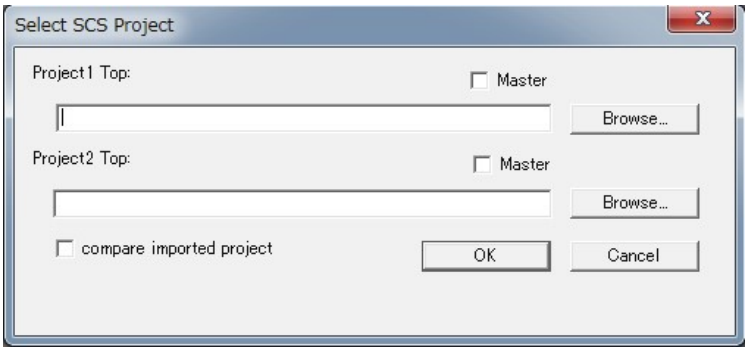


Figure F6.3-1 Select SCS Project dialog box

In the dialog box, the contents specified in the previous project comparison are displayed.

2. For Project1 Top and Project2 Top, specify the path to the top folder of each SCS project.
   a. Click [Browse] and select the top folder of the SCS project, or enter the path directly.
   b. When specifying the master database of the specified SCS project, select the "[Master]" check box. When specifying a work database, leave the "[Master]" check box clear.
3. To compare one project with another project re-created by importing that entire project, select the "[compare imported project]" check box in the select project dialog box. Normally, when comparing a project before changes against the project after changes, leave the "[compare imported project]" check box clear.
4. Click [OK].
   If a password has been set in the project, a dialog box for entering the password appears.
5. Enter the password, and click [OK].

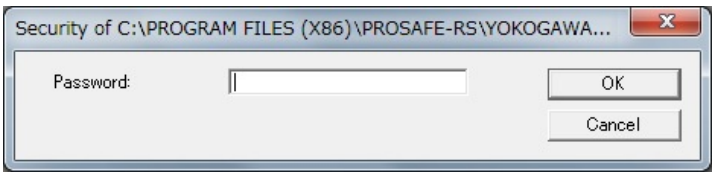


Figure F6.3-2 Project Password Input dialog box (Project 1)

A list of defined items of the two projects appears. All of the check boxes of the items are clear.

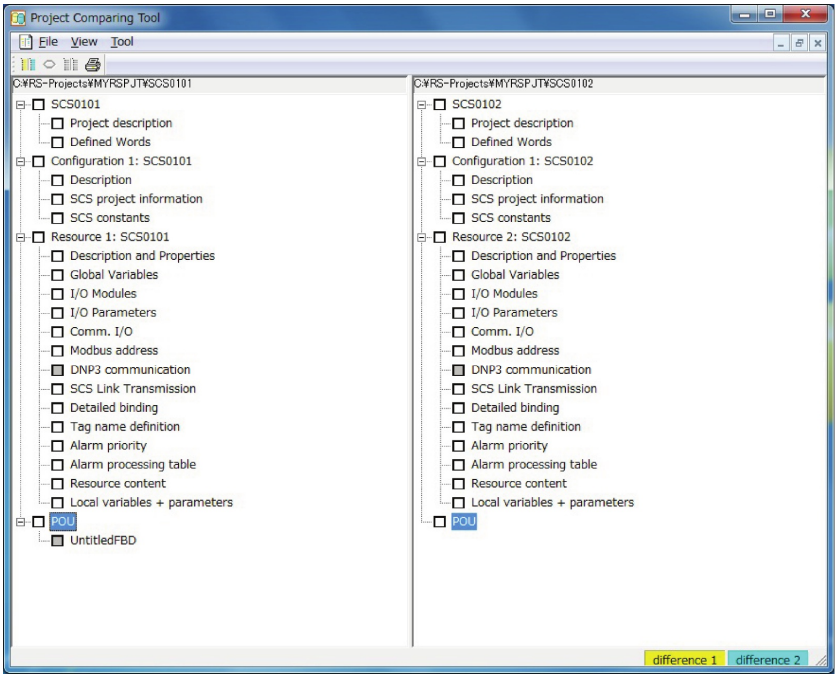


Figure F6.3-3 Project Comparing Tool (at start-up)

TIP

An error message appears in the following cases:

- The specified folder is not an SCS project folder.
- The specified path does not exist.
- The specified SCS project is opened on the SCS Manager of another SENG.
- The password entered is not correct.

Note that if the wrong password is entered three times consecutively, the process is discontinued, and it returns to the Select SCS Project dialog box.

6. Select the check boxes of items in which you want to detect differences.
   When a check box is selected on the tree on either the left or right, the check box of the same item is selected on the other tree.

TIP

- You can select all items at once in this way: From the menu bar, select[Tool] > [Select items]In the dialog box that appears, select [Select All].

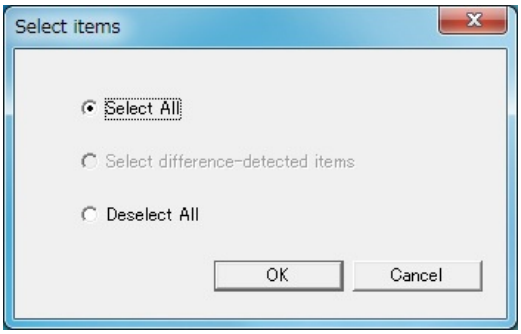


Figure F6.3-4 Select items dialog box

- Check boxes of the items that exist in only one of the projects are displayed in gray and cannot be selected for comparison.

7. From the menu bar, select [File] > [Compare Projects] to start the project comparison.
   A progress bar is displayed during difference detection.

When the comparison is finished, difference-detected items are marked in yellow on Project 1 and in cyan on Project 2. For items in which any difference was detected, the top-level item name is also marked, so that it is easy to see where there are differences even when the tree is collapsed.
When the SCS project subject to comparison has a difference of having or not having engineering data created with AD Organizer, the background color of the SCS station node will not be changed.

Executing project comparison for the second time and thereafter

To perform another SCS project comparison after a project comparison was executed after the Project Comparing Tool was started up, perform the following procedure.

1. From the menu bar, select [File] > [Select projects paths].
   The Select SCS Project dialog box appears.
2. Specify the paths to the SCS projects to be compared, and perform the compare operation.

Printing a project comparison results summary

A summary of the differences detected by executing a project comparison can be printed.

To print a summary of project comparison results, perform the following procedure.

1. With the comparison results displayed in the window of the Project Comparing Tool, select [File] > [Print summary] from the menu bar.
   The comparison results are printed.

An example of a printed summary of project comparison results is shown in the following figure.

```
Project Compare Result Summary  [Time:2017/02/27 10:00:00]
[for comparing imported project]
Project1: C:\RS-Projects\Ti\ToolCompare\RSPJT1\SCS1105          Ver:0.1  ProjectDate:2017/02/11
Project2: C:\RS-Projects\Ti\ToolCompare\RSPJT3\SCS1105[Master]  Ver:1.0  ProjectDate:2017/02/17

Project1                                                  Project2
* SCS1105                                                 * SCS1105
  * Project description                Not Changed          * Project description
  * Defined words                      Not Changed          * Defined words

* Configuration 1:SCS1105                                 * Configuration 1:SCS1105
  * Description                        Not Changed          * Description
  * SCS project information            Not Changed          * SCS project information
  * SCS constants                      Not Changed          * SCS constants

* Resource 1105: SCS1105                                  * Resource 1105: SCS1105
  * Description and properties         Not Changed          * Description and properties
  * Global variables                   Changed              * Global variables
  * I/O modules                        Changed              * I/O modules
  * I/O parameters                     Changed              * I/O parameters
  * Comm. I/O                          Not Changed          * Comm. I/O
    Modbus address                     -----------            Modbus address
    DNP3 communication                 -----------            DNP3 communication
  * SCS link transmission              Not Changed          * SCS link transmission
  * Detailed binding                   Not Changed          * Detailed binding
  * Tag name definition                Not Changed          * Tag name definition
  * Alarm priority                     Not Changed          * Alarm priority
  * Alarm processing table             Not Changed          * Alarm processing table
  * Resource content                   Not Changed          * Resource content
  * Local variables + parameters       Not Changed          * Local variables + parameters

* POU                                                      * POU
  * Prog01                             Not Changed          * Prog01
    Prog02                             Deleted                -
  * Prog03                             Changed              * Prog03
  * FB01                               Changed              * FB01
    FU01                               -----------            FU01
     -                                 Added                  Prog04
     -                                 Added                  FU02
```

Figure F6.3-5 Example of printed summary of comparison results

Information printed in project comparison results summary

The following information is printed in the header:

- Time: Time that summary was printed
- [for comparing imported project]: Printed when the compare imported project check box is selected in the Select SCS Project dialog box.
- Project 1, Project 2: Paths to compared project data
  In the case of a master database, [Master] is printed.
- Ver: Version number
  Version number set by Version Control Tool. This item remains blank for non version-controlled projects.
- Project Date: Project date (date set in project properties)

For the items that were compared, an asterisk (*) is printed, and the following information is printed in the center column:

- Changed: There is a difference
- Not Changed: There is no difference
- Deleted: Item that exists only in Project 1
- Added: Item that exists only in Project 2
- ----------: Item that was not compared

F6.4 Checking contents of detected differences

After project data comparison has been executed, the detailed contents of detected differences can be displayed and printed.

If a password is set for POUs, password input is required.

Displaying detailed differences

Differences are displayed in a Difference Display window for each selected item. Although multiple windows can be displayed at a time, only one POU Difference Display window can be displayed. For this reason, if another POU is selected while a certain POU's differences are displayed, the previously opened window will close.

Display procedure for items other than POUs for which a password is set

To display detailed differences, perform the following procedure.

1. From the tree view where project comparison results are displayed, click one item name for which you wish to see the detailed differences.
2. From the menu bar, select [Tool] > [Show details].
   The Difference Display window of the selected item appears.

Display procedure for POUs for which a password is set

Password input is required when displaying the detailed differences of a POU for which a password is set. The input POU password is stored, and is saved until the path to the project is changed in the Select Project dialog box. For this reason, password input is not required when displaying the detailed differences of a certain POU after displaying the detailed differences of the same POU using the correct password.

To display the detailed differences of a POU for which a password was set, perform the following procedure.

1. From the project comparison results display, click the POU name for which you wish to see the detailed differences.
2. From the menu bar, select [Tool] > [Show details].
   A dialog box for entering the POU password of Project 1 appears.



Figure F6.4-1 POU Password Input dialog box (Project 1)

3. Enter the POU password.
4. Click [OK].
   If release of password protection is successful, a dialog for entering the POU password of Project 2 appears.

   If the wrong password is entered three times consecutively, the process is discontinued.

TIP

- After the process is discontinued, if that POU is selected again and the [Show details] command is executed, the password input dialog box appears.
- When [Cancel] or [Skip] is clicked in the Password Input dialog box, the display of detailed differences is discontinued.

5. Similarly, input the POU password for Project 2 and click [OK].
   If release of password protection is successful, the Difference Display window of the selected POU appears.

Difference Display window

Differences are displayed in a window of the engineering function, such as builders, that is started up in "viewer mode." Only browsing is enabled in this window. The definitions cannot be edited or downloaded.

In the Difference Display window, the definitions of Project 1 are displayed on the top pane and those of Project 2 are displayed on the bottom pane, with the differences displayed in red. The toolbar has "Find Next" and "Find Previous" buttons. When either button is clicked, a difference is selected and highlighted. The highlight moves to the next or previous difference each time the button is clicked.

The following figure is an example of the display when a POU is selected.

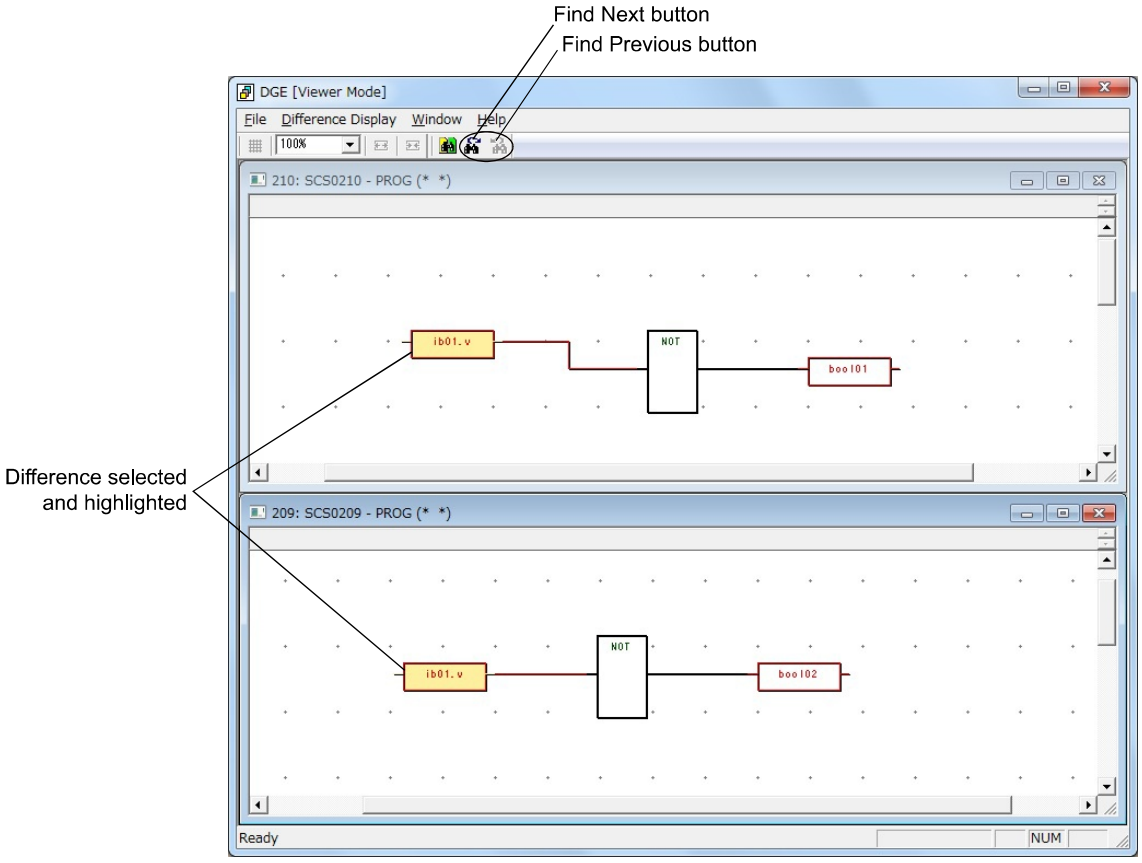


Figure F6.4-2 Example of detailed difference display when a POU is selected

Differences in the positions or shapes of graphics in POU diagrams are also displayed as differences.

The following figure is an example of the display when an item other than a POU is selected.

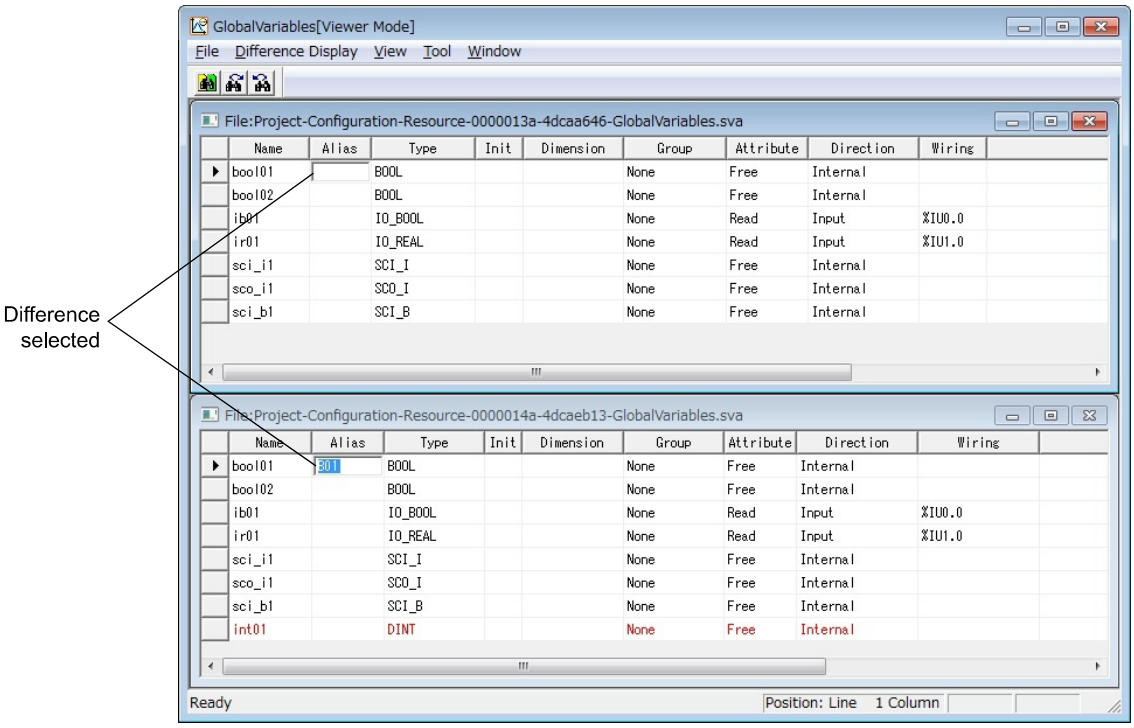


Figure F6.4-3 Example of detailed difference display when an item other than a POU is selected

Printing detailed differences

This section describes the procedure for printing the details of detected differences after a project comparison. Password input is required when printing the information for a POU that has a password.

Perform the following procedure to print detailed differences.

1. From the project comparison results display, select the check box of the item for which you wish to print the detailed differences.
   To select all the check boxes of the items where differences were detected, select [Tool] > [Select Items] from the menu bar; in the displayed dialog box, select "Select difference-detected items."
2. From the menu bar, select [File] > [Print].
   The Start Print dialog box appears.
3. Click [OK] to start printing.
   - When password-set POUs are not selected, differences are printed for all selected items, and the process ends.
   - If any password-set POU is selected, a dialog box for entering the POU password appears. Proceed with the following procedure.
4. Perform any of the following operations in the dialog box for entering the POU password.
   - To print, enter the POU password and click [OK].
   - To print the next POU without printing the current POU, click [Skip].
   - To discontinue the printing process, click [Cancel].

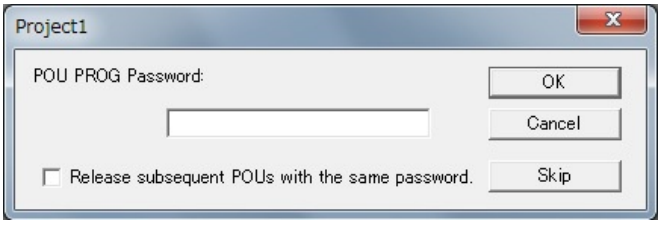


Figure F6.4-4 POU Password Input dialog box (Project 1)

TIP

- When the "Release subsequent POUs with the same password" check box is selected, the password input dialog will not appear for subsequent POUs with the same password.

  Note that passwords for POUs of Project 1 and POUs of Project 2 are handled separately.
- If the wrong password is entered three times consecutively, the process is discontinued and moves to the printing for the next POU.

If release of POU password protection for Project 1 is successful, the POU password input dialog box for Project 2 appears.

5. Enter the POU password for Project 2.
   The differences of the POU are printed.

When the differences of all selected items have been printed, the process ends.

If there are POUs that failed to release password protection or skipped POUs, a warning dialog box that displays a list of those POUs appears when the printing is finished.

Print format of differences

The definition contents of Project 1 and Project 2 are alternately printed for each item. The differences are surrounded with a box, and are printed in red if printed in color.

The printing format is in accordance with the settings for self-documentation. Chapter numbers are the same as when printing by self-documentation, with page numbers in order when printed.

SEE ALSO

For more information about printing format of self documents, refer to:

"■ Self-documentation" on page F2-2

F7. Online monitoring

This function is used to monitor the application logic executed on the SCS.

It updates and displays the currently running program, values of variables that were assigned to function blocks, and condition status at regular intervals regardless of the SCS security level, as follows:

- Displays values of input/output variables and internal variables
- Displays BOOL-type variables and BOOL signal lines in different colors according to values. The user can customize the colors used for TRUE/FALSE
- Displays whether a variable is locked or not

The online monitoring function can be divided into the following four categories based on the display method:

- FBD Status Display
  FBD windows of Multi-Language Editor
- LD Status Display
  LD windows of Multi-Language Editor
- ST Status Display
  ST windows of Multi-Language Editor
- Variable Value List Display
  I/O Lock Window

  SCS Link Transmission Lock Window

  Inter-SCS Communication Lock Window

  Communication I/O Lock Window

  Dictionary View

  Spy List

When iDefine is used, you can use the online monitoring function by connecting to ProSafe-RS from iDefine through the iDefine Test Manager.

SEE ALSO

For more information about I/O Lock Window, refer to:

F8.8.1, “I/O Lock window” on page F8-31

For more information about SCS Link Transmission Lock Window, refer to:

F8.9, “SCS Link Transmission Lock window” on page F8-44

For more information about Inter-SCS Communication Lock Window, refer to:

F8.10, “Inter-SCS Communication Lock window” on page F8-55

For more information about Communication I/O Lock Window, refer to:

F8.11, “Communication I/O Lock window” on page F8-69

Starting the window for online monitoring

Lock windows can be launched while SCS Manager is in the editing mode or debug mode. In the case of online monitoring-related windows other than lock windows, online monitoring is enabled when SCS Manager enters the logic simulation mode or debug mode.

To switch to logic simulation mode, select [Simulation] from the SCS Manager [Debug] menu. To enter the debug mode, select [Debug] from the [Debug] menu of SCS Manager.

Online monitoring and security

Whether you can perform forcing on online monitoring related windows differs, depending on the security level of the SCS. In addition to the security settings for the database, the ability to view the POU also depends on whether a password has been set in the POU or not.

Relationship with SCS security levels

On online monitoring related windows, you can perform online monitoring at any SCS security level.

- Use windows related to online monitoring at security Level 2 to monitor the application logic status without changing values of variables and other data inadvertently.
- Lower the security level and use the forcing function to specify variables in the online monitoring window.

Relationship with database security

On the Online Monitoring related windows, the POU can always be accessed in read-only mode regardless if the SCS project and the library are in read-only mode or protected by a password. The accessibilities of the POU vary with password protection. How POU can be accessed is shown as follows:

- When accessing a POU without password protection, the POU can be opened in read-only mode.
- When accessing a POU with password protection, password entry is required for the first time opening the POU, and the POU will be opened in read-only mode. From the second time, the POU will be opened in read-only mode without prompting for password.
- When accessing a POU with password protection, the POU cannot be opened unless the password is properly entered.

F8. Forcing function

The forcing function enables you to fix a variable (lock a variable) and forcibly modify the value. Specifically, you can lock the variables in an application logic, channel input and output values of the I/O module, and the data of SCS link transmission, inter-SCS safety communication, subsystem communication, and safety subsystem communication.

Run the forcing function in the following windows:

- I/O Lock Window
- SCS Link Transmission Lock Window
- Inter-SCS Communication Lock Window
- Communication I/O Lock Window
- Multi-Language Editor (FBD)
- Multi-Language Editor (LD)
- Dictionary View
- Spy List window

IMPORTANT

- To execute the forcing function, it is necessary to set the SCS security level to Level 1 or 0.
- The forcing function can be used in the target test, the SCS simulation test and the logic simulation test. However, the I/O Lock Window, SCS Link Transmission Window, Inter-SCS Communication Lock Window, and Communication I/O Lock Window cannot be started for the logic simulation test.

When iDefine is used, you can use the forcing function by connecting to ProSafe-RS from iDefine through the iDefine Test Manager of AD Organizer. The conditions to use the forcing function and the actions that can and cannot be done from iDefine are described as follows:

- To execute the forcing function from iDefine, you must set the SCS security level to 0.
- From iDefine, the forcing function can be applied only on the following variables:
  - I/O variables that were defined using the Safety I/O Editor and imported to iDefine.
  - Variables that were defined using iDefine
- You can lock the I/O modules in SCS from iDefine.
- You cannot force the SCS link transmission data, inter-SCS safety communication data, and subsystem communication from iDefine. Instead, you must use SCS Link Transmission Lock window, the Inter-SCS Communication Lock window and the Communication I/O Lock window respectively.

SEE ALSO For more information about Forcing from iDefine, refer to:

4., "PROSAFE-RS IO MODULE" in iDefine User Guide (Yokogawa Extensions) (PR12002-MAN-980_01)

Applications of the forcing function

The forcing function is used in SCS maintenance and application debugging.

In application debugging, the forcing function is used for the following purposes:

- Setting the variable and the function block parameter values for debugging the application logic
- Locking Input/Output Modules
- Locking Input/Output Channels for the Purpose of Wiring Tests
- Locking for the purpose of inter-SCS safety communication tests (producing or consuming sides)
- Forcing during debugging of the application logic that uses subsystem communication and safety subsystem communication
- Disconnect I/O during maintenance of a communication module
- Disconnect I/O during maintenance of a PROFINET IO-Device connected to the fire and gas communication module

In SCS maintenance, the forcing function is used for the following purposes:

- Locking I/O variables for all channels of each input/output module if the required input/output module is not available or the field wiring has not been completed
- Locking I/O variables for all channels of each AIO/DIO module when channels of the AIO/DIO module are faulty and the module has to be replaced
- Locking input/output modules to prevent nuisance tripping during online modification of input/output modules
- Locking input/output channels for maintenance
- Locking input/output channels to prevent nuisance tripping during online modification of application logic
- Locking function blocks on the producing or consuming sides to prevent nuisance tripping due to error occurrence in inter-SCS safety communication during online change download and offline download

The forcing function can be used in target tests, SCS simulation tests and logic simulation tests. However, the I/O Lock Window, SCS Link Transmission Lock Window and Communication I/O Lock Window cannot be used for the logic simulation tests.

Debugging application logic

If you lock variables, you can change values such as input data and function block parameter. As a result, debugging application logic can be performed on different conditions.

Locking Input/Output modules

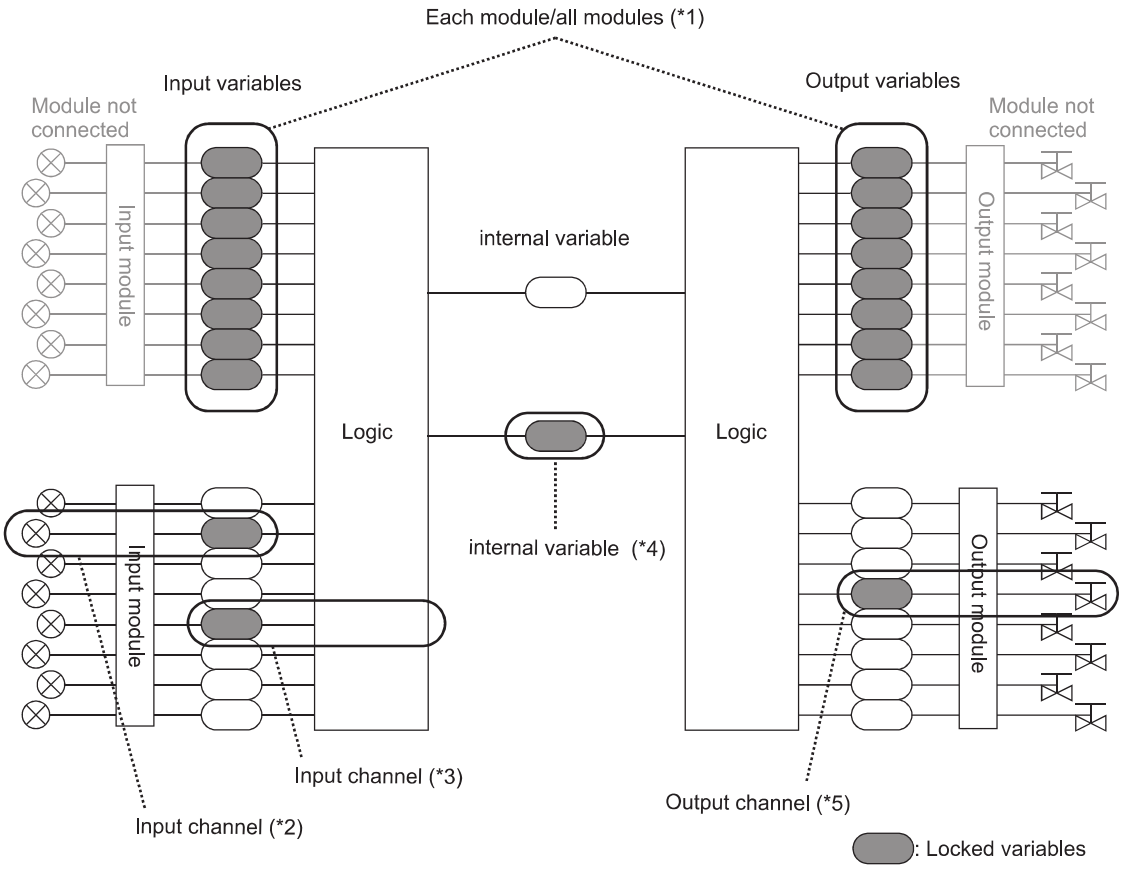
Variables can be locked for all channels of each input/output module if the required input/output module is not available or the field wiring has not been completed, thereby preventing the application logic from being influenced by input data and data status changes of input/output channels.

It is also possible to lock all the variables of multiple input/output modules in one operation.

Locking Input/Output channels for the purpose of wiring tests

By locking input variables, it is possible to conduct wiring tests on the input side (field wiring/device) without transmitting changes of values of the input channels and conditions on the input side to the logic side. The actual input values can be checked in the I/O Lock window.

Similarly, by locking output variables, it is possible to conduct wiring tests on the output side without transmitting changes of the values of the logic side to the output channels. In this case, the operation on the output side can be checked by changing the values of the locked output variables.



*1: Disconnection of AIO/DIO module
*2: Input field wiring test
*3: Logic debugging by changing input data
*4: Logic debugging by changing internal variable
*5: Output field wiring test

Figure F8-1 Applications of the forcing function

● Locking for debugging Inter-SCS safety communication

It is possible to lock and set values for function blocks using the Inter-SCS Communication Lock Window in order to debug inter-SCS safety communication applications. By locking either the producing or consuming side function blocks and setting values for individual function blocks, it is possible to change the execution conditions of application logics for debugging.

■ System function blocks related to the locking function

The locking units will differ depending on the target of the Forcing. The locking status can be managed with a system function block. System function blocks related to the locking function are shown in the table below.

Table F8-1 System function blocks related to the subjects of forcing

Target	Unit of locking	Related System function blocks	Precaution at locking
I/O channels of AIO/DIO modules (*1)	Each channel, or each module	SYS_FORCE • If the total number of locked variables exceeds the pre-defined limit, this function block can issue a diagnostic information message to notify the user. • If the duration of locking exceeds the pre-defined time limit, this function block allows generating a diagnostic information message to notify the user. • It is possible to unlock all locked variables.	If I/O variables are locked, even when an error occurs in the corresponding channel of the I/O device, the error will not be relayed to the logic.(*2)
Variables in application logic (*1)	Each variable		In the case of SCSP2/ SCSP3/SCSL2, if you lock internal variables, the CPU load (execution time) increases compared to the status where no internal variables are locked.
Subsystem communication data (*3)	Each module	SYS_FORCE_SC (*4) • If the duration of locking exceeds the pre-defined time limit, this function block allows generating a diagnostic information message to notify the user. • It is possible to unlock all locked variables. It is also possible to cancel the lock status of variables that are deleted by online change while being locked.	If subsystem communication is locked, even when an error occurs in the data status, it is not notified to the logic.
Safety subsystem communication data (*5)	Each communication definition (each PROFINET module)	SYS_FORCE_SF (*4) • Subsystem communication data and I/O variables are not included in communication definitions. • You can use the forcing function to force an unlocking of all locked communication I/O definitions. • When the state of there being one or more locked communication definitions continues for more than the specified monitoring time, a diagnostic information message is issued and notified to the user. This diagnostic information message is resent every time the specified amount of monitoring time passes. • A diagnostic information message is notified when the maximum number of communication definitions that can be locked at the same time is exceeded. When returning to the maximum number of less, a diagnostic information message for recovery is notified.	When safety subsystem communication is locked, even when an error occurs in the data status, it is not notified to the logic.

Continues on the next page

Table F8-1 System function blocks related to the subjects of forcing (Table continued)

Target	Unit of locking	Related System function blocks	Precaution at locking
Inter-SCS safety communication data (*3)	Each SCS	SYS_FORCE_BD • If the total number of stations whose inter-SCS safety communication data is locked exceeds the pre-defined limit, this function block can issue a diagnostic information message to notify the user. • If the duration of locking inter-SCS safety communication data exceeds the pre-defined time limit, this function block can issue a diagnostic information message to notify the user. • It is possible to unlock all locked producer FBs and consumer FBs. The locked status of a producer FB or consumer FB that has been deleted while being locked can be canceled through an online change.	If inter-SCS safety communication data is locked, even when an error occurs in the data status, it is not notified to the logic.
SCS link transmission data (*3)	Each SCS	SYS_FORCE_LT • If the total number of stations whose SCS link transmission data is locked exceeds the pre-defined limit, this function block can issue a diagnostic information message to notify the user. • If the duration of locking SCS link transmission data exceeds the pre-defined time limit, this function block can issue a diagnostic information message to notify the user. • It is possible to unlock all locked link transmission data. The locked status of link transmission data that has been deleted while being locked can be canceled through an online change.	If SCS link transmission data is locked, even when an error occurs in the data status, it is not notified to the logic.

*1: Forcing can also be run from iDefine.
*2: Diagnostic information messages notifying abnormality are generated, however. Some system function blocks detect errors without being affected by locking.
*3: Forcing cannot be run from iDefine.
*4: Only whether or not subsystem communication data is locked is detected. The number of locks is not counted.
*5: Controls the forcing status of safety communication I/O definitions.

SEE ALSO For more information about CPU load when internal variables are locked with SCSP2/SCSP3/SCSL2, refer to:

A7.3, “Locking of internal variables and performance in SCSP3/SCSL2/SCSP2” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

F8.1 Variable locking

It is possible to fix (lock) values of I/O variables and internal variables of the application logic to constant values, regardless of the input values from the actual input devices and application operation results.

This section describes the behavior of the input variables, the output variables and the internal variables when they are locked, as well as the behavior of the system function blocks during locking.

Overview of variable locking

All variables of the application logic have two values: a value written from the input side and a value read from the output side. Normally, the value on the output side is constantly overwritten with the value on the input side during the execution of the application logic. For this reason, the value written to the variable and the value read from the variable match each other.

The locking function is a function to stop overwriting values on the output side with values on the input side. As a result, the values maintained on the output side are used regardless of the values from the input side.

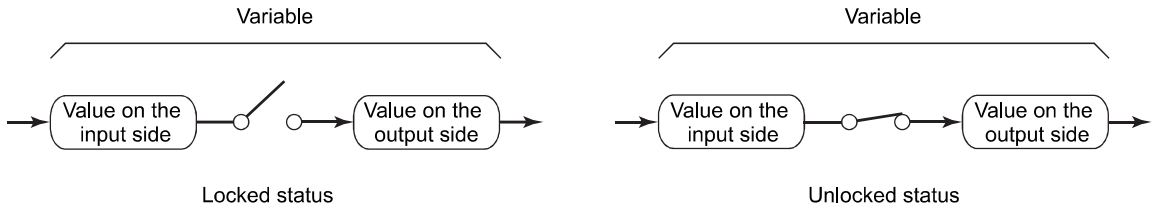


Figure F8.1-1 Overview of the locking function

In the case of an input variable, the value on the input side is the input from the input channel and is called physical data. The value of an input variable on the output side is read by the application logic and is called logical data.

An input variable consists of input data and data status.

In the case of an output variable, the value of the input side is the result of application logic processing and is called logical data.

The value of the output side of an output variable is the output to the output channel and is called physical data. An output variable also consists of output data and data status, in the same way as an input variable.

CAUTION

- When unlocking I/O variables, make sure to check the logical data and physical data of I/O data and data status. Check that there will be no adverse effects of unlocking on the system, such as a value changing abruptly after canceling the lock, causing nuisance tripping. Physical data cannot be referenced from iDefine. If you have locked the I/O data from iDefine, pay extra attention when you unlock it.
- While the forcing function is executed, the system's safety functions are disabled. If you use the forcing function for the purpose of maintenance after starting the actual operation, quit the forcing function immediately after the completion of system maintenance and enable the system's safety functions so that they operate normally. At the completion of a target test or when quitting SCS Manager during a target test, a dialog box appears to call attention to locked variables. In this case, display a list of the locked variables using the I/O Lock window or other means and cancel the lock status of these variables.

Locking input variables

If an input variable is locked, the value of the input variable will no longer be overwritten with the value input from the input channel. The input data and data status from the input channel and those from the input variable are separated.

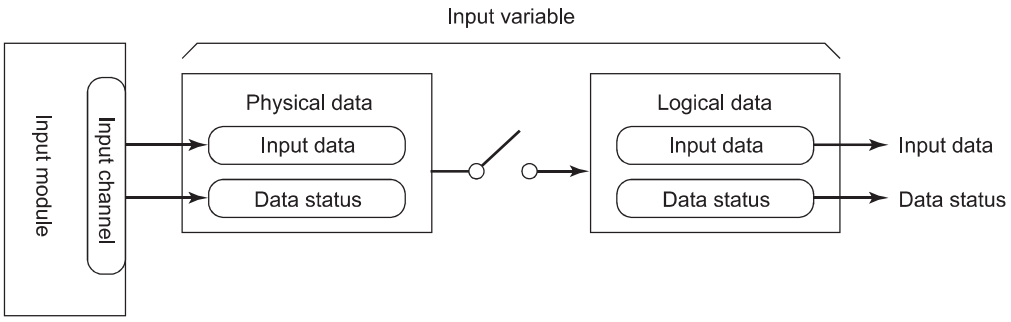


Figure F8.1-2 Locking input variables

If an input variable is locked, its logical data will no longer be overwritten with the value of the physical data. The value of the logical data matches the value of the physical data at the time of locking for both the input data and data status. The locked variable values can be changed after the lock operation.

Unlocking input variables

When the lock status of an input variable is canceled, the logical data will be overwritten with the value of the physical data again. Since input data values used by the application logic may change abruptly or the data status may change, caution is required not to adversely influence the operation of the application. For this reason, before canceling a lock, make sure to check that input data and data status match for physical data and logical data; if they are different, make sure that there will be no adverse effect on the application when unlocking.

Operations at input channel errors

While an input variable is locked, the data status of the input channel is disconnected. For this reason, even if an error occurs in the channel, the error cannot be detected by observing the data status of the input variable. Note that a diagnostic information message is notified at failure of the channel as well as its recovery from an error, regardless of whether or not the input channel is locked.

Notification of operation result via diagnostic information messages

If an input variable is locked or unlocked, the operation performed and the results of the operation are notified as a diagnostic information message.

Locking output variables

If an output variable is locked, the value of the output variable will no longer be overwritten with the value set by the application logic. The output channel and application logic are disconnected.

For output variables, the data status flows in the opposite direction of the output data.

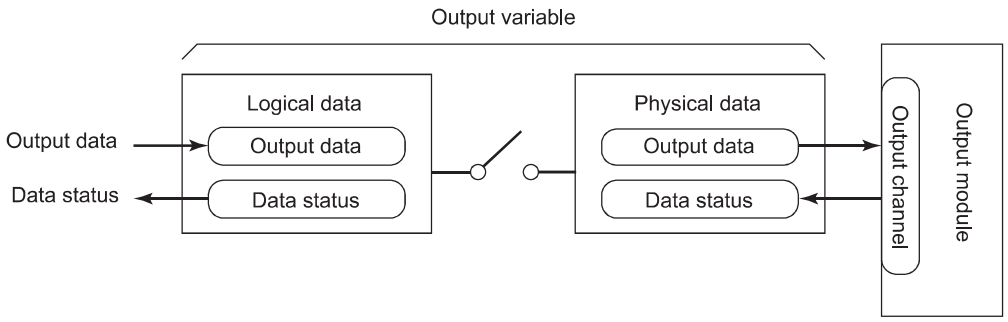


Figure F8.1-3 Locking output variables

If an output variable is locked, its values are fixed as follows.

- As for the output data, its physical data will no longer be overwritten with the value of the logical data. The value of the physical data matches the value of the logical data at the time of locking.
- As for the data status, the logical data status will no longer be overwritten with the value of the physical data status. The value of the logical data status matches the value of the physical data status at the time of locking.

Unlocking output variables

When the lock status of an output variable is canceled, the physical data will be overwritten with the value of the logical data again for the output data, and the logical data status will be overwritten with the value of the physical data status again. When the lock status is canceled, the output data values overwritten with the application logic may change or the data status used in the application logic may change. Thus, caution is required not to adversely influence the output to the field and the operation of the application. For this reason, before releasing a lock, make sure that the output data and data status of the physical data and logical data are consistent; if they are not, make sure that there will be no inadvertent affect to the applications when releasing the lock.

Operations at output channel errors

While an output variable is locked, the data status of the output channel is disconnected. For this reason, even if an error occurs in the channel, the error cannot be detected by observing the data status of the output variable. Note that a diagnostic information message is notified at the time of failure of the channel as well as its recovery from an error, regardless of whether or not the output channel is locked.

Notification of operation result via diagnostic information messages

If an output variable is locked or unlocked, the operation performed and the results of the operation are notified as a diagnostic information message.

Locking internal variables

If an internal variable is locked, it will no longer be overwritten by an input value or an application. If an array used in a ST (Structured Text) statement is locked, all the elements of the array will be locked.

In the case of SCSP2/SCSP3/SCSL2, an internal variable can be locked only when [Yes] is set for Extend Scan Period Automatically and [Enable] is set for Locking of Internal Variables in SCS Constants Builder. Note that if any internal variable is locked, the processing time of the application logic becomes longer.

In the case of internal variables, the value on the input side is called physical data and the value on the output side is called logical data.

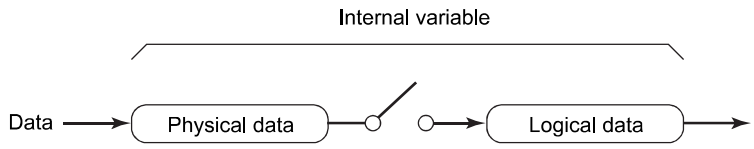


Figure F8.1-4 Locking internal variables

If an internal variable is locked, its logical data will no longer be overwritten with the value of the physical data. The value obtained by reading the internal variable is fixed with the value of logical data. The value of the logical data matches the value of the physical data when locked.

Unlocking internal variables

When the lock status of an internal variable is canceled, the logical data will be overwritten with the value of the physical data again. For an array, all the elements of the array will be unlocked. Since the data value overwritten with the application logic may change, caution is required not to adversely influence the operation of the application. For this reason, before canceling a lock, make sure to check that the data match for physical data and logical data; if they are different, make sure that there will be no adverse effect on the application when unlocking.

Notification of operation result via diagnostic information messages

If an internal variable is locked or unlocked, the operation performed and the results of the operation are notified as a diagnostic information message.

Operations of system function blocks during locking

System function blocks are divided into two types: those to which the actual status is notified regardless of the lock status of a variable, and those to which no module and channel errors are notified while a variable is locked.

- Function blocks to which the actual status is notified regardless of the lock status
  SYS_IOMDSP, SYS_DIAG, SYS_ALRDSP, SYS_OUTEN, SYS_ESBINF, SYS_NODEINF, SYS_N_OUTEN, SYS_N_IOMDSP, SYS_N_NODEINF, SYS_PSUDSP, SYS_CH_OUTEN
- Function blocks to which no module and channel errors are notified during locking
  SYS_IOALLST, SYS_NODEST, SYS_OUTST, SYS_OUTST16, SYS_INST, SYS_CHST, SCI_B, SCI_I, SCI_R, SCO_B, SCO_I, SCO_R, SYS_N_NODEST, SYS_N_IOST16, PNI_I, PNI_R, PSI_I, PSI_R

F8.2 Variable value setting

It is possible to set values for I/O variables and internal variables while they are locked. For a locked array, user can set values to the variables for each array element one by one. Values of variables can be set in the I/O Lock window, Multi-Language Editor and Dictionary View.

If a value is set for a variable while it is locked, the value is fixed to the set value. If you try to change the value of a variable while it is not locked, an error occurs and the value cannot be changed. However, the internal variables and the values for the parameters of the function block can be set without setting a lock only when the security level of SCS is Level 0.

This section describes operations performed when a value is set for each type of variable, namely, the input variable, output variable and internal variable.

Setting values for input variables

In the case of input variables, the variable setting function sets the values of both input data and data status to the corresponding values of the logical data.

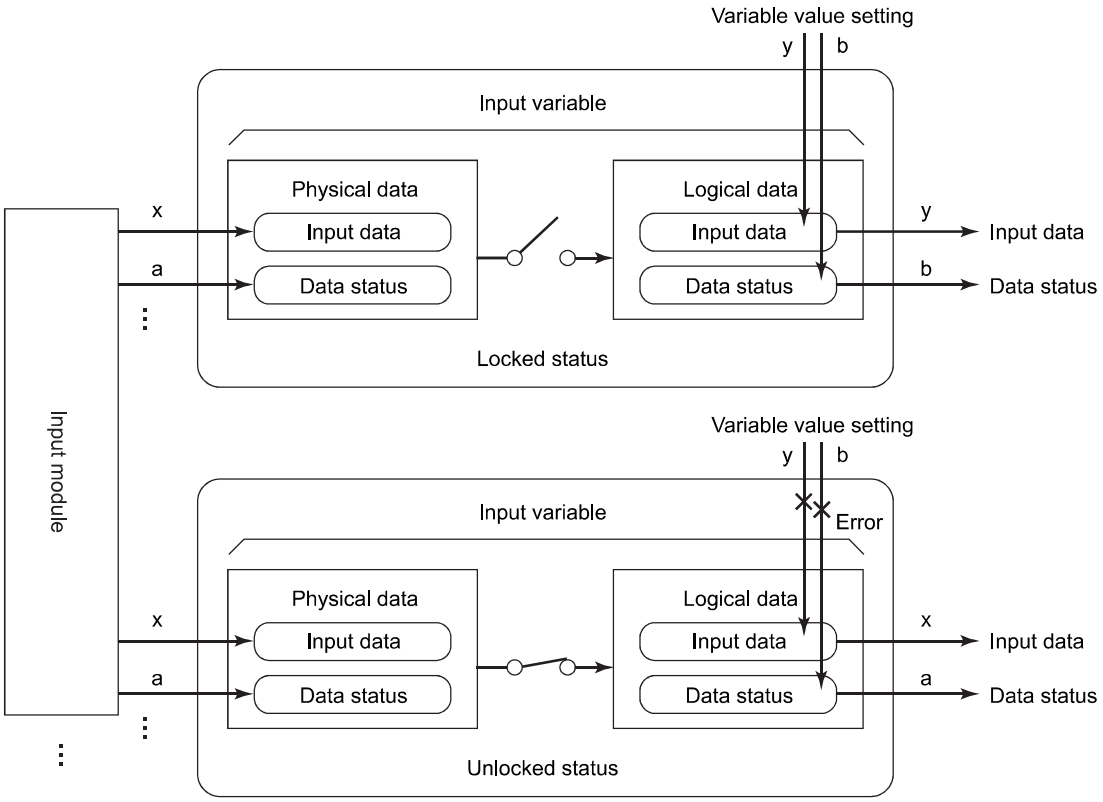


Figure F8.2-1 Setting values for input variables

- If a variable is locked
  The physical data is always updated with the value actually input from the input channel. The value of the logical data, on the other hand, is fixed to the set value because the physical data and the logical data are disconnected. In the application logic, the value fixed for the logical data is used, rather than the actual input value.
- If a variable is not locked
  When changing the data status or data value, an error will occur and the value cannot be changed.

Setting values for output variables

In the case of output variables, the variable setting function sets the value of the output data to the value of the physical data and the value of the data status to the logical data status.

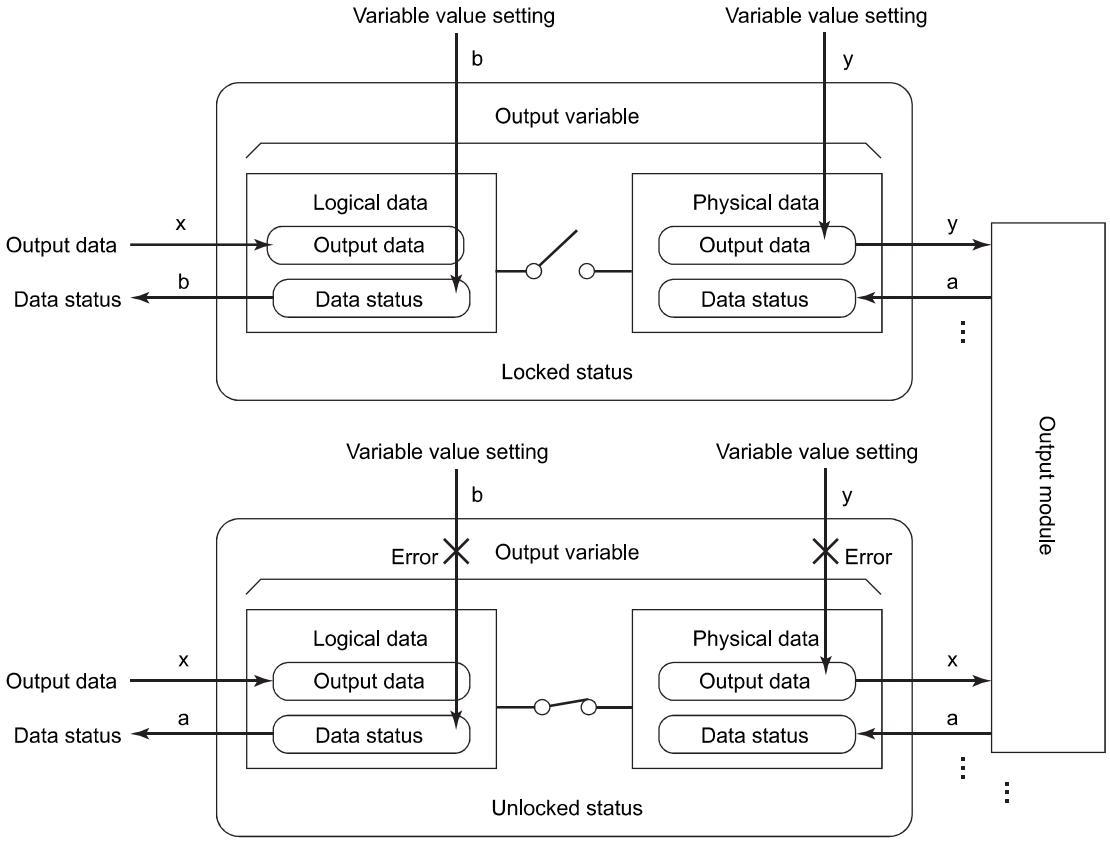


Figure F8.2-2 Setting values for output variables

- If a variable is locked
  The logical output data is always updated with the value calculated by the application logic. The value of the physical data, on the other hand, is fixed to the set value because the physical data and the logical data are disconnected. The value fixed for the physical data is actually output to the output channel. Note that only values in a range of -17.19 to 118.75 (%) can be set for the output variables that are connected to AO channels. Any attempt to set a value outside this range results in an error.

  The physical data status is always updated with the value actually input from the output channel. The value of logical data status, on the other hand, is fixed to the set value because the physical data and the logical data are disconnected. In the application logic, the value fixed for the logical data is used, rather than the actual input value.

- If a variable is not locked
  When changing the data status or data value, an error will occur and the value cannot be changed.

Value setting operation upon output channel error

In the case of an output channel error, the SCS locks the physical output data to the fail-safe value and the output is placed in the Output Disable status. Therefore, even if you lock the output variable corresponding to the error channel and set a desired physical data value using the variable setting function, the set value will be automatically overwritten by the fail-safe value.
Once the output channel returns to normal, you can set a desired physical data value.

If the I/O Parameter for specifying the output value at fault is set as follows, you can lock the output variable corresponding to the output channel error and set a desired value for the physical data:

- DO module: Output Value in Detecting Error or Output Processing at Fault is set to [Hold].
- AO module: Output Processing at Fault is set to [Hold].

SEE ALSO For more information about I/O Parameter related to the output value at fault, refer to:

"● Output value at fault" in "■ Overview of system operations at occurrence of fatal errors and major errors" in G2., "Operations and recovery procedures during the SCS error occurrence" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Setting values for internal variables

In the case of internal variables, the variable setting function sets a value for logical data.

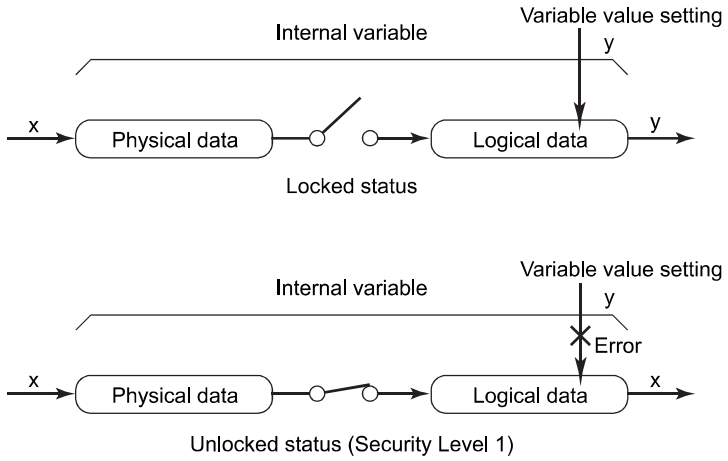


Figure F8.2-3 Setting values for internal variables

- If a variable is locked
  The physical data is always updated with the value written from application logic. The logical data, on the other hand, is fixed to the set value because the physical data and the logical data are disconnected. The value set for the logical data can be obtained by reading the value of the variable.
- If a variable is not locked
  When the SCS security level is Level 1, an attempt to set a value will result in an error, the value cannot be changed. While, if the SCS security level is Level 0, setting a value will not trigger any error. However, since the values of the internal variables in the logic are constantly overwritten by newer values, lock the variables before setting values.

Notification of operation result via diagnostic information messages

If a variable value is set, the operation performed and the results of the operation are notified as a diagnostic information message.

F8.3 Forcing function block parameters

The function block parameters can be forced for debugging the applications. The ranges can be forced in the user-defined function block is different from the other function blocks (hereinafter referred to as standard function blocks). Moreover, the range for the user-defined function blocks varies depending on whether the instance name is assigned or not.

Forcing user-defined function block parameters

For a user-defined function block, if the SCS security level is below Level 1 and the instance parameters are locked, the data values can be changed.

- On Multi-Language Editor, when a user-defined function block is selected and opened from a program POU, the function block window can be displayed. On the window, any selected parameter can be locked and the data value can be changed.
- The locks applied to the parameters, same as the I/O variables and the internal variables, cannot be released from the Multi-language Editor. However, the locks can be released from Dictionary View.
- In the program POU, if an instance in the user-defined function block is not assigned with an instance name, the parameter of the instance cannot be locked and the data value cannot be changed either.

However, if the SCS security level is Level 0, the data value can be changed anyway regardless if the parameter is locked or not.

Forcing standard function block parameters

When the SCS security level is Level 0, the function block parameters can be changed if the parameter is not locked.

- Only the parameter values of the standard function blocks that the instances are assigned with instance names can be changed.
- The parameter values of the standard function blocks can be changed from Dictionary View, but cannot be changed from Multi-Language Editor.

Moreover, when the SCS security level is Level 1, the parameter values of the standard function block cannot be changed. And the standard function block parameters cannot be locked regardless security levels.

Forcing scope and function block type

The following table shows what parameters of different type of function blocks can be forced.

Table F8.3-1 Forcing scope and function block type

Type	FB with Instance Name				FB without Instance Name			
	Target/SCS simulator		Logic simulator		Target/SCS simulator		Logic simulator	
	MLE (*1)	DIC (*2), iDefine (*3)	MLE (*1)	DIC (*2), iDefine (*3)	MLE (*1)	DIC (*2), iDefine (*3)	MLE (*1)	DIC (*2), iDefine (*3)
Basic data type Parameters of User-Defined FB	(*4)	(*5)	(*4)	(*5)	(*6)	(*7)	(*8)	(*7)
User-Defined Parameters of User-Defined FB in another user-defined FB (Local Parameters with Defined Names)	(*4)	(*5)	(*4)	(*5)	(*6)	(*7)	(*8)	(*7)

Continues on the next page

Table F8.3-1 Forcing scope and function block type (Table continued)

Type	FB with Instance Name				FB without Instance Name			
	Target/SCS simulator		Logic simulator		Target/SCS simulator		Logic simulator	
	MLE (*1)	DIC (*2), iDefine (*3)	MLE (*1)	DIC (*2), iDefine (*3)	MLE (*1)	DIC (*2), iDefine (*3)	MLE (*1)	DIC (*2), iDefine (*3)
User-Defined Parameters of User-Defined FB in another user-defined FB (Local Parameters without Defined Names)	(*6)	(*7)	(*8)	(*7)	(*6)	(*7)	(*8)	(*7)
User-Defined Parameters of Standard FB in another user-defined FB (Parameters with Defined Names)	(*7)	(*6)	(*7)	(*8)	(*7)	(*7)	(*7)	(*7)
User-Defined Parameters of Standard FB in another user-defined FB (Parameters without Defined Names)	(*7)	(*7)	(*7)	(*7)	(*7)	(*7)	(*7)	(*7)
Parameters of Standard FB	(*7)	(*6)	(*7)	(*8)	(*7)	(*7)	(*7)	(*7)

*1: MLE: Multi-Language Editor
*2: DIC: Dictionary View
*3: The SCS security level must be set to 0.
*4: Allowed to lock and set data but not unlock.
*5: Allowed to lock, unlock and set data
*6: Allowed to set data only when SCS Security level is Level 0.
*7: Not allowed to lock, unlock and set data.
*8: Allowed to set data only.

TIP

When using a forcing function for a parameter without name or an instance without instance name, the variable name column of the diagnostic information message will indicate its internal name assigned in the SCS Manager.

F8.4 Forcing of SCS link transmission data

Forcing of SCS link transmission data can be performed from the SCS Link Transmission Lock window of the SENG. The forcing function does not distinguish the SCS link transmission safety communication and SCS global switch communication.

Forcing of SCS link transmission data can be performed when the SCS security level is 1 or lower.

TIP

Forcing of SCS link transmission data can be performed only from the SCS Link Transmission Lock window. Forcing (lock operation, viewing lock status, setting values) cannot be performed by selecting link transmission-related function blocks in Dictionary View.

Function configuration of SCS link transmission data locking/unlocking

The relationship between data configuration, lock/unlock operation, and output enable operation regarding SCS link transmission data within an SCS is shown below.

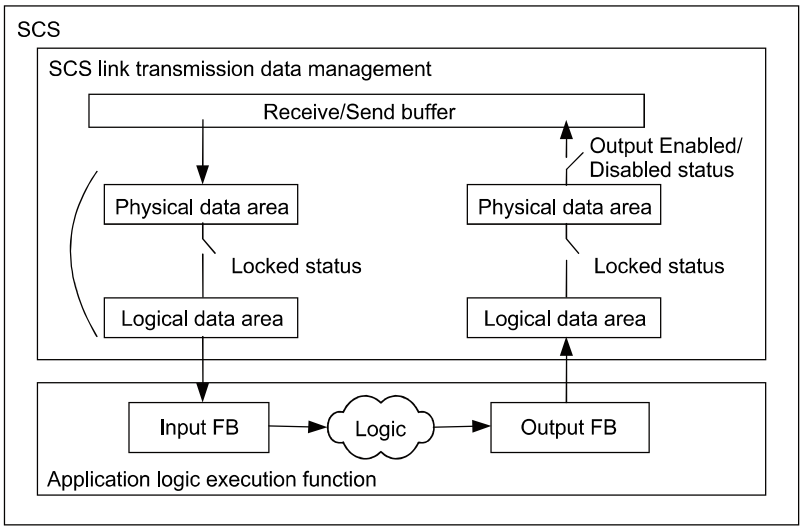


Figure F8.4-1 SCS link transmission data locking/unlocking

- SCS link transmission data has logical data and physical data, like I/O variables. These data can be referenced from the SCS Link Transmission Lock window.
- If the SCS link transmission is locked, logical data of the receive data and physical data of the send data can be set to any value from the SCS Link Transmission Lock window.

Locking SCS link transmission data

- It is possible to lock link transmission data of each station individually.
- When the local station is selected and locked, the send data will be locked. None of the output FB data values will be set to the physical data. The SCS sends the current value of physical data to other stations.
- If a receiving station is selected and locked, data from the applicable station (data value and data status) will be set only to the physical data but not to the logical data.

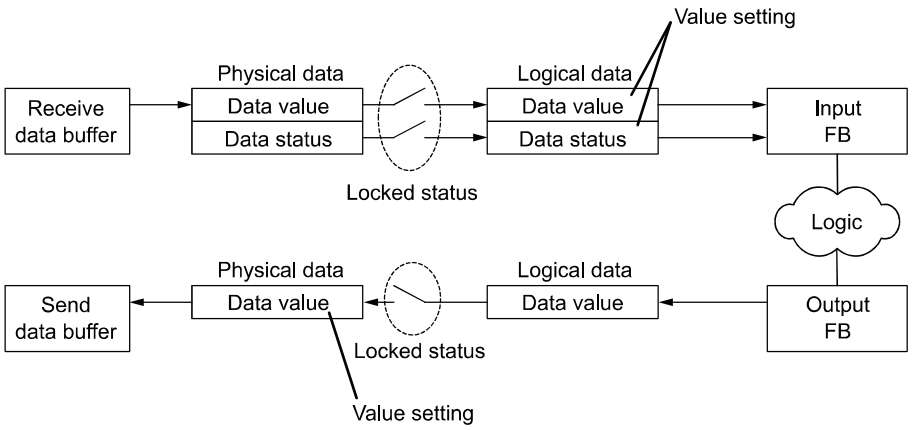


Figure F8.4-2 Forcing of SCS link transmission data

SCS link transmission data value setting

- Setting the value of locked data can be performed for each data item.
- Value setting is possible only for data whose wiring to the SCS link transmission function block is defined.
- A data status can be set for the receive data. However, this will be common for all data of the receiving station. The status cannot be changed for individual data item setting.

TIP

In the Output Disable status, data will not be sent even when the send data is locked and the data value is set. If the output enable operation is performed in the locked status, the set data will be sent.

Management of SCS link transmission lock status

- The SCS link transmission function manages not the number of locked data items, but the number of stations set by the local SCS as targets of link transmission lock.
- When the receive data from a target station is locked, it will be counted in the number of locked stations regardless of whether it is SCS or FCS.
- If the link transmission receive definition of a data from locked receiving station is changed from [Yes] to [No] in SCS Link Transmission Builder and downloaded to the SCS, the number of locked stations is decremented.
- The number of SCS link transmission lock target stations is displayed in the SCS operation status display of SCS maintenance support tool and HIS. It can also be referenced with application logic using a system function block.

System function block that manages locked status of SCS link transmission

- Using the system function block (SYS_FORCE_LT) in an application logic allows you to unlock all SCS link transmission data as well as to monitor elapsed time of locked status.
- The locked status of SCS link transmission data is managed separately from locked input/output modules or variables. Locking the SCS link transmission data does not affect the SYS_FORCE or SYS_FORCE_SC system function blocks.

Locked status notification by diagnostic information messages

The SCS link transmission function sends a diagnostic information message with lock/unlock operation. Checking the diagnostic information message allows you to see which station's data has been locked/unlocked.

Using forcing during SCS maintenance

When the SCS link transmission send data is affected by online change of the application, lock the local station before performing the online change download operation. This can prevent generation of false trips at the receiving side station. When the online change download is complete, confirm that the data to be sent is valid in the SCS Link Transmission Lock window, and then unlock the station.

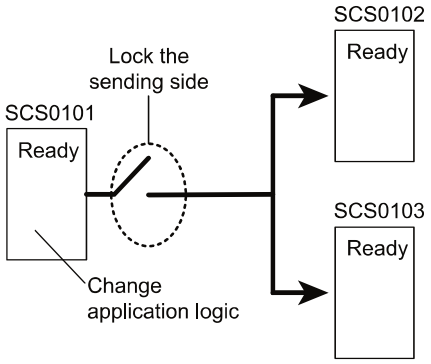


Figure F8.4-3 Locking SCS link transmission during online change

F8.5 Forcing of Inter-SCS safety communication

It is possible to force inter-SCS safety communication data from the Inter-SCS Communication Lock window of SENG. Inter-SCS safety communication data can be forced when the SCS security level is 1 or 0.

IMPORTANT

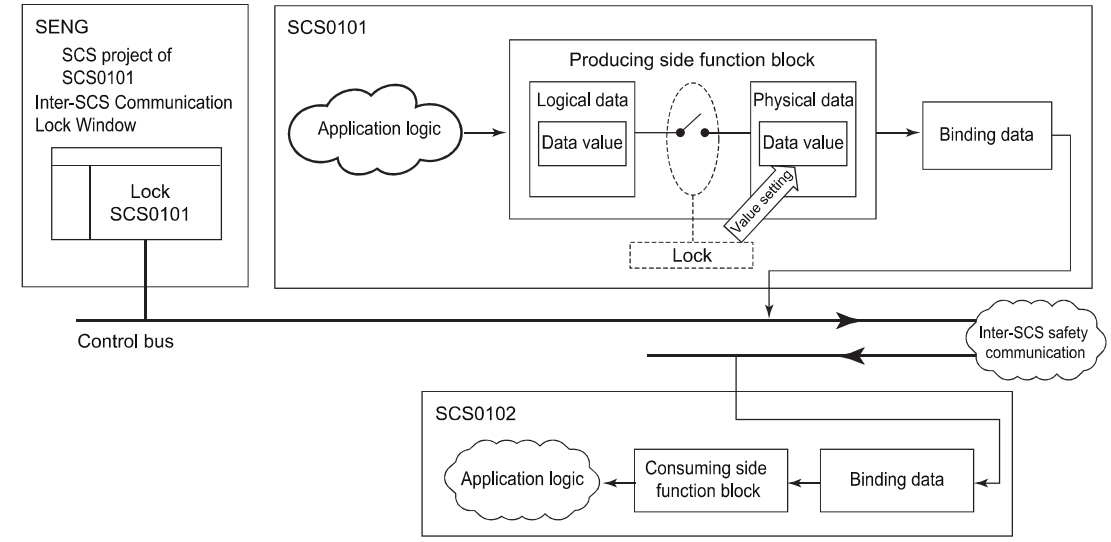
Forcing of inter-SCS safety communication data can be performed only from the Inter-SCS Communication Lock Window. Do not perform forcing operations (lock operation, referencing lock status, value setting) on function blocks related to inter-SCS safety communication from the Dictionary View. Performing lock operation from the Dictionary View causes a communication error.

Overview of forcing of Inter-SCS safety communication data

- Forcing of inter-SCS safety communication data can be performed only from the Inter-SCS Communication Lock Window.
- It is possible to force outputs from function blocks on the producing side and the consuming side of inter-SCS safety communication.
- By locking the local SCS, all the data to be sent by the local SCS is locked at the same time. It is not possible to lock specific receiving stations selectively.
- Data received by consumer inter-SCS safety communication function blocks of the local SCS can be locked collectively for the selected producing SCSs.
- Values can be set only for inter-SCS safety communication function blocks of locked stations. Data values can be set for the producer function blocks. For the consumer function blocks, data values and status can be set. Value settings can be performed for individual inter-SCS safety communication function blocks. In SCS simulation tests, it is possible to set values for multiple function blocks at the same time.

The overview of forcing of inter-SCS safety communication is shown below.

Example: Function blocks on the producing side



Example: Function blocks on the consuming side

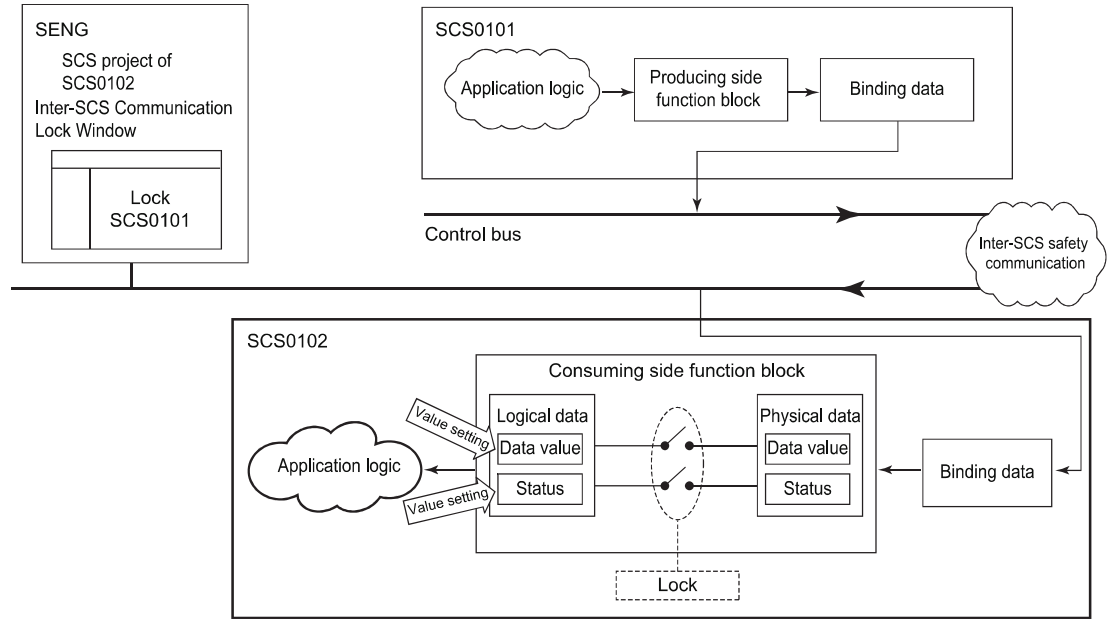


Figure F8.5-1 Overview of forcing of Inter-SCS safety communication

Locking and value setting on function blocks on the producing side

Select and lock the local SCS in the Inter-SCS Communication Lock Window to lock all function blocks on the producing side of the local SCS.

Locking function blocks on the producing side

If a function block on the producing side is locked, the value of the IN parameter is not written to PD (Physical Data), but written only to LD (Logical Data). The OUT parameter outputs the PD value. Thus, the value before locking is output to the binding variable while the function block is locked.

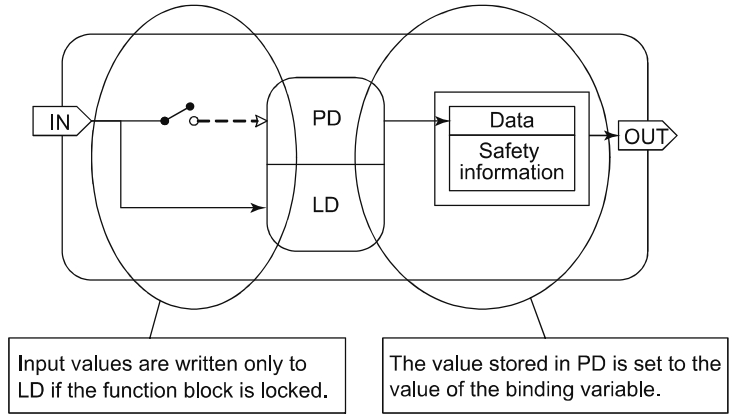


Figure F8.5-2 Locking function blocks on the producing side

● Value setting on function blocks on the producing side

If a value is written to a locked function block on the producing side from the Inter-SCS Communication Lock Window, the value of PD (Physical Data) of the function block on the producing side is overwritten with the specified value and output from the OUT parameter, which is then written to the binding variable. It is not possible to overwrite the data for guaranteeing the communication quality ("Safety information" in "Figure Locking Function Blocks on the Producing side") via value setting.

When the value setting succeeds, the diagnostic information message (No. 4185) is output, and you can check the values before and after the change.

■ Locking and value setting on function block on the consuming side

If you select and lock the SCS sending to the local SCS from the Inter-SCS Communication Lock Window, the consumer function blocks in the local SCS that correspond to the locked SCS are locked.

● Locking function blocks on the consuming side

If a function block on the consuming side is locked, the value of the IN parameter connected to the binding variable is not written to LD (Logical Data), but written to PD (Physical Data). The OUT and NR parameters output the LD value. Thus, the value before locking is output from the OUT and NR parameters while the function block is locked.

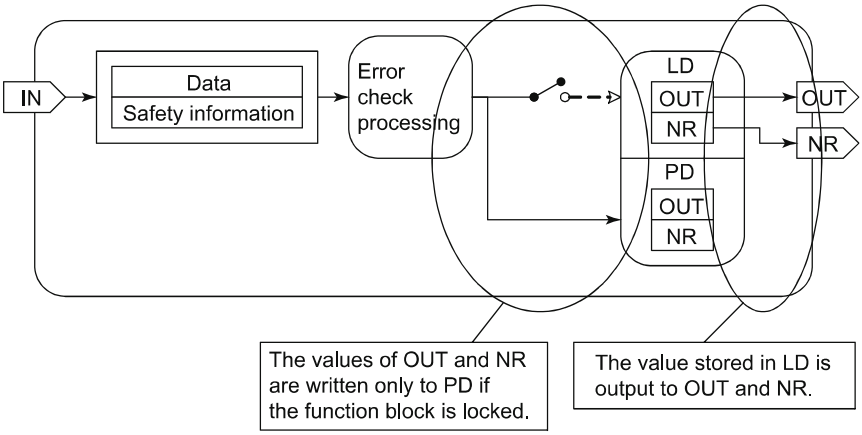


Figure F8.5-3 Locking function blocks on the consuming side

If a function block on the consuming side is locked, only the status of LD (Logical Data) is passed to the application logic that is connected to the function block on the consuming side. For this reason, if an error occurs on the communication path while the function block is locked, it is not possible to detect the error with the application logic. Note that errors on the

communication path detected by the function block on the consuming side are notified via diagnostic information messages even while the function block is locked. The error status is output correctly from CMER of the SYS_DIAG function block.

Value setting on function blocks on the consuming side

If a value is written to a locked function block on the consuming side from the Inter-SCS Communication Lock Window, the value of LD (Logical Data) of the function block on the consuming side is overwritten with the specified value and output from the OUT and NR parameters.

When the value setting succeeds, the diagnostic information message (No. 4185) is output, and you can check the values before and after the change.

F8.6 Forcing function for subsystem communication data

This section describes the Forcing function for subsystem communication data.

Overview

- You can use the Forcing function for subsystem communication data from the Communication I/O Lock Window. You cannot use the Forcing function from the Dictionary View and Multi Language Editor.
- You can use the Forcing function when the SCS security level is 1 or less.
- Communication with subsystems will continue even after subsystem communication data is locked.
- It is not possible to lock a given set of communication data. All data of a module or all input data or output data of a module will be locked simultaneously.
- Data status values are changed for each communication definition. Data values are changed for each communication data item.
- Forcing functions for subsystem communication data and the I/O variables are built upon different structures.
- Communication data of the SLSEVENT data type can be defined for communication modules that are used in connection with the ProSafe-SLS communication function, but such communication data constitute special data that is used for acquiring events and are not wired to the subsystem communication function blocks. Accordingly, communication data of the SLSEVENT data type are not displayed in the Communication Data List View and thus are not applicable to be locked or allowed their values to be set.
- If the communication module (model: ALR121) that is used for communication with ProSafe-SLS is locked, events are the only information that remains unlocked. All of the data, except for events, are locked.

Data flow under the forcing function

- Communication I/O data include logical data and physical data, just like I/O variables. Both logical data and physical data can be referenced from an SENG.
- When subsystem communication data is locked, the communication I/O data management function cuts off the flow of logical data and physical data. If communication input data is locked, inputs from subsystems will not reach the application logic. If communication output data is locked, outputs from the application logic will not reach subsystems.
- Values set in the communication input data through the Forcing function are input to the application logic, and values set to communication output data through the Forcing function are output to the subsystem.

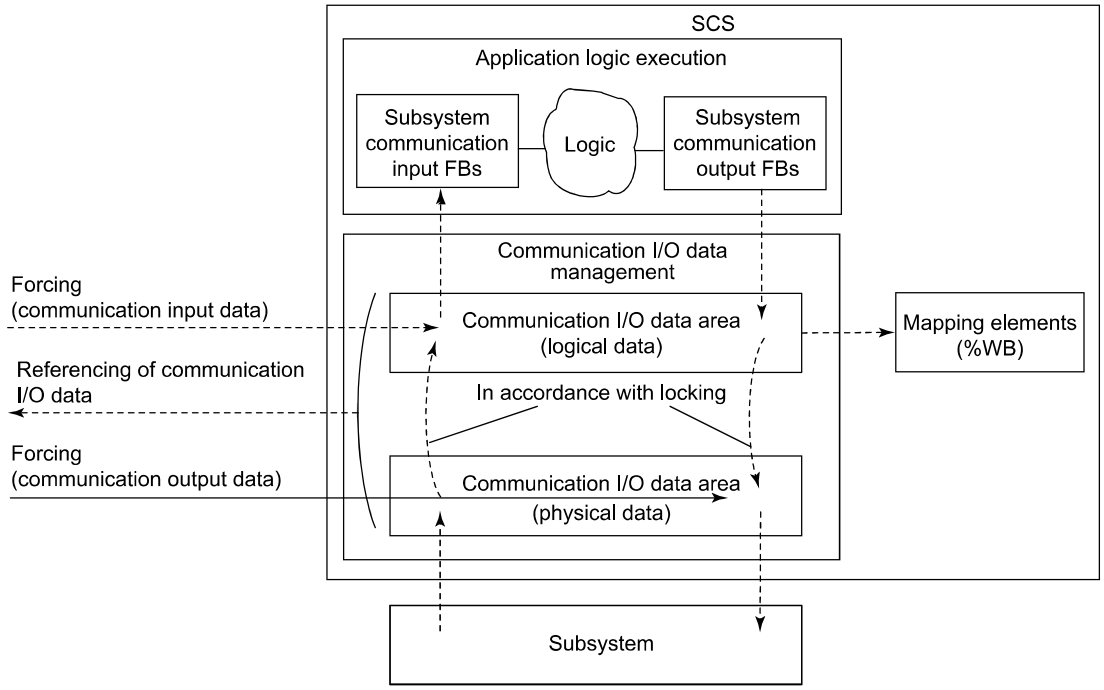


Figure F8.6-1 Communication I/O data management and forcing function

Locking subsystem communication data

Subsystem communication data can be locked or unlocked based on the following units: All subsystem communication data in each scope will be locked or unlocked.

Table F8.6-1 Subsystem communication data locking unit and range

Locking unit	Scope
All subsystem communication module inputs/outputs	All I/O data of a specified module
All subsystem communication module inputs	All input data of a specified module
All subsystem communication module outputs	All output data of a specified module

- Lock operation is performed in the Communication I/O Lock window.
- When the subsystem communication module is locked, refreshing of inputs to the application logic and outputs from the application logic will stop and the previous values will be retained.
- Locking and unlocking will both generate a diagnostic information message.
- All outputs of a module can be locked, even for a subsystem communication module for which no output communications have been defined. As long as subsystem communication outputs are locked before an online change download, output data will be locked even when output communication definitions are added, via the online change, to the module with no output communication definitions. The same applies to inputs.

SCS operations while subsystem communication data is locked

The following table shows how the SCS operates when subsystem communication data is locked.

Table F8.6-2 SCS operations while subsystem communication data is locked

What is locked	Subsystem communication I/O FBs	Subsystem communication
Subsystem communication inputs	The values immediately before locking are retained for data values and data statuses.	Communication is not affected.
Subsystem communication outputs	The values immediately before locking are retained for data statuses.	The values immediately before locking are used as the output values to subsystems.

Setting subsystem communication data values

- Set data values and status after subsystem communication data is locked. If subsystem communication data is not locked when data values and status are set, an error will occur.
- A data value can be set for each communication data item.
- A data status can be set for each communication definition. Changing a data status will affect all communication data in the same communication definition, so check the potential impact thoroughly before changing a data status.
- When a value is set, a diagnostic information message will be notified.

TIP

Communication data corresponds to the wired subsystem communication I/O FBs. Just like I/O variables, subsystem communication I/O FBs consist of data values and statuses. Unlike I/O variables, however, data statuses of subsystem communication I/O FBs indicate the statuses of communication with subsystems. "Communication definition" is a unit of communication between the subsystem communication module and a subsystem. A "communication definition" is a block of data of the same data type specified by the "Size," among the data included in the "Buffer" assigned to each communication module specified by the "Program Name" in the Communication I/O Builder.

Table F8.6-3 Setting subsystem communication data values

Setting target	Subsystem communication I/O FBs	Subsystem communication
Subsystem communication inputs	The values set in the Communication I/O Lock window are reflected in data values and statuses.	Communication is not affected.
Subsystem communication outputs	The data statuses set in the Communication I/O Lock window are output from subsystem communication output FBs.	The data values set in the Communication I/O Lock window are used as the output value to subsystems.

Management of subsystem communication data lock status

- By using the SYS_FORCE_SC function block, the lock status of subsystem communication data can be handled in the application logic.
- The SYS_FORCE_SC function block detects a lock timeout of subsystem communication data and forcibly unlocks subsystem communication data.
- Locking of subsystem communication data does not affect the lock management of I/O variables and internal variables. It does not affect the SYS_FORCE function block.
- Only whether or not subsystem communication data is locked is detected. The number of locks is not counted.

F8.7 Forcing function for safety subsystem communication data

Overview

You can force safety subsystem communication data in units of signals (individual integers, floating-point data).

You can use the Forcing function when the SCS security level is 1 or less.

Data flow under the forcing function

- Safety communication I/O data include logical data and physical data, just like I/O variables. Both logical data and physical data can be referenced from an SENG.
- When safety subsystem communication data is locked, the safety communication I/O data management function cuts off the flow of logical data and physical data. If safety communication input data is locked, inputs from subsystems will not reach the application logic.
- Values set in the safety communication input data through the Forcing function are input to the application logic.

Locking safety subsystem communication data

You can lock the data in units of communication definitions (PROFINET modules) or in units of IOM.

The module refers to the parameter name of PROFINET.

- Locking in units of communication definitions
  When locking or unlocking in units of communication definitions, the SCS alerts a system alarm to notify that the corresponding communication definition has been locked or unlocked.
- Locking in units of IOM
  When locking or unlocking in units of IOM, the SCS alerts a system alarm to notify that the corresponding IOM has been locked or unlocked.

Locking unit

You can lock or unlock data in units of S2LP131 or communication definitions. The following table shows the scope of locking or unlocking.

Table F8.7-1 Locking unit and scope of locking

Locking unit	Scope
S2LP131	All data of the specified S2LP131
Communication definition (*1)	All data of the specified communication definition (integer type, floating-point type)

*1: Up to 20 communication definitions can be locked and unlocked at one locking operation. If you try to lock or unlock more than 20 definitions at a time, an error occurs in the Communication I/O Lock Window and the lock or unlock operation is invalidated. Therefore, when there are more than 20 communication definitions to be locked or unlocked, repeat the lock or unlock operation for 20 or less definitions several times.

Behavior of safety subsystem communication I/O while locked

The following table shows the behavior of Safety communication and Non-Safety communication via safety subsystem communication I/O when safety subsystem communication data is locked.

Table F8.7-2 Behavior of safety subsystem communication I/O while locked

Type of communication	Behavior of FB	PROFINET communication with YFGW410	PROFIsafe communication with GS01
Safety communication	The values immediately before locking are retained for data values and data statuses.	Continued.	Continued.
Non-Safety communication	The values immediately before locking are retained for data values and data statuses.	Continued.	Not applicable

Precautions when performing an SCS online download

Lock S2LP131 prior to executing an SCS online download. Not locking can cause the following events to occur and lead to an unnecessary shutdown of the plant.

- The status of the logic data for Safety and Non-Safety data acquired via S2LP131 will be an error.
- When an existing communication definition number is changed, the locked status of the existing communication definition may change and become unlocked.

Locking behavior in relation to a communication definition added with an online download

When adding a communication definition to safety subsystem communication with an SCS online download, the locking status of the communication definition added with the online download will differ depending on the locking status of the S2LP131 to which the communication definition is added.

Table F8.7-3 Relationship between the locking status and a communication definition added with an online download

Locking status of S2LP131	Status of added communication definition	Behavior of FB
All inputs are locked, or all communication definitions are locked	Locked	The FB references the indefinite value of the locked logical data. By adding the FB after forcing the logical data, the forcibly set value is input to the FB.
Other than the above (not all inputs are locked, or some of the communication definitions are locked)	Unlocked	The initial value of the physical data is reflected onto the logical data and the FB references that logical data.

Setting values to safety subsystem communication data

The value for data and the data status can be set. When a value is set to an unlocked S2LP131 or communication definition, an error will occur.

- Alerting of alarm
  When a value is set, the SCS alerts a system alarm message.

  The status of a communication definition is common amongst identical communication definitions. For this reason, in the case of a communication definition that has multiple signals assigned, when the status of one signal is changed, the status of other signals are also changed. A system alarm indicating that a change has been made is alerted when the status is changed.
- Data subject to value setting
  The data value can be set in units of signals with both Safety and Non-Safety data. The subjects of value setting are integer data and floating-point data.

- Setting and reflection of the data status
  A value for the data status can be set for each communication definition with both Safety and Non-Safety data. Changes of the data status are reflected onto every data status having the same communication definition.

SEE ALSO For more information about safety subsystem communication data handling FB, refer to:

11.5, “SYS_FORCE_SF (safety subsystem communication I/O forcing status management)” in POU Reference Manual (IM 32P03B20-01EN)

Behavior of safety subsystem communication I/O after forcing

I/O behavior of safety subsystem communication after forcing differs depending on the type of communication. The following table shows the types of communication and FB behavior, PROFINET communication with YFGW410, and PROFIsafe communication with GS01.

Table F8.7-4 Behavior of safety subsystem communication I/O after forcing

Type of communication	Behavior of FB	PROFINET communication with YFGW410	PROFIsafe communication with GS01
Safety communication	The values set in the Communication I/O Lock window are reflected as data values and various statuses.	Continued.	Does not affect PROFIsafe communication.
Non-Safety communication	The values set in the Communication I/O Lock window are reflected as data values and data statuses.	Continued.	Not applicable

Management of safety subsystem communication data lock status

You can monitor the forcing status of S2LP131 by using the SYS_FORCE_SF function block. In addition, you can monitor the number of locks for safety subsystem communication definitions, detect exceeded locking status monitoring times, and force unlocking.

Locking of safety subsystem communication I/O does not affect the lock management of I/O variables, subsystem communication I/O data, and internal variables. It does not affect the SYS_FORCE function block and SYS_FORCE_SC function block.

F8.8 Windows used for forcing of I/O variables

Operations of forcing the input/output variables are mainly performed on the I/O Lock Window. You can perform the following operations on the I/O Lock Window.

- Locking and unlocking all channels of multiple AIO/DIO modules
  Lock all modules to prevent nuisance tripping caused by online modifications after the completion of input/output wiring, or to perform maintenance of AIO/DIO modules including replacement .
- Locking and unlocking one input/output channel
  Perform this operation to conduct wiring tests.
- Setting variable values

In addition to the I/O Lock Window, you can also perform forcing operations for the indicated variables and parameters from the following windows:

- Dictionary View
  - All variables including internal variables
  - Parameters in some of function blocks
- Multi-Language Editor
  - Variables used in FBD, LD and ST (if Spy List window is open)
  - Parameters in the User-Defined function blocks

Furthermore, in debug mode and in logic simulation mode, a Spy List window will be shown at the lower part of SCS Manager and Multi-Language Editor, where the following forcing operation can be performed.

- Forcing the variables used in FBD, LD and ST.

A variable locked in a certain window can be unlocked in another window. Similarly, a variable locked in an SENG can be unlocked in another SENG at a different time. However, if you want to unlock variables in Multi-Language Editor, open the Spy List window. You can unlock a variable only when physical value and logical value of the variable are indicated.

SEE ALSO

For more information about Dictionary View, refer to:

"Dictionary View" in "Workbench" in the Workbench User's Guide

For more information about Multi-Language Editor, refer to:

"Multi-Language Editor" in "Workbench," "Language Editor" in the Workbench User's Guide.

Spy List window

In debug mode and in logic simulation mode, a Spy List window will be shown at the lower part of SCS Manager and Multi-Language Editor. On the Spy List window, locking statuses of variables, values of logical and physical data are displayed. After opening the variable dialog box from the Spy List window, the values of the variables used in FBD, LD and ST can be set.

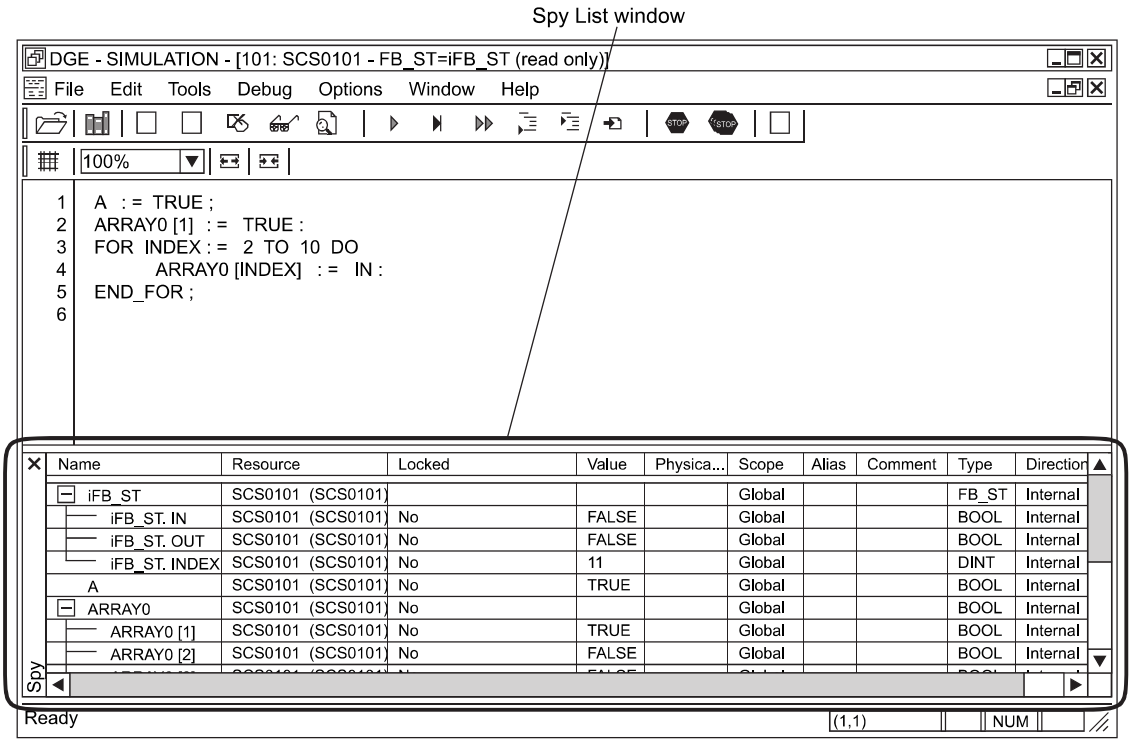


Figure F8.8-1 Spy List window

If you select a function block parameter using Multi-Language Editor, all the parameters for the function block instances that contain the selected parameter will be displayed in the Spy List window. In Multi-Language Editor, when you select a global variable or a local variable, the variable is displayed in the Spy List window. When you are using a global array variable or a local array variable, if one array element is selected (such as ARRAY0[1] in the previous figure), all the elements of the array appear in the Spy List window.

When debugging an ST in Multi-Language Editor, follow these steps to add a variable to the Spy List window.

1. Click [INDEX] in the previous figure.
   All of the parameters for the function block instance that contains that parameter are displayed in the Spy List window.
2. Click the global variable or local variable (such as A in the previous figure).
   The variable is displayed in the Spy List window.

When debugging an FBD/LD in Multi-Language Editor, follow these steps to add a variable to the Spy List window.

1. In the FBD/LD, click the variable.
2. You can run any of the following commands.
   - Right-click and select [Spy Selection] on the displayed menu.
   - On the [Debug] menu, select [Spy Selection].
   - Click the [Spy Selection] tool button.

   The variable is displayed in the Spy List window.

If you want to display only the variables of particular POUs in the Spy List window, you can save the relevant set of variables to a file and display them by reading from that file; thus you can display particular sets of variables by switching between the saved files.

IMPORTANT

It is important that you do not operate the variable of another scope accidentally because multiple variables in different scopes may have the identical name.

The Spy List window may be restarted with previously displayed state. The action is as follows:

- If the debug mode or the logic simulation mode is terminated while the Spy List window is opened, the Spy List window will restart right after the debug mode or the logic simulation mode restarts.
- Under the debug mode or the logic simulation mode, if the Multi-Language Editor is terminated while the Spy List window is opened, the Spy List window will restart after the Multi-Language Editor restarts.
- When starting the Spy List window, it will display the previously displayed variables. When switching SCS projects, the previously displayed variables of that project will be displayed on the Spy List window.

Value setting can be performed in the Value setting dialog box in the same way as in Dictionary View.

SEE ALSO

For more information about Spy List operating procedures, refer to:

"Spying Variables" in "Debug/Simulate" in "Debug" in the Workbench User's Guide

For more information about Dictionary View operations, refer to:

"Write/Lock/Unlock" in "Debug/Simulate" in "Workbench," "Debug" in the Workbench User's Guide

F8.8.1 I/O Lock window

In the I/O Lock Window, you can perform locking and unlocking operations for individual input/output modules and/or input/output channels (input/output variables). Also you can set values to Input/Output variables. The I/O Lock Window allows operation on AIO/DIO modules. In this section, "input/output modules" refers to AIO/DIO modules.

In SCS Simulator of SCS Test Functions, multiple I/O variables can be set all together. Therefore, the initial values of all channels of I/O modules and the testing patterns can be set all together.

How to call up the I/O Lock window

1. Check if the SCS security level is 0 or 1 using the SCS security level operation function.
2. Put the SCS Manager into Debug mode or Editing mode.
   To change to Debug mode, choose [Debug] from [Debug] menu or click [Debug] button on the toolbar.
3. Select [Maintenance] from the [Tools] menu of SCS Manager.
   The Maintenance Launcher menu appears.
4. Select [I/O Lock Window] from the Maintenance Launcher menu.
   The I/O Lock Window appears.

IMPORTANT

- It is not possible to start multiple I/O Lock Windows at the same time, for neither the same SCS project nor different SCS projects.
- The I/O Lock Window cannot be called up while Build or Download is running.
- If you try to execute online change downloading, offline downloading, master offline downloading, or restarting of SCS while the I/O Lock Window is open, an error message is displayed and the downloading or restarting will not be executed.

How to exit the I/O Lock window

To exit the I/O Lock Window, choose [Exit] from [File] menu.

IMPORTANT

- When exiting the I/O Lock Window, if a locked variable exists, a dialog box will be displayed for confirmation. It is necessary to open the I/O Lock Window to unlock the locked variables.
- If the SCS Manager is closed or a different SCS project is opened, the I/O Lock Window will be forcibly closed.

I/O Lock window structure

The I/O Lock Window contains the following components.

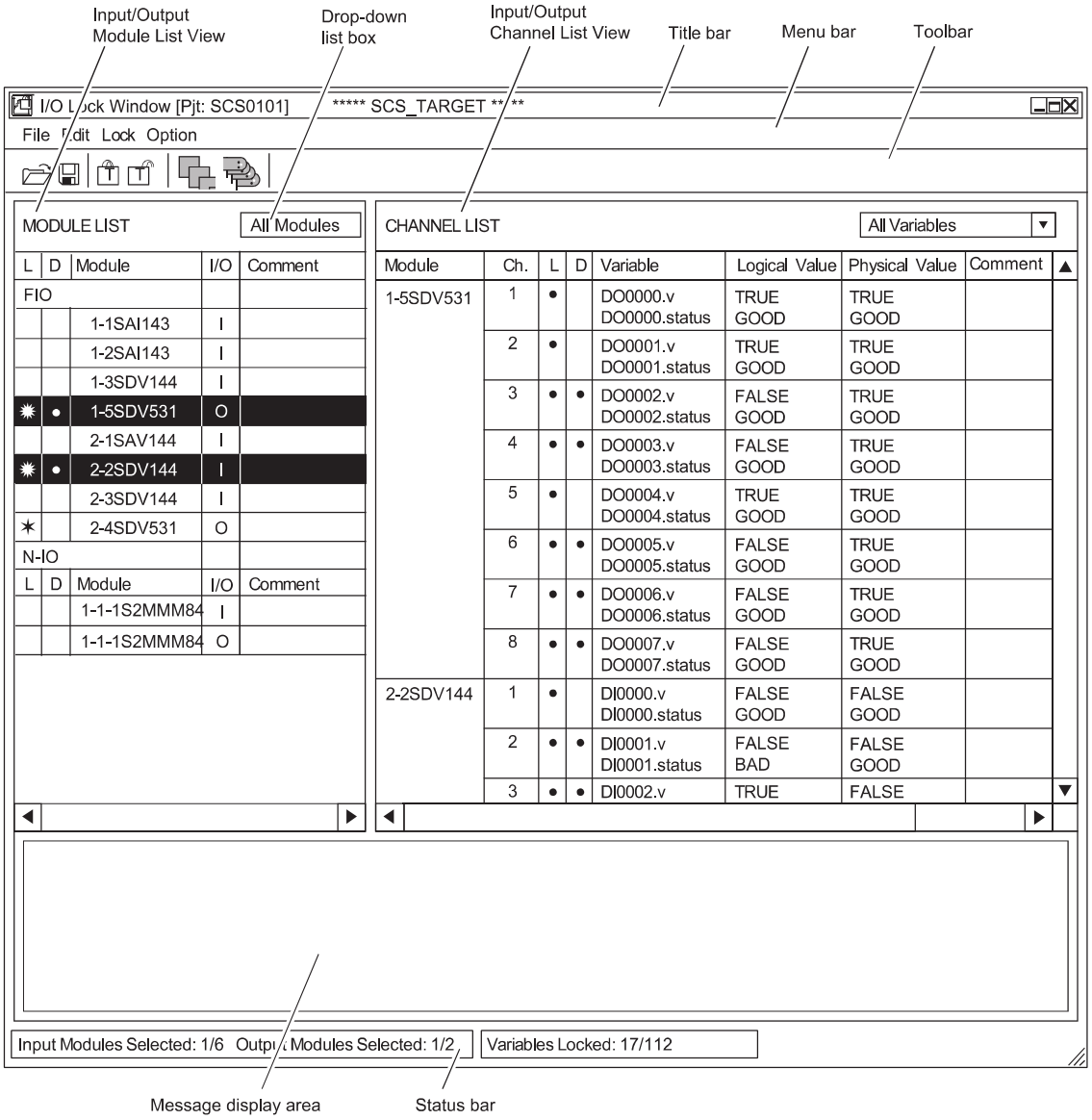


Figure F8.8.1-1 I/O Lock window

The components in the window are explained next.

Title bar

On the title bar, besides window name and project name, the SCS status is also displayed.

- SCS_TARGET: Indicates communication with the SCS.
- SCS_SIMULATOR: Indicates communication with the SCS simulator.
- <Non>: Indicates the SCS is not running.

For logic simulation test, "SIMULATION" will be displayed in the position of SCS status.

Menu bar

The following menus are provided on the menu bar:

- [File] Menu
- [Edit] Menu

- [Lock] Menu
- [Option] Menu

The menu items provided on each menu are explained as follows.

Table F8.8.1-1 File menu

Menu item	Description
Import Values...(*1)	Imports the values of the I/O variables from a file for setting all together.
Export Values...(*1)	Exports the values of the I/O variables to a file for setting all together.
Exit	Exits from the I/O Lock Window.

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Table F8.8.1-2 Edit menu

Menu item	Description
Cut (*1)	Deletes the selected character string and copies it onto the clipboard.
Copy (*1)	Copies the selected character string onto the clipboard.
Paste (*1)	Inserts the character string stored in the clipboard.
Delete (*1)	Deletes the selected character string.
Select All	Selects all displayed modules (same action as pressing the [Ctrl] key and [A] key together).

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Table F8.8.1-3 Lock menu

Menu item	Description
Lock Modules	Locks all modules selected.
Unlock Modules	Unlocks all modules selected.
Set Values (*1)	Sets multiple I/O variables together.

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Table F8.8.1-4 Option menu

Menu item			Description
Numerical Display	REAL	1.234E+12	Exponential notation
		12.34567	Displays 5 decimal places.
		123.4567	Displays 4 decimal places.
		1234.567	Displays 3 decimal places.
		12345.67	Displays 2 decimal places.
		123456.7	Displays 1 decimal places.
Data Acquiring Mode	All Modules		Changes data acquiring mode to "All Modules" mode.
	Selected Modules		Changes data acquiring mode to "Selected Modules" mode.

Toolbar

The following buttons are provided on the toolbar.

Table F8.8.1-5 Toolbar buttons

Button	Description
(*1)	Imports the values of the I/O variables from a file for setting together. (Same action as [Import Values] on the [File] menu.)
(*1)	Exports the values of the I/O variables to a file for setting all together. (Same action as [Export Values] on the [File] menu.)
	Locks all modules selected (same action as [Lock Modules] on the [Lock] menu).
	Unlocks all modules selected (same action as [Unlock Modules] on the [Lock] menu).
(*1)	Sets multiple I/O variables together (same action as [Set Values] on the [Lock] menu).
(All Modules) (Selected Modules)	Same action as the [Data Acquiring Mode] task on [Option] menu. Toggles between [All Modules] mode and [Selected Modules] mode.

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Data acquisition modes

When getting data values and data statuses of channels from SCS, the acquisition mode can be selected.

- ALL Modules Mode
  Sequentially retrieves the data values and data statuses from all channels of the input/output modules defined in the SCS project.
- Selected Modules Mode
  Sequentially retrieves the data values and data statuses of channels from the I/O modules selected on the I/O Module List View.

  The text of "Updating Selected Modules" is displayed on the I/O Module List View and on the I/O Channel List View.

I/O Module List view

This view displays a list of input/output modules that are defined in the currently open SCS project. The following modules, which do not have any input/output channels, are not displayed.

- ESB bus coupler module (SEC402, SEC401, L1EC402, L1EC401)
- Serial communication module (ALR111, ALR121)
- Ethernet communication module (ALE111)
- N-ESB bus coupler module (S2EN402, S2EN404)

If an input/output module is in dual-redundant configuration, only the module allocated to the odd slot is displayed regardless of which module is operating.

The following table lists the items displayed in the I/O Module List View.

Table F8.8.1-6 Items displayed in the I/O Module List view

Item name	Display
L	Shows locking status of an input/output module
D	Shows consistency or inconsistency of the logical data and physical data of channels of an input/output module
Module	The I/O module name ("node number - slot number" for an FIO and "node number - unit number - slot number" for an N-IO) will be added to the beginning.

Continues on the next page

Table F8.8.1-6 Items displayed in the I/O Module List view (Table continued)

Item name	Display
I/O	Signal direction of an I/O module ("I" for input and "O" for output. In the case of a universal-type module, when both the input channel and the output channel can be configured, module names having the same node number, unit number, and slot number is displayed in two rows together with an "I" for input and an "O" for output.)
Comment	Comments entered for an input/output module

Lock status of Input/Output modules

Displays the locking statuses of the channels according to I/O modules.

Table F8.8.1-7 Display of lock status

Display	Meaning
(No symbol)	No channel is locked.
✶ (yellow)	Some channels are locked.
✹ (red)	All channels are locked.
? (black)	Unable to communicate with SCS.

Data consistency or inconsistency of Input/Output module channels

Data of digital inputs/outputs is considered to be inconsistent if the values of the logical data and physical data of the data value or data status are not same.

Data of analog inputs/outputs is considered to be inconsistent if the logical data status and the physical data status are not same.

Table F8.8.1-8 Consistency and inconsistency

Display	Meaning
(No symbol)	All channels are consistent.
● (yellow)	Some channels are inconsistent.
⦿ (red)	All channels are inconsistent.
? (black)	Unable to communicate with SCS.

The action for updating the display of the consistency and inconsistency of the input/output module data varies with data acquisition mode.

- ALL Modules Mode
  Sequentially gets the data values and data statuses of all channels from all the input/output modules defined in the SCS project and update them in the up-down order as their displays.
- Selected Modules Mode
  Sequentially gets the data values and data statuses of channels from the input/output modules selected on I/O Module List View and update them in the up-down order as their displays. The statuses of the unselected modules are indicated with (?) in "D" column.

Filtering

It is possible to filter and display input/output modules using a drop-down list box.

Table F8.8.1-9 Drop-down list box of the I/O Module List view

Menu item	Operation
All Modules	Both input modules and output modules are shown.

Continues on the next page

Table F8.8.1-9 Drop-down list box of the I/O Module List view (Table continued)

Menu item	Operation
Input Modules	Only input modules are shown.
Output Modules	Only output modules are shown.

Pop-up menu

Click the right mouse button on the I/O Module List View to display the pop-up menu.

The menu item in the pop-up menu is shown as follows.

Table F8.8.1-10 Pop-up menu of the I/O Module List view

Menu item	Description
Select All	Selects all displayed modules (same function as pressing the [Ctrl] key and [A] key together).

I/O Channel List view

This view displays information of each channel for input/output modules selected in the I/O Module List View. Channels to which no variable is assigned are not shown in the I/O Channel List View. If multiple channels of S2MMM843 are bundled for a high current output of DO, only the channel with the smallest channel number is displayed.

Table F8.8.1-11 Items displayed in the I/O Channel List view

Item name	Display
Module	Name of an input/output module
Ch.	Channel number (1 to 8, or 1 to 16)
L	Channel lock status
D	Channel data consistency or inconsistency
Variable	Name of an input/output variable that is wired (data value, data status)
Logical Value	Logical data of data value and data status, respectively
Physical Value	Physical data of data value and data status, respectively
Set Value (*1)	Set value of data value and data status, respectively
Comment	Comment entered for the input/output variable

*1: Displayed and editable only when the SCS project target name is SCS_SIMULATOR.

Channel lock status

Displays channel locking status.

Table F8.8.1-12 Display of lock status

Display	Meaning
(No symbol)	The channel is unlocked.
✶ (red)	The channel is locked.
? (black)	Unable to communicate with SCS.

Data consistency or inconsistency of channel

Data of digital inputs/outputs is considered to be inconsistent if the values of the logical data and physical data of the data value or data status are not same.

Data of analog inputs/outputs is considered to be inconsistent if the logical data status and the physical data status are not same.

Table F8.8.1-13 Consistency and inconsistency

Display	Meaning
(No symbol)	Data is consistent.
● (red)	Data is inconsistent.
? (black)	Unable to communicate with SCS.

Logical data and physical data

A BOOL-type data value is displayed as either [TRUE] or [FALSE]. A REAL-type data value is displayed using the display format selected from the [Option] menu.

Data status is displayed as either [GOOD] or [BAD]. If the data status is BAD, the background color is displayed in yellow. [******] is displayed if communication with SCS is disabled.

REAL-type data is displayed along with the engineering unit symbol. The displayed engineering unit symbol depends on the module type and the settings specified in I/O Parameter Builder. At this time, if the unit is %, the value is normalized to 0 to 100%. For other units, the data is the physical quantity.

Updating displays of logical data, physical data and Match/Mismatch of channel data

The action for updating the displays of the matching and mismatching of the channels as well as the logical data and physical data varies with the data acquisition mode.

- ALL Modules Mode
  Sequentially retrieves the data values and data statuses of all channels from all the input/output modules defined in the SCS project. The displays will be updated right after the data acquisition for the channels displayed in the I/O Channel List View is completed.
- Selected Modules Mode
  Sequentially retrieves the data values and data statuses of channels from the input/output modules selected in the I/O Module List View. The displays will be updated right after the data acquisition for the channels displayed in the I/O Channel List View is completed.

Filtering

It is possible to filter the input/output channels to be displayed using a drop-down list box.

Table F8.8.1-14 Drop-down list box of the I/O Channel List view

Item	Operation
All Variables	Information about all channels wired to input/output variables for input/output modules selected in the I/O Module List View is displayed.
Locked Variables	Information about all locked channels wired to input/output variables for input/output modules selected in the I/O Module List View is displayed.
Unlocked Variables	Information about all unlocked channels wired to input/output variables for input/output modules selected in the I/O Module List View is displayed.

Pop-up menu

Only when the SCS project target name is SCS_SIMULATOR, click the right mouse button on the I/O Channel List View to display a pop-up menu.

The items on the pop-up menu are as follows:

Table F8.8.1-15 Items on pop-up menu in the I/O Channel List view

Items	Description
Cut	Same as the [Cut] command on the [Edit] menu.

Continues on the next page

Table F8.8.1-15 Items on pop-up menu in the I/O Channel List view (Table continued)

Items		Description
Copy		Same as the [Copy] command on the [Edit] menu.
Paste		Same as the [Paste] command on the [Edit] menu.
Delete		Same as the [Delete] command on the [Edit] menu.
Select All		Same as the [Select All] command on the [Edit] menu.
Input Values ►	Set .v=TRUE	Sets the data of Set Value to TRUE.
	Set .v=FALSE	Sets the data of Set Value to FALSE.
	Clear .v	Clears the data of Set Value.
	Set .status=GOOD	Sets the data status of Set Value to GOOD.
	Set .status=BAD	Sets the data status of Set Value to BAD.
	Clear .status	Clears the data status of Set Value.

Message display area

The results of locking, unlocking and setting operations are displayed as messages. The last displayed message is cleared at each operation.

Status bar

The status bar shows the following information about the input/output modules displayed in the I/O Module List View.

- Input Modules Selected: Number of selected input modules/Number of all input modules
- Output Modules Selected: Number of selected output modules/Number of all output modules
- Variables Locked: Number of locked input/output variables/Number of all input/output variables

F8.8.2 Locking and unlocking all variables of I/O module

On I/O Lock Window, all I/O variables of an I/O module can be locked and unlocked together. This section explains the operating procedures.

Selection of Input/Output modules

You can select any number of input/output modules in the I/O Module List View.

- Select [All Modules] in the drop-down list box to display all input/output modules.
- Select [Input Modules] in the drop-down list box to display all input modules. Universal-type modules for which an input channel is defined are also displayed.
- Select [Output Modules] in the drop-down list box to display all output modules. Universal-type modules for which an output channel is defined are also displayed.

The following operation displays the information of channels in I/O Channel List View.

- Click an input/output module name, the information regarding the channels of the module at the clicked line is displayed.
- To select an input/output module, click the name of the first module and then click the name of the last module while holding down the [Shift] key on the keyboard. The information regarding the channels of the selected modules is displayed.
- Click an input/output module while pressing the [Ctrl] key, the information regarding the channels of the module at the clicked line is added to the current displays.
- Selecting [Select All] from the pop-up menu in I/O Module List View displays the information of channels for all I/O modules that are displayed in I/O Module List View.

Locking all Input/Output modules

With this operation, you can lock all input/output variables wired to each channel of the selected input/output modules in a batch.
If some of the input/output variables of the selected input/output modules have already been locked, they will be kept locked even if you lock all modules.

The procedure is as follows:

1. Select the input/output modules you want to lock in a batch in the I/O Module List View.
2. Check the differences between the data value and data status of the logical data and physical data of each channel of the selected input/output modules in the I/O Channel List View to confirm that locking will not cause any problem.
3. Select [Lock Modules] on the [Lock] menu. Alternatively, click the [Lock] button on the toolbar.
   The confirmation dialog box appears. Click the [OK] button to perform a lock operation. All selected input/output modules are locked.

   Click the [Cancel] button to cancel the operation.

Unlocking all Input/Output modules

Using this operation, you can unlock all I/O variables wired to each channel of the selected I/O modules in a batch.
If the selected I/O modules contain some unlocked I/O variables, those variables will be kept unlocked even if you unlock all modules.

The procedure is as follows:

1. Select the input/output modules you want to unlock in a batch in the I/O Module List View.

2. Check the differences between the data value and data status of the logical data and physical data of each channel of the selected input/output modules in the I/O Channel List View to confirm that unlocking will not cause any problem.
3. Select [Unlock Modules] on the [Lock] menu. Or click the [Unlock] button on the toolbar.
4. When a confirmation dialog box is displayed, click [OK] so as to unlock all the communication data of the selected station. Clicking [Cancel] will cancel the unlocking.
5. If there are discrepancies between the logical data and physical data of any of the channels of the input/output modules to be unlocked, the dialog box for reconfirmation appears. Click the [OK] button to perform the unlock operation. All selected input/output modules are unlocked.
   Click the [Cancel] button if you want to cancel the operation.

F8.8.3 Set I/O variables of I/O modules

On I/O Lock Window, the I/O variables can be set one by one or can be set all together per I/O module. In SCS Simulator of SCS Test Functions, it is possible to set multiple I/O variables together per I/O module.

This section explains the operating procedures.

Setting each variable value

For each variable, the data value and data status can be set.

IMPORTANT

Setting values to variables cannot be executed while Build or Download is running.

In the I/O Channel List View, double-click anywhere between the channel field and the physical data field on a certain row to open the Write STATUS dialog box for the data value or data status of the I/O variable at the row.

When you open the Variables dialog box, the logical data and physical data default values are displayed. Either logical data or physical data is displayed, depending on whether the input/output variables are locked or unlocked. When displaying data values, the engineering unit symbols are displayed at the end of the data values for REAL variables. At this time, if the unit is %, the value is normalized to 0 to 100%. For other units, the data is the physical quantity.

- For BOOL Data
  When the dialog box is opened, the logical data or the physical data will be displayed with either [TRUE] or [FALSE] button pressed.
- For Data Status
  When the dialog box is opened, the logical data will be displayed with either [GOOD] or [BAD] data status button pressed.

The following table shows whether logical or physical data are displayed for the initial value of the selected I/O variable, data and data status respectively.

Table F8.8.3-1 Initial values on Write STATUS dialog box

Data Value (.v) and Data Status (.status)	Locked	Unlocked
Input Variable Data Value (.v)	Logical	Logical
Input Variable Data Status (.status)	Logical	Logical
Output Variable Data Value (.v)	Physical	Logical
Output Variable Data Status (.status)	Logical	Logical

The above can be set on the Write STATUS dialog box.

SEE ALSO For more information about procedure for setting values using the variables dialog box, refer to:

"Write/Lock/Unlock" in "Debug/Simulate" in "Workbench," "Debug" in the Workbench User's Guide

Set multiple I/O variables together

Using the SCS Simulator, you can set multiple I/O variables together.

The following operations can be performed on the locked I/O variables among the I/O variables wired to the I/O channels of the selected I/O modules.

- Set values to I/O variables.

- Save the set values for the I/O variables in a file.
- Read values from a file and set them to I/O variables.

Note that the number of I/O variables set at a time should be 700 or less. If more variables are set at a time, some of the system alarm messages informing the data setting or data status setting may not be transmitted.

Enter the values to be set to I/O variables

The value of a variable can be entered to the "Set Value" item on I/O Channel List View.

The value can be entered by any of the following operations. After entering the values, you need to set all the values to the I/O variables.

- Enter a Value Directly
  On I/O Channel List View, click Set Value item on the row of the channel that you want to enter the value for. By clicking the data value or data status, they can be entered directly.

  For BOOL type data, each click will move among TRUE, FALSE and a space (non specified) for selections.
- Edit Values for Channels
  From [Edit] menu or from the pop-up menu after a right click, you can use [Cut], [Copy], [Paste] and [Del] commands to edit the "Set Value" items of multiple channels.
- Enter a value by clicking [Input Values] on the pop-up menu
  Right clicking on the I/O Channel List View, a pop-up menu will be displayed. Using [Input Values] on the pop-up menu, the data values and data status for "Set Value" items can be set.

  For example, if you want to set data status of all channels to BAD, you can use [Select All] command on the pop-up menu to select "Set Value" items of all channels, and then you can choose [Set.STS=BAD] of the [Input Values] from the pop-up menu.

Set the values to multiple I/O variables

For the selected I/O modules, the locked I/O variables among the wired I/O variables can be set all together to the values defined in the "Set Value" items on the I/O Channel List View.

IMPORTANT

Setting values to variables cannot be executed while Build or Download is running.

The procedure is as follows:

1. On I/O Module List View, choose a module that you want to set values for.
2. Choose [Set Values] from the [Lock] menu or click [Set Values] button on the toolbar so as to display Set Values dialog box.
3. Click [OK] to set values. The values are set to all the wired and locked I/O variables. You can cancel the setting by clicking [Cancel].

Export the setting values to a file

The values for "Set Value" items of the I/O variables can be exported to a file.
The procedure is as follows:

1. Choose [Export Values] from the [File] menu, or click the [Export Values] button on the toolbar so as to display a dialog box for selecting files.
2. Specify a CSV file name and then click [Save]. The data values and data statuses for the channels assigned with the variables of the I/O modules on the I/O Module List View will be exported.

IMPORTANT

Do not edit the exported file if you want to import the file later.

Import the setting values from a file

The values for "Set Value" items of the I/O variables can be imported from a file.

IMPORTANT

Do not import any file other than the file exported from I/O Lock Window.

The procedure is as follows:

1. Choose [Import Values] from the [File] menu, or click the [Import Values] button on the toolbar so as to display a dialog box for selecting files.
2. Choose the CSV file that contains the setting values and then click [Open]. The channels assigned with the variables of the I/O modules on the I/O Module List View will be displayed with the imported data values and data statuses.

F8.9 SCS Link Transmission Lock window

On SCS Link Transmission Lock Window, the communication data of SCS Link transmission can be locked or unlocked. Also you can set values to SCS Link transmission data.

In SCS Simulator of SCS Test Functions, it is possible to set values to multiple communication data together. Therefore, the initial values of communication data and testing patterns can be defined all together.

How to call up the SCS Link Transmission Lock window

1. Check if the SCS security level is 0 or 1 using the SCS security level operation function.
2. Put the SCS Manager into Debug mode or Editing mode. To change to Debug mode, choose [Debug] from [Debug] menu or click [Debug] button on the toolbar.
3. Select [Maintenance] from the [Tools] menu of SCS Manager.
   The Maintenance Launcher menu appears.
4. Select [SCS Link Transmission Lock Window] from the Maintenance Launcher menu.
   The SCS Link Transmission Lock Window appears.

IMPORTANT

- It is not possible to start multiple SCS Link Transmission Lock Windows at the same time, for neither the same SCS project nor different SCS projects.
- The SCS Link Transmission Lock Window cannot be called while Build or Download is running.

SEE ALSO For more information about functions for operating SCS security levels, refer to:

B3., “Security of SCS” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

How to exit the SCS Link Transmission Lock window

To exit the SCS Link Transmission Lock Window, choose [Exit] from [File] menu.

IMPORTANT

- When exiting the SCS Link Transmission Lock Window, if the locked variables exist, a dialog box will be displayed for confirmation. It is necessary to reopen the SCS Link Transmission Lock Window to unlock the locked variables.
- If the online change download is performed and completed while the SCS Link Transmission Lock Window is not closed, an error of database inconsistency may occur. Under this circumstance, a message for restarting SCS Link Transmission Lock Window will be displayed. You need to follow the message to restart it.
- If the SCS Manager is closed or a different SCS project is opened, the SCS Link Transmission Lock Window will be forcibly closed.

SCS Link Transmission Lock window structure

The SCS Link Transmission Lock Window contains the following components.

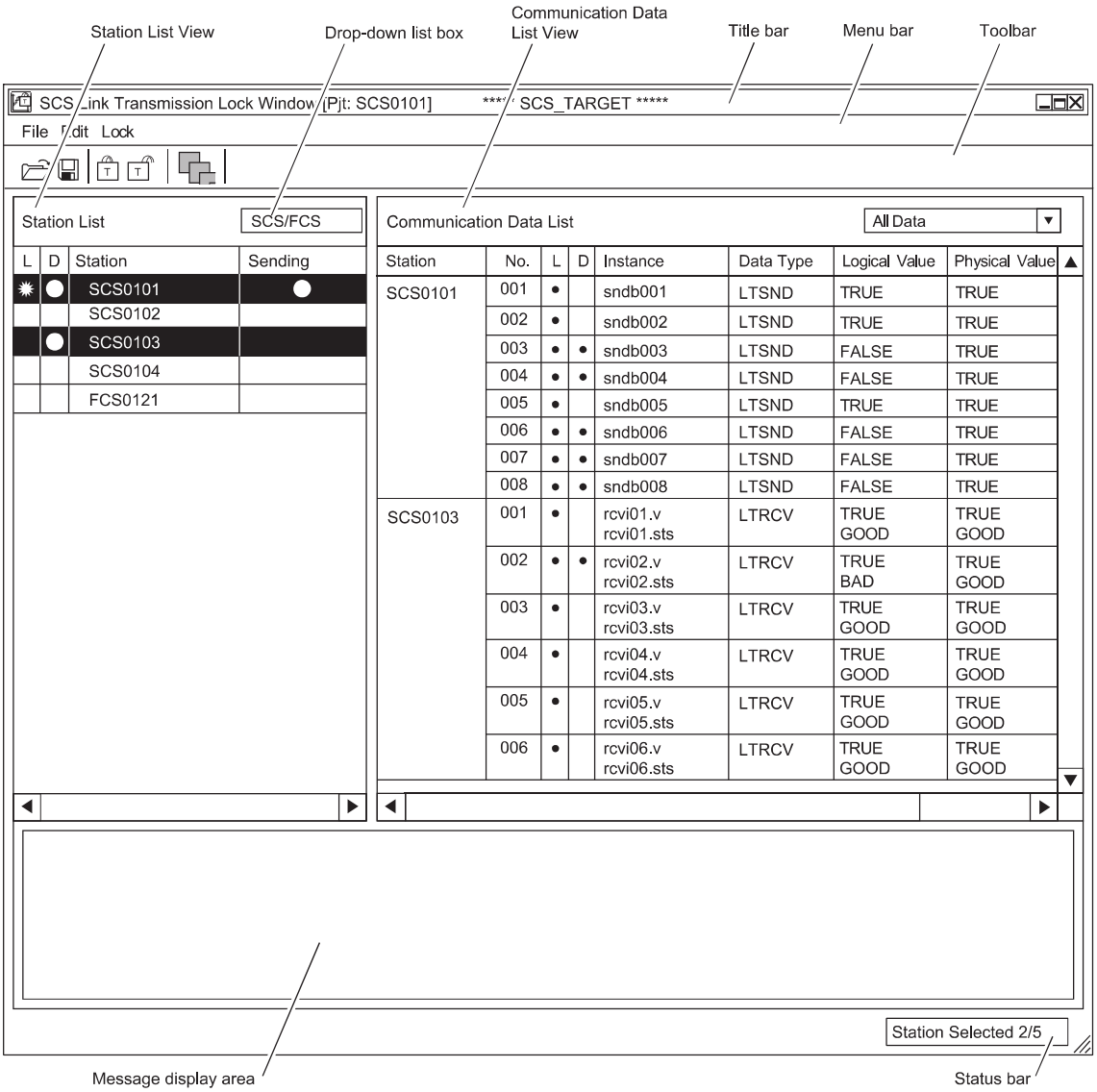


Figure F8.9-1 SCS Link Transmission Lock window

Title bar

On the title bar, besides window name and project name, the SCS status is also displayed.

- SCS_TARGET: Indicates communication with the SCS.
- SCS_SIMULATOR: Indicates communication with the SCS simulator.
- <Non>: Indicates the SCS is not running.

For logic simulation test, "SIMULATION" will be displayed in the position of SCS status.

Menu bar

The following menus are provided on the menu bar:

- [File] Menu
- [Edit] Menu
- [Lock] Menu

The menu items provided on each menu are explained as follows.

Table F8.9-1 File menu

Menu item	Description
Import Values...(*1)	Imports from a file the values that are used to set communication data.
Export Values... (*1)	Exports to a file the values that were used to set communication data.
Exit	Exits from the SCS Link Transmission Lock Window.

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Table F8.9-2 Edit menu

Menu item	Description
Cut (*1)	Deletes the selected character string and copies it onto the clipboard.
Copy (*1)	Copies the selected character string onto the clipboard.
Paste (*1)	Inserts the character string stored in the clipboard.
Delete (*1)	Deletes the selected character string.
Select All	Selects all displayed modules (same action as pressing the [Ctrl] key and [A] key together).

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Table F8.9-3 Lock menu

Menu item	Description
Lock Communication Data	Locks communication data of a station.
Unlock Communication Data	Unlocks communication data of a station.
Set Values (*1)	Collectively sets values of communication data.

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Toolbar

The following buttons are provided on the toolbar.

Table F8.9-4 Toolbar buttons

Button	Description
 (*1)	Imports from a file the values that are used to set communication data. This is the same as selecting [File] - [Import Values] from the menu bar.
 (*1)	Exports to a file the values that were used to set communication data. This is the same as selecting [File] - [Export Values] from the menu bar.
	Locks all communication data of a station. Same as choosing [Lock Communication Data] from [Lock] menu.
	Unlocks all communication data of a station. Same as choosing [Unlock Communication Data] from [Lock] menu.
 (*1)	Sets all communication data values. Same as choosing [Set Values] from [Lock] menu.

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Station List view

Lists local station and other stations communicating with local station.

The following items are shown on the Station List View.

Table F8.9-5 Items on Station List view

Item	Description
L	Shows the communication data locking status of the station.
D	Shows the communication data consistency or inconsistency of the station.
Station	Station name
Sending	Indicates whether the local station is sending.

Communication data locking status of stations

The communication data locking statuses of stations are displayed.

Table F8.9-6 Display of lock status

Item	Description
(No symbol)	No communication data is locked.
✹ (red)	All communication data are locked.
? (black)	SENG is unable to communicate with the station.

Communication data consistency of stations

It is regarded as inconsistent if any of the logical data and physical data of data values or data status are not the same.

Table F8.9-7 Consistency of communication data

Item	Description
(No symbol)	All communication data are consistent.
● (yellow)	Some communication data are inconsistent.
⦿ (red)	All communication data are inconsistent.
? (black)	SENG is unable to communicate with the station.

Output status of the local station

The output status of the local station is displayed.

Table F8.9-8 Output status of local station

Display	Description
● (green)	Output of the local station is enabled.
☒ (red)	Output of the local station is disabled.
? (black)	SENG cannot communicate with the local station.
(Blank)	Other station.

Filtering

The display can be filtered according to station type using the drop-down list box.

Table F8.9-9 Drop-down list box

Menu item	Description
SCS/FCS	All stations are shown.
SCS	SCS stations including local station are shown.
FCS	FCS, GSGW and APCS stations are shown.

Pop-up menu

Click the right mouse button on the Station List View to display the pop-up menu.

The menu item in the pop-up menu is shown as follows.

Table F8.9-10 Pop-up menu

Menu item	Description
Select All	Selects all displayed stations (same as choosing [Select All] from the [Edit] menu).

Communication Data List view

Displays the SCS Link Transmission data information for the station selected on the Station List View. The communication data that are not wired with the SCS Link Transmission function block will not be displayed.

Table F8.9-11 Items on Communication Data List view

Item	Description
Station	Station number
No.	Bit number (The number assigned on SCS Link Transmission Builder)
L	Communication data lock status
D	Communication data consistency or inconsistency
Instance	Instance name of the wired SCS Link Transmission function block
Data Type	Function block name
Logical Value	Logical data of data value and data status, respectively
Physical Value	Physical data of data value and data status, respectively
Set value (*1)	Set value of data value and data status, respectively
Comment	Comment entered for the SCS Link Transmission function block

*1: Displayed and editable only when the SCS project target name is SCS_SIMULATOR.

Communication data locking status

Displays the communication data locking status.

Table F8.9-12 Locking status

Item	Description
(No symbol)	The communication data is unlocked.
✶ (red)	The communication data is locked.
? (black)	SENG is unable to communicate with the station.

Communication data consistency

It is regarded as inconsistent if any of the logical data and physical data for data values or data statuses are not the same.

Table F8.9-13 Consistency of communication data

Item	Description
(No symbol)	The communication data is consistent.
● (red)	The communication data is inconsistent.
? (black)	SENG is unable to communicate with the station.

Logical data and physical data

The data value is displayed as either [TRUE] or [FALSE].

Data status is displayed as either [GOOD] or [BAD]. If the data status is BAD, the background color is displayed in yellow. [******] is displayed if communication with the station is disabled. However, the Link Transmission Data Output function block (LTSND) in the local station does not have data status.

Filtering

The displayed communication data can be filtered using the drop-down list box.

Table F8.9-14 Drop-down list box on the Communication Data List view

Menu Item	Description
All Data	Displays information of all communication data
Locked Data	Displays information of locked communication data
Unlocked Data	Displays information of unlocked communication data

Pop-up menu

Only when the SCS project target name is SCS_SIMULATOR, click the right mouse button on the Communication Data List View may display a pop-up menu.

The items on the pop-up menu are as follows:

Table F8.9-15 Items on pop-up menu in the Communication Data List view

Items		Description
Cut		Same as the [Cut] command on the [Edit] menu.
Copy		Same as the [Copy] command on the [Edit] menu.
Paste		Same as the [Paste] command on the [Edit] menu.
Delete		Same as the [Delete] command on the [Edit] menu.
Select All		Same as the [Select All] command on the [Edit] menu.
Input Values ►	Set .V=TRUE	Sets the data value in the Set Value cells to TRUE.
	Set .V=FALSE	Sets the data of Set Value to FALSE.
	Clear .V	Clears the data value in the Set Value cells.
	Set .STS=GOOD	Sets the data status of Set Value to GOOD.
	Set .STS=BAD	Sets the data status of Set Value to BAD.
	Clear .STS	Clears the data status of Set Value.

Selecting communication data

Only when the SCS project target name is SCS_SIMULATOR, the communication data can be selected on the Communication Data List View.

- Clicking a communication data while pressing the [Shift] key on the keyboard, the communication data can be selected.
- Clicking a communication data while pressing the [Ctrl] key on the keyboard, the communication data of the line can be selected.
- Choosing [Select All] from pop-up menu, all communication data can be selected.

Message display area

The results of locking, unlocking and setting operations are displayed as messages. The last displayed message is cleared at each operation.

Status bar

The status bar shows the following information about the stations displayed in the Station List View.

- Station Selected: Number of selected stations/Number of all stations

F8.9.1 Locking and unlocking all SCS link transmission data of a station

On SCS Link Transmission window, all SCS Link Transmission data of a station can be locked and unlocked together. This section explains the operating procedures.

Selecting station

Choose a station on the Station List View. With the following operations, the communication data information can be displayed on the Communication Data List View.

- You can display the communication data of the station by clicking on a station name.
- To select a consecutive group of stations, click the name of the first station and then click the name of the last station while holding down the [Shift] key on the keyboard. The communication data of the selected stations appears.
- If you click a station name while holding down the [Ctrl] key on your keyboard, the communication data of the station on the clicked line is added to the current display.

Locking communication data of a station

The communication data of SCS Link Transmission can be locked together for a selected station.
The procedure is as follows:

1. Choose a station for locking the communication data on the Station List View.
2. Check the discrepancies of the data values and data status between the logical communication data and physical communication data on the Communication Data List View, and make sure that the discrepancies are acceptable when locking the data.
3. Choose [Lock Communication Data] from [Lock] menu or click [Lock] button on the toolbar.
4. When a confirmation dialog box is displayed, click the [OK] button so as to lock all the communication data of the selected station.
   Clicking [Cancel] will cancel the locking.

Unlocking communication data of a station

The communication data of SCS Link Transmission can be unlocked together for a selected station.
The procedure is as follows:

1. Choose a station for unlocking the communication data on the Station List View.
2. Check the discrepancies of the data values and data status between the logical communication data and physical communication data on the Communication Data List View, and make sure that the discrepancies are acceptable when unlocking the data.
3. Choose [Unlock Communication Data] from [Lock] menu or click the [Unlock] button on the toolbar.
4. When a confirmation dialog box is displayed, click [OK] so as to unlock all the communication data of the selected station. Clicking [Cancel] will cancel the unlocking.
5. If inconsistency between any logical data and physical data exists, a reconfirmation dialog box will be displayed. Click the [OK] button on this dialog box to unlock all the communication data together.
   Clicking [Cancel] will cancel the unlocking.

F8.9.2 Set values of SCS link transmission data

On SCS Link Transmission Lock Window, communication data values of a locked station can be set one by one or all together per station.

The collective setting of communication data values on a station-by-station basis is possible when using the SCS Simulator during testing.

This section explains the operating procedures.

Set value to each communication data

The value can be set to each communication data.

However, the data status can only be set to all the data of the station. All the data in the station will use the defined data status.

IMPORTANT

Setting values to communication data cannot be executed while Build or Download is running.

On the Communication Data List View, double-clicking somewhere between No. and a physical data, a Write Data Value dialog box for that line of communication data will be displayed.

In the dialog box, the initial data values and data status of the selected data will be displayed, and setting data values on this dialog box is allowed.

- For Data Value
  When Write Data Value dialog box is opened, the logical data or the physical data will be displayed with either TRUE or FALSE button pressed.
- For Data Status
  When Write Data Value dialog box is opened, the logical data will be displayed with either GOOD or BAD button pressed.

The initial communication data values and data statuses of the logical data and physical data are shown as follows:

Table F8.9.2-1 Initial data on Write Data Value dialog box

Data Value (.v) and Data Status (.status)	Locked	Unlocked
Value of Received Communication Data (.v)	Logical	Logical
Status of Received Communication Data (.status)	Logical	Logical
Value of Sent Communication Data (.v)	Physical	Logical

The above can be set on the Write Data Value dialog box.

SEE ALSO For more information about procedure for setting values using the setting of values dialog box, refer to:

"Write/Lock/Unlock" in "Debug/Simulate" in "Workbench," "Debug" in the Workbench User's Guide

Set values to multiple items of communication data together

Using the SCS Simulator, you can set values to multiple communication data items together. The following operations can be performed on the SCS Link Transmission communication data of the selected station.

- Set values to the communication data.
- Save the set values for the communication data in a file.

- Read values form a file and set them to the communication data.

Note that the number of communication data values set at a time should be 700 or less. If more data values are set at a time, some of the system alarm messages informing the data setting or data status setting may not be transmitted.

Enter the values to be set to communication data

The values can be entered in the [Set Value] cells on the Communication Data List View. The value can be entered by any of the following operations. After entering the values, you need to set all the values to the communication data.

- Enter a Value Directly
  In the Communication Data List View, click the [Set Value] cell on the line of the communication data that you want to enter the value for. By clicking the data value or data status, they can be entered directly.

  For setting data, each click will move among TRUE, FALSE and a space (non specified) for selections.

- Edit Multiple Data Values
  From [Edit] menu or from the right-click menu, you can use [Cut], [Copy], [Paste] and [Del] commands to edit the values of consecutive [Set Value] cells.

- Enter Values Using [Input Values] on Pop-up Menu
  Right clicking on the Communication Data List View, a pop-up menu will be displayed. Using the [Input Values] command on the pop-up menu, you can enter data values or data status in the [Set Value] cells.

  For example, if you want to set all communication data to FALSE, use the [Select All] command on the pop-up menu to select all [Set Value] cells, and then choose [Input Values] - [Set.V=FALSE] on the pop-up menu.

Set values to all communication data

For the selected station, the values in the [Set Value] cells on the Communication Data List View can be set together to the communication data.

IMPORTANT

Setting values to communication data cannot be executed while Build or Download is running.

The procedure is as follows:

1. On the Station List View, choose a station that you want to set values for.
2. Choose [Set Values] from the [Lock] menu or click [Set Values] button on the toolbar so as to display Set Values dialog box.
3. Click [OK]. All the values entered in the [Set Value] cells will be set to the communication data. If no values are entered, the communication data will not be defined with values. You can cancel the setting by clicking [Cancel].

Export the setting values to a file

The values of the communication data in the [Set Value] cells can be exported to a file. The procedure is as follows:

1. Choose [Export Values] from the [File] menu, or click the [Export Values] button on the toolbar so as to display a dialog box for selecting files.
2. Specify a CSV file name and then click [Save]. The communication data values and data statuses of all the stations displayed in the Station List View are exported to the file.

IMPORTANT

Do not edit the exported file if you want to import the file later.

Import the setting values from a file

The values of communication data for [Set Value] cells can be imported from a file.

IMPORTANT

Do not import any file other than the file exported from SCS Link Transmission Lock Window.

The procedure is as follows:

1. Choose [Import Values] from the [File] menu, or click the [Import Values] button on the toolbar so as to display a dialog box for selecting files.
2. Choose the CSV file that contains the setting values and then click [Open]. The communication data values and data statuses for all the stations displayed on the Station List View are read from the file and displayed in the [Set Value] cells.

F8.10 Inter-SCS Communication Lock window

On the Inter-SCS Communication Lock Window, the communication data of inter-SCS safety communication can be locked or unlocked. You can also set data values to inter-SCS safety communication FBs.

In SCS Simulator of SCS Test Functions, it is possible to set values to multiple communication data together. Therefore, the initial values of communication data and testing patterns can be defined all together.

How to call up the Inter-SCS Communication Lock window

1. Check if the SCS security level is 0 or 1 using the SCS security level operation function.
2. Put the SCS Manager into Debug mode or Editing mode. To change to Debug mode, choose [Debug] from [Debug] menu or click [Debug] button on the toolbar.
3. Select [Maintenance] from the [Tools] menu of SCS Manager. The Maintenance Launcher menu appears.
4. Select [Inter-SCS Communication Lock Window] from the Maintenance Launcher menu. The Inter-SCS Communication Lock Window appears.

IMPORTANT

- The Inter-SCS Communication Lock Window cannot be launched while Build or Download is running on SCS Manager.
- It is not possible to start multiple Inter-SCS Communication Lock Windows at the same time, for neither the same SCS project nor different SCS projects.
- If the SCS Manager is closed or a different SCS project is opened, the Inter-SCS Communication Lock Window will be forcibly closed.
- If you try to execute online change downloading, offline downloading, master offline downloading, or restarting of SCS while the Inter-SCS Communication Lock Window is opened, an error message is displayed and the downloading or restarting will not be executed.

SEE ALSO For more information about functions for operating SCS security levels, refer to:

B3., “Security of SCS” in ProSafe-RS User’s Guide (IM 32P01B10-01EN)

How to exit the Inter-SCS Communication Lock window

To exit the Inter-SCS Communication Lock Window, choose [Exit] from [File] menu.
When exiting the Inter-SCS Communication Lock Window, if any locked inter-SCS safety communication FBs exist, a dialog box will be displayed for confirmation. Clicking [OK] will close the Inter-SCS Communication Lock Window.

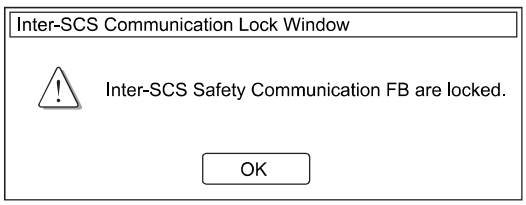


Figure F8.10-1 Confirmation dialog box

To unlock the locked inter-SCS safety communication FBs, it is necessary to launch the Inter-SCS Communication Lock Window again and unlock them.

Inter-SCS Communication Lock window structure

The Inter-SCS Communication Lock Window contains the following components.

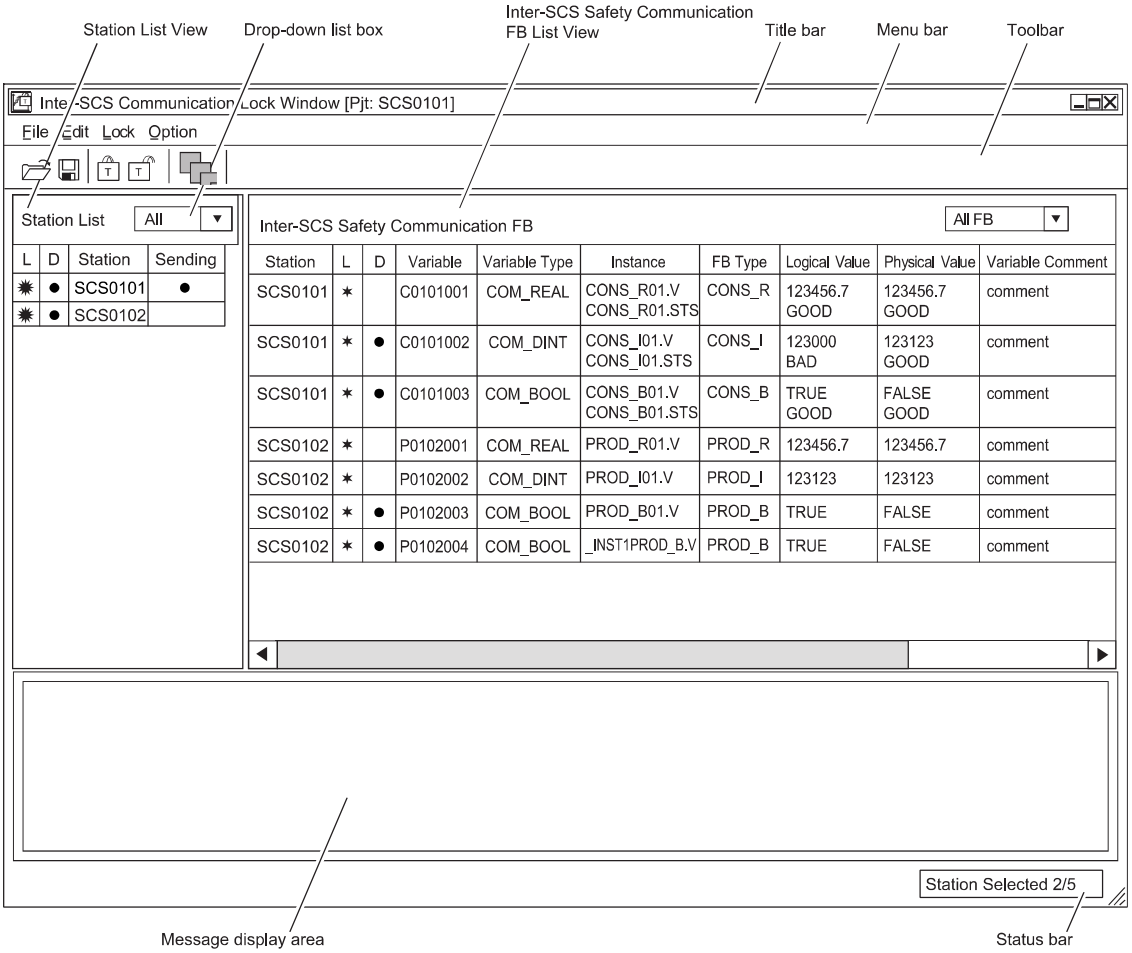


Figure F8.10-2 Inter-SCS Communication Lock window

Title bar

On the title bar, besides window name and project name, the SCS status is also displayed.

- SCS_TARGET: Indicates communication with the SCS.
- SCS_SIMULATOR: Indicates communication with the SCS simulator.
- <No display>: Indicates that the SCS is not running.

During logic simulation test, "SIMULATION" will be displayed in the position of SCS status.

Menu bar

The following menus are provided on the menu bar:

- [File] Menu
- [Edit] Menu
- [Lock] Menu

- [Option] Menu

The menu items provided on each menu are explained as follows.

Table F8.10-1 File menu

Menu item	Description
Import Values... (*1)	Imports from a file the values to be collectively set to inter-SCS safety communication FBs.
Export Values... (*1)	Exports to a file the values collectively set to inter-SCS safety communication FBs.
Exit	Exits from the Inter-SCS Communication Lock Window.

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Table F8.10-2 Edit menu

Menu item	Description
Cut (*1)	Deletes the selected character string and copies it onto the clipboard.
Copy (*1)	Copies the selected character string onto the clipboard.
Paste (*1)	Inserts the character string stored in the clipboard.
Delete (*1)	Deletes the selected character string.
Select All	Selects all displayed modules (same action as pressing the [Ctrl] key and [A] key together).

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Table F8.10-3 Lock menu

Menu item	Description
Lock Inter-SCS Safety Communication FB	Locks all inter-SCS safety communication FBs associated with the selected station.
Unlock Inter-SCS Safety Communication FB	Unlocks all inter-SCS safety communication FBs associated with the selected station.
Set Values (*1)	Collectively sets values to inter-SCS safety communication FBs.

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Table F8.10-4 Option menu

Menu item			Description
Numerical Display	INT	Decimal	Decimal expression
		Hexa-Decimal	Hexadecimal expression
	REAL	1.234E+12	Exponential notation
		12.34567	Displays 5 decimal places.
		123.4567	Displays 4 decimal places.
		1234.567	Displays 3 decimal places.
		12345.67	Displays 2 decimal places.
		123456.7	Displays 1 decimal places.

Toolbar

The following buttons are provided on the toolbar.

Table F8.10-5 Toolbar buttons

Button	Description
(*1)	Imports from a file the values to be collectively set to inter-SCS safety communication FBs (same as selecting [File] - [Import Values] from the menu bar).
(*1)	Exports to a file the values collectively set to inter-SCS safety communication FBs (same as selecting [File] - [Export Values] from the menu bar).
	Locks all inter-SCS safety communication FBs associated with the selected station (same as choosing [Lock Communication Data] from the [Lock] menu).
	Unlocks all inter-SCS safety communication FBs associated with the selected station (same as choosing [Unlock Communication Data] from the [Lock] menu).
(*1)	Sets all values of inter-SCS safety communication FBs together (same as choosing [Set Values] from the [Lock] menu).

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Station List view

This view displays a list of local station and other stations performing inter-SCS safety communication with the local station.

The following items are shown on the Station List View.

Table F8.10-6 Items on Station List view

Item	Display
L	Lock status of inter-SCS safety communication FBs of the station
D	Data consistency of inter-SCS safety communication FBs of the station
Station	Station name
Sending	Whether the local station is sending

Lock status of Inter-SCS safety communication FBs of stations

The lock status of inter-SCS safety communication FBs is displayed for each station.

Table F8.10-7 Lock status

Display	Meaning
(Blank)	No inter-SCS safety communication FBs is locked.
✹ (red)	All inter-SCS safety communication FBs are locked.
? (black)	SENG cannot communicate with the station.

Data consistency of Inter-SCS safety communication FBs of stations

It is regarded as inconsistent if any of the logical data and physical data of data values or data status are not the same. In the case of REAL-type data, however, it is regarded as inconsistent only if the logical data and physical data of data status are not the same.

Table F8.10-8 Data consistency

Display	Meaning
(Blank)	All inter-SCS safety communication FB data are consistent.
● (yellow)	Some inter-SCS safety communication FB data are inconsistent.
⦿ (red)	All inter-SCS safety communication FB data are inconsistent.
? (black)	SENG cannot communicate with the station.

Output status of the local station

The output status of the local station is displayed.

Table F8.10-9 Output status of local station

Display	Description
● (green)	Output of the local station is enabled.
☒ (red)	Output of the local station is disabled.
? (black)	SENG cannot communicate with the local station.
(Blank)	Other station.

Filtering

The display can be filtered according to the role of the station using the drop-down list box.

Table F8.10-10 Filter menu items in drop-down list box

Menu item	Displayed Stations
ALL	All stations
PROD	SCSs for which producer inter-SCS safety communication FBs are defined in the SCS project
CONS	SCSs sending to the consumer inter-SCS safety communication FBs in the SCS project

Pop-up menu

Click the right mouse button on the Station List View to display the pop-up menu.

The menu item in the pop-up menu is shown as follows.

Table F8.10-11 Pop-up menu

Menu item	Description
Select All	Selects all displayed stations (same as choosing [Select All] from the [Edit] menu).

Inter-SCS safety communication FB list view

This view displays information of inter-SCS safety communication FBs associated with the station selected on the Station List View. Among inter-SCS safety communication FBs used in programs, those directly connected to binding variables are displayed.

Table F8.10-12 Items displayed in the Inter-SCS safety communication FB list view

Item name	Description
Station	Station name
L	Lock status of the inter-SCS safety communication FB
D	Data consistency of the inter-SCS safety communication FB
Variable	Binding variable
Variable Type	Type of binding variable
Instance	Instance name of the inter-SCS safety communication FB
FB Type	Type of the inter-SCS safety communication FB
Logical Value	Logical data of data value and data status
Physical Value	Physical data of data value and data status

Continues on the next page

Table F8.10-12 Items displayed in the Inter-SCS safety communication FB list view (Table continued)

Item name	Description
Set value (*1)	Setting values of data value and data status
Variable Comment	Comment of the binding variable

*1: Displayed and editable only when the target name of the SCS project is SCS_SIMULATOR.

Station name

For producer inter-SCS safety communication FBs, the station name of the local station is displayed.

For consumer inter-SCS safety communication FBs, the station name of the sending station is displayed.

Lock status of Inter-SCS safety communication FB

The lock status of inter-SCS safety communication FB is displayed.

Table F8.10-13 Display of lock status

Display	Meaning
(Blank)	Not locked
✶ (red)	Locked
? (black)	SENG cannot communicate with the station.

TIP

The lock status is only shown in the Inter-SCS Communication Lock Window. It cannot be viewed on Dictionary View of the Workbench.

Data consistency of Inter-SCS safety communication FBs

It is regarded as inconsistent if any of the logical data and physical data of data values or data status are not the same. In the case of REAL-type data, however, it is regarded as inconsistent if the logical data and physical data of data status are not the same.

Table F8.10-14 Data consistency of Inter-SCS safety communication FB

Display	Meaning
(Blank)	Consistent
● (red)	Inconsistent
? (black)	SENG cannot communicate with the station.

Binding variable

Binding variables directly connected to inter-SCS safety communication FBs are displayed.

Instance name of Inter-SCS safety communication FB

"Instance name.V" and "instance name.STS" are displayed (V refers to data, while STS refers to data status). However, producer inter-SCS safety communication FBs do not have data status.

TIP

If an inter-SCS safety communication FB does not have an instance name, an instance name automatically generated by the system is displayed.

Table F8.10-15 Examples of automatically generated instance names

FB type	Automatically generated instance name	Remark
CONS_B	__INSTnCONS_B (For FBD) __LCFBCONS_Bn (For LD)	n is a number given by the system.
CONS_I	__INSTnCONS_I (For FBD) __LCFBCONS_In (For LD)	
CONS_R	__INSTnCONS_R (For FBD) __LCFBCONS_Rn (For LD)	
PROD_B	__INSTnPROD_B (For FBD) __LCFBPROD_Bn (For LD)	
PROD_I	__INSTnPROD_I (For FBD) __LCFBPROD_In (For LD)	
PROD_R	__INSTnPROD_R (For FBD) __LCFBPROD_Rn (For LD)	

Logical data and physical data

A BOOL-type data value is displayed as either [TRUE] or [FALSE].

A DINT- or REAL-type data value is displayed using the format selected from the [Option] menu.

Data status is displayed as either [GOOD] or [BAD]. If the data status is BAD, the background color is displayed in yellow. [******] is displayed if communication with the station is disabled. However, producer inter-SCS safety communication FBs do not have data status.

TIP

- Inter-SCS safety communication FBs used as parameters are not displayed in the Inter-SCS Communication Lock Window, and forcing cannot be performed on them.
- Binding variables are displayed only when they are directly connected to inter-SCS safety communication FBs and also set in the binding list.
- If multiple consumer inter-SCS safety communication FBs are connected to a single binding variable, the same binding variable is displayed with each of the consumer inter-SCS safety communication FBs.
- If multiple binding variables are connected to a single producer inter-SCS safety communication FB, the same FB is displayed with each of the binding variables.
- Only the Inter-SCS Communication Lock Window shows both logical and physical data values.

Filtering

It is possible to filter the inter-SCS safety communication FBs to be displayed using the drop-down list box.

Table F8.10-16 Drop-down list box menu of the Inter-SCS safety communication FB list view

Item	Displayed FB
All FB	Information of all inter-SCS safety communication FBs
Locked FB	Information of locked inter-SCS safety communication FBs
Unlock FB	Information of unlocked inter-SCS safety communication FBs

Pop-up menu

If the target name of the SCS project is SCS_SIMULATOR, clicking the right mouse button in the Inter-SCS Safety Communication FB List View displays a pop-up menu.

The items on the pop-up menu are as follows:

Table F8.10-17 Items on pop-up menu in the Inter-SCS safety communication FB list view

Items		Description
Cut		Same as the [Cut] command on the [Edit] menu.
Copy		Same as the [Copy] command on the [Edit] menu.
Paste		Same as the [Paste] command on the [Edit] menu.
Delete		Same as the [Delete] command on the [Edit] menu.
Select All		Same as the [Select All] command on the [Edit] menu.
Input Values ►	Set .V=TRUE	Sets the data value in the Set Value cells to TRUE.
	Set .V=FALSE	Sets the data of Set Value to FALSE.
	Clear .V	Clears the data value in the Set Value cells.
	Set .STS=GOOD	Sets the data status of Set Value to GOOD.
	Set .STS=BAD	Sets the data status of Set Value to BAD.
	Clear .STS	Clears the data status of Set Value.

Selecting Inter-SCS safety communication FB

If the SCS project target name is SCS_SIMULATOR, you can select the [Set Value] column of inter-SCS safety communication FBs to set values.

- By clicking the [Set Value] column of an inter-SCS safety communication FB while pressing the [Shift] key of the keyboard, the selection range of inter-SCS safety communication FBs can be widened.
- By clicking the [Set Value] column of an inter-SCS safety communication FB while pressing the [Ctrl] key of the keyboard, multiple inter-SCS safety communication FBs of the clicked lines can be selected.
- By selecting [Select All] from the pop-up menu, the [Set Value] column of all inter-SCS safety communication FBs can be selected.

Message display area

The results of locking, unlocking and value setting operations are displayed as messages. The previously displayed message is cleared at each operation. Displayed messages are stored in the log.

Status bar

The status bar shows the number of stations displayed in the Station List View in the following format.

- Station Selected: Number of selected stations/Number of all stations

F8.10.1 Locking and unlocking all Inter-SCS safety communication FBs associated with a station

On Inter-SCS Communication Lock Window, all inter-SCS safety communication FBs associated with a station can be locked or unlocked together. This section explains the operating procedures.

Selecting station

Choose one or more stations in the Station List View. With the following operations, the information of inter-SCS safety communication FBs is displayed in the Inter-SCS Safety Communication FB List View.

- If you simply click a station name, the information of the inter-SCS safety communication FBs associated with the station is appears.
- To select a consecutive group of stations, click the name of the first station and then click the name of the last station while holding down the [Shift] key on the keyboard. The information of the inter-SCS safety communication FBs associated with the selected stations appears.
- If you click a station name while holding down the [Ctrl] key on your keyboard, the information of the inter-SCS safety communication FBs associated with the station on the line is displayed in addition to the currently displayed information.

Locking Inter-SCS safety communication FBs of a station

All the inter-SCS safety communication FBs associated with a selected station can be locked together.

IMPORTANT

The inter-SCS safety communication FBs cannot be locked while Build or Download is running.

The procedure is as follows:

1. Choose a station for locking the communication data on the Station List View.
2. In the Inter-SCS Safety Communication FB List View, check the discrepancies between the logical data and physical data of the inter-SCS safety communication FBs' data values and data status, and make sure that the discrepancies are acceptable when locking the data.
3. Choose [Lock Inter-SCS Safety Communication FB] from the [Lock] menu or click [Lock] button on the toolbar.
4. On the confirmation dialog box displayed, click [OK] so as to lock all the inter-SCS safety communication FBs associated with the selected station.
   Clicking [Cancel] will cancel the locking.

IMPORTANT

Always use the Inter-SCS Communication Lock Window to lock inter-SCS safety communication FBs. An error occurs if you lock binding variables of inter-SCS safety communication FBs from Dictionary View or Multi-Language Editor.

Unlocking Inter-SCS safety communication FBs of a station

All the inter-SCS safety communication FBs associated with a selected station can be unlocked together.

IMPORTANT

The inter-SCS safety communication FBs cannot be unlocked while Build or Download is running.

The procedure is as follows:

1. Choose a station to be unlocked in the Station List View.
2. In the Inter-SCS Safety Communication FB List View, check the discrepancies between the logical data and physical data of the inter-SCS safety communication FBs' data values and data status, and make sure that the discrepancies are acceptable when unlocking the data.
3. Choose [Unlock Inter-SCS Safety Communication FB] from the [Lock] menu or click the [Unlock] button on the toolbar.
4. On the confirmation dialog box displayed, click [OK] to unlock; or click [Cancel] if you want to cancel.
5. If any inconsistency between logical data and physical data exists in the FBs to be unlocked, a reconfirmation dialog box will be displayed. In the case of REAL-type data, the reconfirmation dialog box will not be displayed even if inconsistency between data values exists. Click [OK] to unlock.
   All the inter-SCS safety communication FBs associated with the selected station are unlocked.
   Click [Cancel] if you want to cancel the unlocking.

F8.10.2 Set values of Inter-SCS safety communication FBs

On Inter-SCS Communication Lock Window, data values can be set for individual inter-SCS safety communication FBs or for all inter-SCS safety communication FBs together on a station-by-station basis.

The collective setting on a station-by-station basis is possible when using the SCS Simulator during testing.

This section explains the operating procedures.

Set value to each Inter-SCS safety communication FB

Data values and data status can be set for each inter-SCS safety communication FB of the station whose inter-SCS safety communication FBs are locked.

IMPORTANT

You cannot set values to inter-SCS safety communication FBs while Build or Download is running.

In the Inter-SCS Safety Communication FB List View, double-clicking in a cell between L column and Physical Value column on any line will open a dialog box for setting data values or data status of the inter-SCS safety communication FB for that line.

If you double-click the area showing the data value, the Write Data Value dialog box appears. If you double-click the area showing the data status, the Write Data Status dialog box appears.

In these dialog boxes, a data value or data status is set for an individual inter-SCS safety communication FB.

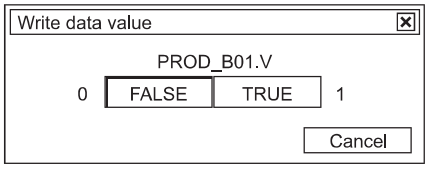


Figure F8.10.2-1 Write Data Value dialog box (BOOL-type data)

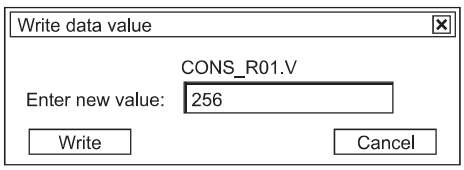


Figure F8.10.2-2 Write Data Value dialog box (REAL/INT-type data)

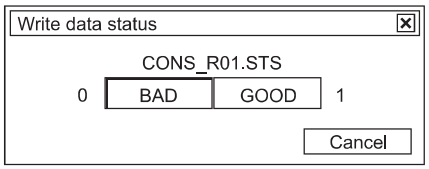


Figure F8.10.2-3 Write Data Status dialog box

For BOOL-type data, the Write Data Value dialog box or Write Data Status dialog box will be opened, showing the button corresponding to the current value pressed.

The Write Data Value dialog box for REAL/INT-type data will be opened, showing the current data value.

Whether logical data or physical data is displayed in the dialog box is determined according to which data value is settable. If a value can be set for logical data, logical data is displayed. If a value can be set for physical data, physical data is displayed. The following table shows the data displayed in the dialog box.

Table F8.10.2-1 Data displayed on Write data value/Write data status dialog box

Data Value (.v) and Data Status (.status)	Locked	Unlocked
Data value of consumer inter-SCS safety communication FB (.v)	Logical data	Logical data
Data status of consumer inter-SCS safety communication FB (.status)	Logical data	Logical data
Data value of producer inter-SCS safety communication FB (.v)	Physical data	Logical data

Value setting operations on the Write Data Value/Status dialog box are the same as on Dictionary View.

SEE ALSO For more information about procedure for setting values using the "Write data value" dialog box, refer to:

"Write/Lock/Unlock" in "Debug/Simulate" in "Workbench," "Debug" in the Workbench User's Guide

Set values to multiple Inter-SCS safety communication FBs together

Using the SCS Simulator, you can set values to multiple inter-SCS Safety Communication FBs together.
The following operations can be performed collectively on the data values and data status of inter-SCS Safety Communication FBs of the selected station. (Setting of data status is only possible for consumer inter-SCS safety communication FBs.)

- Set values to inter-SCS safety communication FBs.
- Save the setting values for inter-SCS safety communication FBs in a file.
- Read values from a file and set them to inter-SCS safety communication FBs.

Enter the values to be set to Inter-SCS safety communication FBs

The values can be entered in the [Set Value] cells of the Inter-SCS Safety Communication FB List View.
The value can be entered by any of the following operations. After entering the values, you need to write them to the inter-SCS safety communication FBs.

- Enter a Value Directly
  In the Inter-SCS Safety Communication FB List View, click the [Set Value] cell on the line of the inter-SCS safety communication FB you want to enter the value for. By specifically clicking the data value or data status, they can be entered directly.

  In the case of BOOL-type data, each click will move among TRUE, FALSE, and a space (not specified) for selection.

  In the case of DINT/REAL-type data, values can be directly entered using your keyboard.
- Edit Multiple Data Values
  From [Edit] menu or from the right-click menu, you can use [Cut], [Copy], [Paste] and [Del] commands to edit the values of consecutive [Set Value] cells.
- Enter Values Using [Input Values] on Pop-up Menu
  Right clicking in the Inter-SCS Safety Communication FB List View will display a pop-up menu. Using the [Input Values] command on the pop-up menu, you can enter data values or data status in the [Set Value] cells.

  For example, if you want to specify FALSE for BOOL-type data values in all inter-SCS safety communication FBs, on the pop-up menu, click [Select All] to select the Set Value

items for all data. Next, on the pop-up menu, click [Input Values] and select [Set.V=FALSE].

Set values to all Inter-SCS safety communication FBs

All the values in the [Set Value] cells in the Inter-SCS Safety Communication FB List View can be set together to the inter-SCS safety communication FBs associated with the selected station.

IMPORTANT

Setting values to all the inter-SCS safety communication FBs cannot be executed while Build or Download is running.

The procedure is as follows:

1. In the Station List View, choose a station you want to set values for.
2. Choose [Set Values] from the [Lock] menu or click the [Set Values] button on the toolbar. A dialog box appears, asking you whether or not to execute setting values.
3. Click [OK]. All the values entered in the [Set Value] cells will be set to the communication data. If no values are entered (blank), values will not be set to the corresponding inter-SCS safety communication FBs.
   You can cancel the setting by clicking [Cancel].

Export the setting values to a file

The values for inter-SCS safety communication FBs in the [Set Value] cells can be exported to a file.
The procedure is as follows:

1. Choose [Export Values] from the [File] menu, or click the [Export Values] button on the toolbar so as to display a dialog box for selecting files.
2. Specify a CSV file name and then click [Save]. The inter-SCS safety communication FBs' data values and data statuses of all the stations displayed in the Station List View will be exported to the file.

IMPORTANT

Do not edit the exported file if you want to import the file later.

Import the setting values from a file

The values of inter-SCS safety communication FBs for [Set Value] cells can be imported from a file.

IMPORTANT

Do not import any file other than the file exported from Inter-SCS Communication Lock Window.

The procedure is as follows:

1. Choose [Import Values] from the [File] menu, or click the [Import Values] button on the toolbar so as to display a dialog box for selecting files.

2. Choose the CSV file that contains the setting values and then click [Open]. The data values and data statuses of inter-SCS safety communication FBs for all the stations displayed in the Station list View are read from the file and displayed in the [Set Value] cells.

F8.11 Communication I/O Lock window

This section gives an overview of the Communication I/O Lock window.

The Communication I/O Lock window is used to change or lock input from or output to subsystems by using the Forcing function. The modules subject to these functions are ALR111M, ALR121M, and ALE111M.

The Communication I/O Lock window is also used to lock subsystem communication I/O. The applicable I/O module is S2LP131.

In SCS Simulation test, it is possible to set values to multiple communication data together. Therefore, the initial values of communication data and testing patterns can be defined all together.

The Communication I/O Lock window is used to perform the following tasks:

- Debug the application logic that uses subsystem communication or safety subsystem communication
- Disconnect I/O during maintenance of a subsystem communication module or fire and gas communication module
- Lock communication I/O related to subsystem communication data or safety subsystem communication data during online change download

Positioning of the Communication I/O Lock window

The Communication I/O Lock window is one of the windows used mainly for maintenance purposes. The Communication I/O Lock window is launched from SCS Manager.

The positioning of the Communication I/O Lock window is as follows:

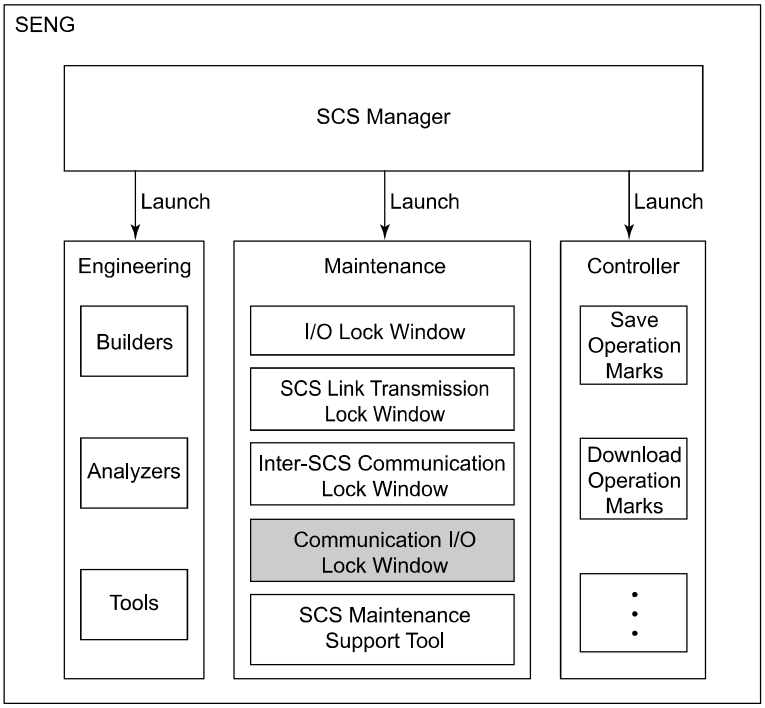


Figure F8.11-1 Positioning of Communication I/O Lock window in SENG

The following figure shows the relationship between the Communication I/O Lock Window and the Forcing function for SCS:

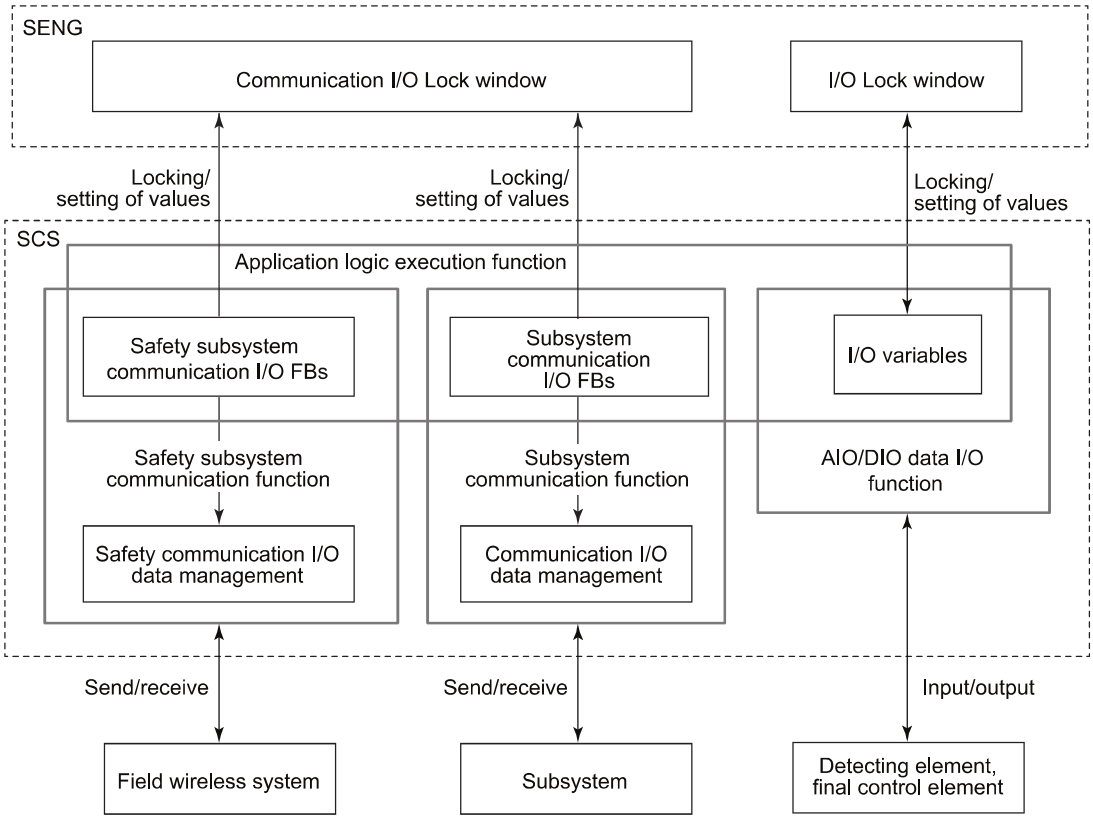


Figure F8.11-2 Relationship between the SCS, subsystem, and safety subsystem

Functions of the Communication I/O Lock window

Locking and unlocking

The I/O of subsystem communication data and safety subsystem communication data can be locked or unlocked. The lock status is also displayed for locked data.

Subsystem communication modules can be locked or unlocked in the following units.

- Lock or unlock all input data in a communication module
- Lock or unlock all output data in a communication module
- Lock or unlock all input/output data in a communication module

Fire and gas communication modules can be unlocked in the following units.

- Lock or unlock all inputs of a fire and gas communication module
- Lock or unlock each communication definition (PROFINET module) connected to a fire and gas communication module

Setting of values

Values can be set when the input or output data of subsystem communication and safety subsystem communication is locked. Logical data and physical data are displayed for each value.

A data value can be set for each communication data item. A data status can be set for each communication definition.

When the SCS project target name is SCS_SIMULATOR, it is possible to set values to multiple communication data together.

Start the Communication I/O Lock window

1. Check if the SCS security level is 0 or 1 using the SCS security level operation function.
2. Put the SCS Manager into Debug mode or Editing mode.
   To change to Debug mode, choose [Debug] from [Debug] menu or click [Debug] button on the toolbar.
3. Select [Maintenance] from the [Tools] menu of SCS Manager.
   The Maintenance Launcher menu appears.
4. Select [Communication I/O Lock Window] from the Maintenance Launcher menu.
   The Communication I/O Lock window appears.

IMPORTANT

- The Communication I/O Lock window cannot be started while Build or Download is running in SCS Manager.
- Multiple Communication I/O Lock windows cannot be launched simultaneously regardless of whether or not the windows are for the same SCS project or different SCS projects.
- The Communication I/O Lock window will be forcibly closed when SCS Manager is closed or a different SCS project is opened.

Exit the Communication I/O Lock window

To exit the Communication I/O Lock window, on the [File] menu, select [Exit].
When you try to exit the Communication I/O Lock window, a confirmation dialog box appears if any communication module, fire and gas communication module, or safety subsystem communication input is locked. Click [OK] to close the Communication I/O Lock window.

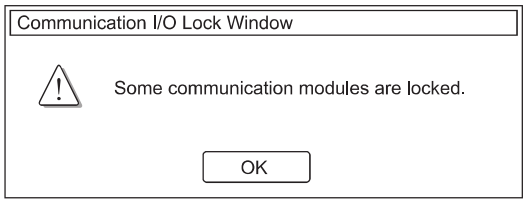


Figure F8.11-3 Confirmation dialog box

To unlock the applicable communication module, start the Communication I/O Lock window again and perform the necessary operation.

IMPORTANT

If you commenced an online change download when the Communication I/O Lock window is open, close the Communication I/O Lock window after the online change download is completed.

If the Communication I/O Lock window remains open after completion of an online change download in which the database related to subsystem communication or safety subsystem communication is changed, a database discrepancy error may occur when the displayed data is refreshed subsequently. When this error occurs, a message prompting you to re-open the Communication I/O Lock window will be displayed.

F8.11.1 Structure of the Communication I/O Lock window

This section describes the window structure and components of the Communication I/O Lock window.

The screen configuration of the Communication I/O Lock window differs between the subsystem communication mode and the safety subsystem communication mode.

The mode can be switched from the Mode menu.

The window configuration of the Communication I/O Lock window is as follows:

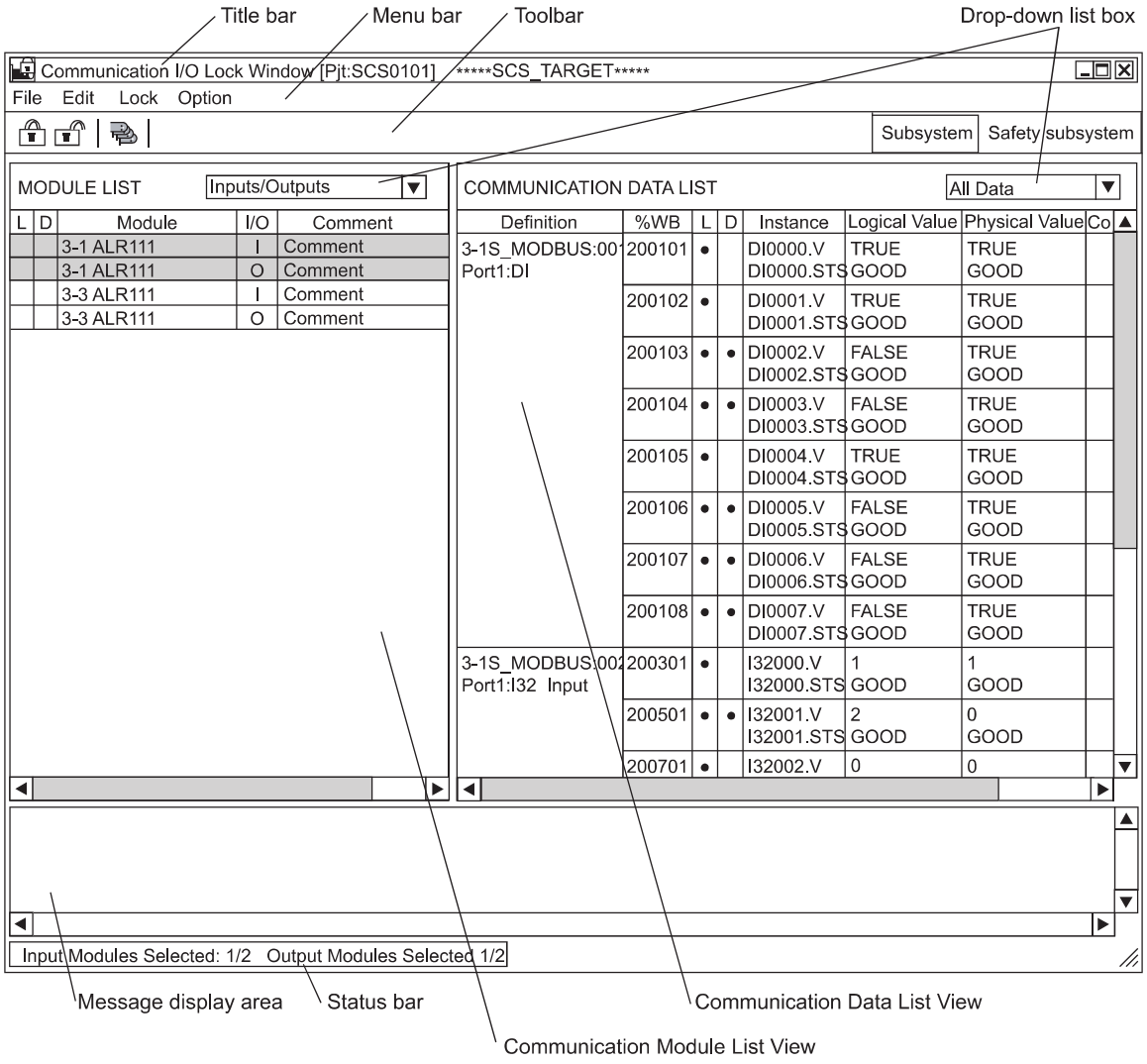


Figure F8.11.1-1 Communication I/O Lock window for the subsystem communication mode

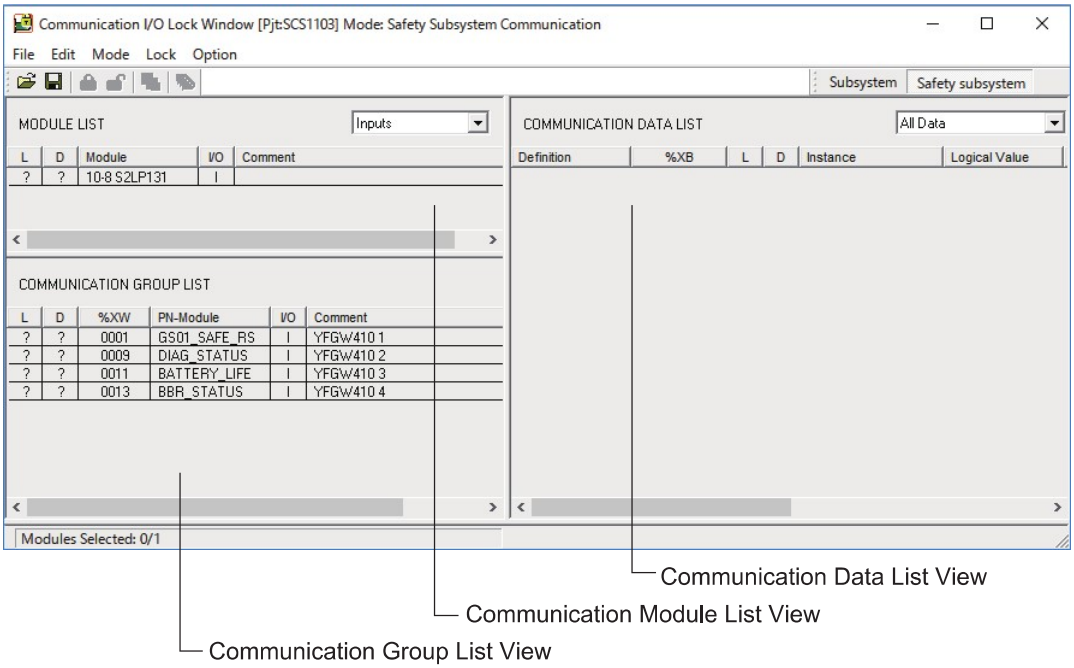


Figure F8.11.1-2 Communication I/O Lock window for the safety subsystem communication mode

The following section explains the elements that make up the window.

Title bar

The status of the SCS is displayed as follows:

- SCS_TARGET
- SCS_SIMULATOR
- (No display)

For logic simulation test, "SIMULATION" will be displayed in the position of SCS status.

The mode is displayed as follows:

Mode: xxxxxxx

Menu bar

The following menus are provided on the menu bar:

- File menu
- Edit menu
- Mode menu
  The Mode menu is available only for SCS of type S2SC70/L1SC70 which is engineered by I/O list engineering.
- Lock menu
- Option menu

The following menu items are provided on each menu:

Table F8.11.1-1 File menu

Menu item	Description
Import Values...(*1)	Imports the values for setting all together to communication data from a file.

Continues on the next page

Table F8.11.1-1 File menu (Table continued)

Menu item	Description
Export Values...(*1)	Exports the values for setting all together to communication data to a file.
Exit	Exits from the Communication I/O Lock window.

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Table F8.11.1-2 Edit menu

Menu item	Description
Cut(*1)	Cut
Copy(*1)	Copy
Paste(*1)	Paste
Delete(*1)	Delete
Select All	Select All (the same as pressing the [Ctrl] key + the [A] key on the keyboard)

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Table F8.11.1-3 Mode menu

Menu item	Description
Subsystem Communication	Switches to the subsystem communication screen.
Safety Subsystem Communication	Switches to the safety subsystem communication screen.

Table F8.11.1-4 Lock menu

Menu item	Description
Lock Modules	Locks all modules selected.
Unlock Modules	Unlocks all modules selected.
Set Values(*1)	Sets all values of communication data.

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Table F8.11.1-5 Option menu

Menu item			Description
Numerical Display	INT	Decimal	Decimal expression(*1)
		Hexadecimal	Displays in hexadecimal number format.
	REAL	1.234E+12	Exponential notation
		12.34567	Displays 5 decimal places.
		123.4567	Displays 4 decimal places.
		1234.567	Displays 3 decimal places.
		12345.67	Displays 2 decimal places.
		123456.7	Displays 1 decimal places.
Data Acquiring Mode	All Modules		Changes data acquiring mode to "All Modules" mode
	Selected Modules		Changes data acquiring mode to "Selected Modules" mode

*1: A negative sign is added if the value of a signed integer is negative.

Toolbar

The following buttons are provided on the toolbar:

Table F8.11.1-6 Toolbar buttons

Button	Description
(*1)	Imports the values for setting all together to communication data from a file. Same as choosing [Import Values] from [File] menu.
(*1)	Exports the values for setting all together to communication data to a file. Same as choosing [Export Values] from [File] menu.
	Locks all modules selected. Same as choosing [Lock Modules] from [Lock] menu.
	Unlocks all modules selected. Same as choosing [Unlock Modules] from [Lock] menu.
(*1)	Sets all values of communication data. Same as choosing [Set Values] from [Lock] menu.
(All Modules) (Selected Modules)	Switch data acquisition modes (same as the [Data Acquiring] on the [Option] menu. Switches between [All Modules] and [Selected Modules])
[Subsystem] (displayed on right edge as a string)	Switching to the subsystem communication mode Enabled with I/O list engineering, when the SCS type is S2SC70/ L1SC70 (similar to [Subsystem Communication] in the [Mode] menu)
[Safety Subsystem] (displayed on right edge as a string)	Switching to the safety subsystem communication mode Enabled with I/O list engineering, when the SCS type is S2SC70 (similar to [Safety Subsystem Communication] in the [Mode] menu)

*1: Displayed only when the SCS project target name is SCS_SIMULATOR.

Data acquisition mode

The data acquisition mode is used when acquiring data values and statuses from an SCS.

- "All modules" mode
  Communication data corresponding to the communication definitions of all subsystem communication modules defined in the applicable SCS project will be acquired sequentially.
- "Selected modules" mode
  Communication data corresponding to the communication definitions of the subsystem communication modules selected in the Communication Module List View will be acquired sequentially.

  While data is acquired, "Updating Selected Modules" is displayed in the Communication Module List View and Communication Data List View.

Communication Module List view

The Communication Module List view displays a list of communication modules defined in the current SCS project opened with SCS Manager. However, Modbus slave modules are excluded. The following communication modules are displayed:

Table F8.11.1-7 Displayed communication modules

Mode	Module model name	Display method
Subsystem communication mode	ALR111M ALR121M ALE111M	Displayed in the form of the following two lines for each module: • A line indicating the input communication definition • A line indicating the output communication definition This view always shows two lines even when there are no communication definitions or a subsystem communication FB is not specified for a communication definition.

Continues on the next page

Table F8.11.1-7 Displayed communication modules (Table continued)

Mode	Module model name	Display method
Safety subsystem communication mode	S2LP131	A single line indicating the input communication definition is displayed for each module. This is displayed even when there are no communication definitions or a fire and gas communication FB is not specified for a communication definition.

When the subsystem communication module is used in a dual-redundant configuration, information of the module in the odd-number slot is displayed regardless of which module is currently operating. Note, however, that the L and D fields show the corresponding statuses of the module on the control side.

The following items are displayed in the Communication module list view:

Table F8.11.1-8 Items displayed in Communication Module List view

Item	Description
L	Lock status of communication data for the communication module
D	Consistency/discrepancy of logical data and physical data of communication data for the communication module
Module	Communication module name (with node number (n) and slot number (s))
I/O	Signal direction of the communication module ([I]: input, [O]: output)
Comment	Comments for the communication module

Lock status of communication data for the communication module

Table F8.11.1-9 Lock status display (L field)

LED	Meaning
(No symbol)	None of the communication data is locked.
✶(yellow)	Part of the communication data is locked
✹ (red)	All communication data are locked.
? (black)	Communication with the SCS is disabled.

Consistency/discrepancy of logical data and physical data of communication data for the communication module

Discrete inputs and outputs are deemed to have "discrepancy" if the logical data and physical data of the data value or data status are different.

Analog inputs and outputs are deemed to have "discrepancy" if the logical data and physical data of the data status are different.

Table F8.11.1-10 Data consistency/discrepancy display (D field)

Display	Meaning
(No symbol)	All communication data are consistent.
● (yellow)	Some communication data have discrepancy.
⦿ (red)	All communication data have discrepancy.
? (black)	Communication with the SCS is disabled.

The consistency/discrepancy display of communication data for each communication module varies depending on the data acquisition mode.

- When the data acquisition mode is "All Modules"

Data corresponding to all communication modules defined in the applicable SCS project will be refreshed and displayed sequentially.

- When the data acquisition mode is "Selected Modules"
  Data corresponding to the communication modules selected in the Communication Module List View will be refreshed and displayed sequentially. A "?" symbol will be shown in the D field for communication modules that are not selected.

Filtering

Using a drop-down list box, communication module I/O can be filtered based on input/output. Only Inputs can be selected in the safety subsystem communication mode.

Table F8.11.1-11 Drop-down list box in Communication Module List view

Menu item	Operation
Inputs/Outputs	Both the input and output lines of communication definitions are displayed.
Inputs	Only the input lines of communication definitions are displayed.
Outputs	Only the output lines of communication definitions are displayed.

Pop-up menu

Click the right mouse button on the Communication Module List View to display the pop-up menu.
The following menu items are displayed in the pop-up menu:

Table F8.11.1-12 Pop-up menu in Communication Module List View

Menu item	Description
Select All	Selects all displayed modules. Same as choosing [Select All] from [Edit] menu and same action as pressing the [Ctrl] key and [A] key together.

Communication group list view

In the safety subsystem communication mode, lists are displayed to the number of PROFINET modules displayed in the Fire and Gas Comm. I/O Definition tab of Communication I/O Builder. A list is displayed for every fire and gas communication module that is connected.

This list view is not displayed in the subsystem communication mode.

The following table shows the items that are displayed in the communication group list view.

Table F8.11.1-13 Items displayed in the communication group list view

Item name	Displayed content	Meaning
L	Lock status of the communication data for the PROFINET module	The displays and meanings are the same as in the communication module list view.
D	PROFINET module communication data consistency	The displays and meanings are the same as in the communication module list view.
%XW	Element number	The element number of the corresponding PROFINET module.
PN-Module	PROFINET module name	The module name displayed here is that which is defined in the column for Module Name on the Safety Subsystem Comm. I/O Definition tab of Communication I/O Builder.

Continues on the next page

Table F8.11.1-13 Items displayed in the communication group list view (Table continued)

Item name	Displayed content	Meaning
I/O	PROFINET module signal direction	The displays and meanings are the same as in the communication module list view.
Comment	Comments for the PROFINET module	The comment defined in the column for Comment on the Safety Subsystem Comm. I/O Definition tab of Communication I/O Builder is displayed. This is based on the Device Tag for the signal definition in Safety Communication I/O Editor of AD Organizer.

Communication Data List view

The information of communication data wired to subsystem communication I/O FB or safety subsystem communication I/O FB is displayed for the communication modules selected in the Communication Module List view.

When the communication input line of a communication module is selected in the Communication Module List View, information of the communication data corresponding to the applicable input communication definition will be displayed.

When the communication output line of a communication module is selected in the Communication Module List View, information of the communication data corresponding to the applicable output communication definition will be displayed.

With S_SLSMOD, the subsystem communication program for the ProSafe-SLS communication function, communication data of the SLSEVENT data type can be defined. However, SLSEVENT is special data for event collection and cannot be wired to the subsystem communication function blocks. Accordingly, communication data of SLSEVENT data type are not displayed in the Communication Data List View and thus not locked or allow values to be set.

Table F8.11.1-14 Items displayed in Communication Data List view

Item	Description
Definition	Communication definition
%WB, or %XB	Element number
L	Lock status of communication data
D	Consistency/discrepancy of communication data
Instance	Instance name of the wired subsystem communication I/O FB
Logical Value	Logical data of data value and data status
Physical Value	Physical data of data value and data status
Set Value(*1)	Set value of data value and data status, respectively
Comment	Comment for the subsystem communication I/O FB

*1: Displayed and editable only when the SCS project target name is SCS_SIMULATOR.

Communication definition

The display items of the communication definition of the subsystem communication are as follows:

```
n-sConnectionDevice:c
Portp:DataType
```

Table F8.11.1-15 Display items of the communication definition of the subsystem communication

Item	Description
n	Node number
s	Slot number
ConnectionDevice	Communication program name S_MODBUS: For RTU mode Modbus communication S_MODTCP: For Modbus/TCP S_SLSMOD: For ProSafe-SLS communication
c	Communication definition number
p	Port number
DataType	Data type DI: Discrete input DO: Discrete output I16 Input: Analog input (16-bit signed integer) I32 Input: Analog input (32-bit signed integer) U16 Input: Analog input (16-bit unsigned integer) R32 Input: Analog input (32-bit floating) I16 Output: Analog output (16-bit signed integer) I32 Output: Analog output (32-bit signed integer) U16 Output: Analog output (16-bit unsigned integer) R32 Output: Analog output (32-bit floating)

TIP

Communication definition numbers specify communication definitions defined in one subsystem communication module. A "communication definition" is a block of data of the same data type specified by the "Size," among the data included in the "Buffer" assigned to each communication module specified by the "Program Name" in the Communication I/O Builder. Communication definition numbers are sequential numbers (starting from 1) assigned for each subsystem communication module.

The display items of the communication definition of the safety subsystem communication are as follows:

```
n-sConnectionDevice:AlarmInfo
DataType
```

Table F8.11.1-16 Display items of the communication definition of the safety subsystem communication

Item	Description
n	Node number
s	Slot number
ConnectionDevice	Communication program name S_FGCOM: For fire and gas communication
AlarmInfo	String of alarm information
DataType	Data type I8 Input: Analog input (8-bit signed integer) I16 Input: Analog input (16-bit signed integer) I32 Input: Analog input (32-bit signed integer) U8 Input: Analog input (8-bit unsigned integer) U16 Input: Analog input (16-bit unsigned integer) U32 Input: Analog input (32-bit unsigned integer) R32 Input: Analog input (32-bit floating)

Element number

- When %WBnnnnbb, nnnn is 2001 through 3000, bb is 01 through 16
- When %XBnnnnbb, nnnn is 0001 through 4000, bb is 01

Lock status of communication data

Table F8.11.1-17 Lock status display (L field)

LED	Meaning
(No symbol)	Communication data is not locked.
✶ (red)	Communication data is locked.
? (black)	Communication with the SCS is disabled.

Consistency/discrepancy of communication data

Discrete inputs and outputs are deemed to have "discrepancy" if the logical data and physical data of the data value or data status are different.

Analog inputs and outputs are deemed to have "discrepancy" if the logical data and physical data of the data status are different.

Table F8.11.1-18 Communication data consistency/discrepancy display (of D field)

Display	Meaning
(No symbol)	Communication data is consistent.
● (red)	Communication data has discrepancy.
? (black)	Communication with the SCS is disabled.

Instance name

The instance name of the subsystem communication I/O FB wired to %WB or the fire and gas communication I/O FB wired to %XB is displayed. The display and meaning of the instance name is as follows:

V: Data value

STS: Status

Logical data and physical data

For BOOL-type data, "TRUE" or "FALSE" is displayed. DINT-type data and REAL-type data are shown in the display format specified in the [Option] menu. The data status is displayed as either "GOOD" or "BAD". If communication with the SCS is disabled, "******" is shown.

Refreshing of communication data consistency/discrepancy, logical data and physical data display

How the consistency or discrepancy of each communication data is displayed, and how data values and statuses of logical data and physical data is refreshed, depend on the data acquisition mode.

- When the data acquisition mode is "All Modules"
  Data will be acquired sequentially from the communication definitions of all subsystem communication modules and fire and gas communication modules defined in the applicable SCS project. The display of the Communication Data List View will be refreshed once communication data is acquired.
- When the data acquisition mode is "Selected Modules"
  Data will be acquired sequentially from the communication definitions of the communication modules selected in the Communication Module List View. If only communication module inputs are selected, data will be acquired only from the input communication definitions. If only communication module outputs are selected, data will be acquired only from the output communication definitions. The display of the Communication Data List View will be refreshed once communication data is acquired.

Filtering

The communication data to be displayed can be filtered using the drop-down list box.

Table F8.11.1-19 Drop-down list box of Communication Data List view

Item	Operation
All Data	Information of all communication data is displayed.
Locked Data	Only information of locked communication data is displayed.
Unlocked Data	Only information of unlocked communication data is displayed.

Pop-up menu

Click the right mouse button on the Communication Data List View to display a pop-up menu. However, this is available only when the SCS project target name is SCS_SIMULATOR. The following menu items are displayed in the pop-up menu:

Table F8.11.1-20 Items on pop-up menu in the Communication Data List View

Menu item		Description
Cut		Same as [Cut] command on [Edit] menu.
Copy		Same as [Copy] command on [Edit] menu.
Paste		Same as [Paste] command on [Edit] menu.
Delete		Same as [Delete] command on [Edit] menu.
Select All		Same as [Select All] command on [Edit] menu.
Input Values ▶	Set .V=TRUE	Sets the data of Set Value to TRUE (only for DI/DO).
	Set .V=FALSE	Sets the data of Set Value to FALSE (only for DI/DO).
	Clear .V	Clears the data of Set Value.
	Set .STS=GOOD	Sets the data status of Set Value to GOOD.
	Set .STS=BAD	Sets the data status of Set Value to BAD.
	Clear .STS	Clears the data status of Set Value.

Selecting communication data

If the SCS project target name is SCS_SIMULATOR, you can select any communication data in the Communication Data List View.

- Clicking a communication data while pressing the [Shift] key on the keyboard, the communication data of the continuous lines can be selected.
- Clicking a communication data while pressing the [Ctrl] key on the keyboard, the communication data of the separated lines can be selected.
- Choosing [Select All] from pop-up menu, all communication data can be selected.

Message display area

The results of all data locking operations, all data unlocking operations and Forcing function operations are displayed as messages. The displayed messages are cleared each time a new operation is executed.

Status bar

The status bar shows the following information relating to the subsystem communication modules shown in the Communication Module List View.

- Input Selected: Number of selected input lines/number of all input lines
- Output Selected: Number of selected output lines/number of all output lines

F8.11.2 Operations in the Communication I/O Lock window

The following operations can be performed in the Communication I/O Lock window:

- Lock all input data and/or all output data for each subsystem communication module
- Unlock all input data and/or all output data for each subsystem communication module
- Set data values and data status for locked data
- Set all input data and/or all output data for each subsystem communication module (only in SCS Simulation Test).
- Lock or unlock all inputs of a fire and gas communication module
- Lock or unlock each communication definition (PROFINET module) connected to a fire and gas communication module

Performing an all lock or all unlock operation by selecting input and output of a given module will lock or unlock all subsystem communication data of the module.

You can also specify locked data and set values individually. A data value (V) is set for each communication data item, while a data status value (STS) is set for each communication definition.

In SCS Simulation Test, you can set values all together to the communication data for the communication modules.

IMPORTANT

- None of the previously mentioned operations can be executed during a build or download.
- If you select more than 20 PROFINET modules in the communication group list and try to perform an all lock or all unlock operation, an error will result.

Selection of communication modules and communication groups

A desired communication module can be selected in the Communication Module List view.

A desired communication group can be selected in the Communication Group List view.

- Selecting [Inputs/Outputs] in the drop-down list box will display communication definitions for all inputs and outputs.
- Selecting [Inputs] in the drop-down list box will display communication definitions for all inputs.
- Selecting [Outputs] in the drop-down list box will display communication definitions for all outputs.

When the following operations are performed, communication data is displayed in the Communication Data List view:

- Clicking an input line or output line of a communication module or communication group without pressing the [Shift] key or [Ctrl] key on the keyboard will display the communication data for the communication definitions of the communication module or communication group of the clicked line.
- Clicking an input line or output line of a communication module or communication group while holding down the [Shift] key on the keyboard will display the communication data for the communication definitions of the communication modules or communication groups of the lines between the line previously clicked (without holding down the [Shift] key) and the line clicked this time.

- Clicking an input line or output line of a communication module or communication group while holding down the [Ctrl] key on the keyboard will display the communication data for the communication definitions of the communication module or communication group of the clicked line, in addition to the communication data currently shown.
- Selecting [Select All] in the pop-up menu on the Communication List view will display communication data for the communication definitions of all communication modules currently shown in the Communication Module List view.

Locking all I/O of communication modules

Communication modules can be locked in the following units.

- All inputs of a communication module
- All outputs of a communication module
- All inputs and outputs of a communication module
  Inputs and outputs are specified at the same time.
- All inputs of a fire and gas communication module
- Lock of each PROFINET module connected to a fire and gas communication module
  A PROFINET module corresponds to a communication definition.

1. In the Communication Module List view, select the communication modules you want to perform "all lock" for.
2. In the Communication Data List view, check for discrepancy between the logical data and physical data of each data value and status of the selected subsystem communication module to confirm that locking will not cause any problems.
3. From the menu bar, select [Lock] > [Lock Modules]. Alternatively, click the [Lock] button on the toolbar.
   If you have selected more than 20 PROFINET modules in step 1, an error dialog box appears and the I/O of the modules will not be locked.

   If you have selected 20 or less PROFINET modules, a confirmation dialog box appears.
4. To execute the operation, click [OK].
   The selected inputs or outputs are locked at a time.

Unlocking all I/O of communication modules

This function unlocks all of the selected communication modules in a batch.

1. In the Communication Module List view, select the communication modules you want to perform "all unlock" for.
2. In the Communication Data List view, check for discrepancy between the logical data and physical data of each data value and status of the selected subsystem communication module to confirm that unlocking will not cause any problems.
3. From the menu bar, select [Lock] > [Unlock Modules]. Alternatively, click the [Unlock] button on the toolbar.
   If you have selected more than 20 PROFINET modules in step 1, an error dialog box appears and the I/O of the modules will not be unlocked.

   If you have selected 20 or less PROFINET modules, a confirmation dialog box appears.
4. To execute the operation, click [OK].
   The selected inputs or outputs are unlocked at a time if there is no discrepancy between the logical data and physical data for the communication data of the communication definitions of the target modules.

A reconfirmation dialog box appears if there is any discrepancy between the logical data and physical data for the communication data of the communication definitions of the target modules.

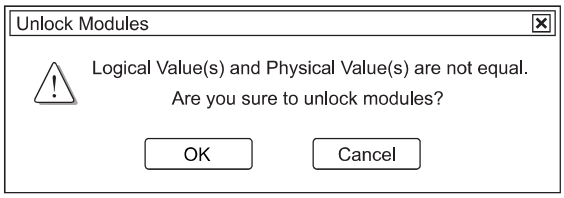


Figure F8.11.2-1 Unlock reconfirmation dialog box

5. Click [OK] to perform the unlock. To cancel the operation, click [Cancel].

Set value to each communication data

For each communication data, the value of data and data status can be set.

IMPORTANT

Setting values to communication data cannot be executed while Build or Download is running.

Double-clicking any field between "%WB" and "Physical Value" for locked data in the Communication Data List View will display the dialog box in which you can set the data value or status of the communication data in the clicked line.

If the upper part of the line showing a data value is double-clicked, the Write data value dialog box appears. If the lower part of the line showing a data status is double-clicked, the Write data status dialog box appears.

Set values in these dialog boxes. A data value is set for each communication data item, while a data status is set for each communication definition. Once a data status value is set, the value will be reflected in all data statuses within the same communication definition.

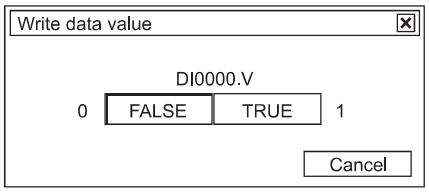


Figure F8.11.2-2 Write Data Value dialog box (discrete input/output)

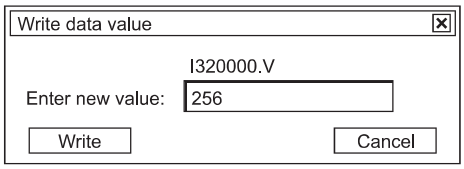


Figure F8.11.2-3 Write Data Value dialog box (analog input/output)

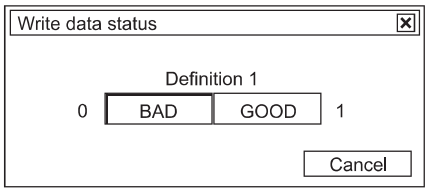


Figure F8.11.2-4 Write Data Status dialog box

When the Write data value dialog box or Write data status dialog box opens for a discrete input or output, the button corresponding to the current value is already selected.

With an analog input or output, the current value is displayed when the Write data value dialog box opens.

Whether logical data or physical data is displayed is determined based on which of the two values can be set at the time. Logical data is displayed if the logical data can be set, and physical data is displayed if the physical data can be set. The following table shows the default display for the dialog box.

Table F8.11.2-1 Initial displays of Write Data Value dialog box

Data	Initial display	
	Locked	Not locked
Input communication data: Data value	Logical data	Logical data
Input communication definition: Data status	Logical data	Logical data
Output communication data: Data value	Physical data	Logical data
Output communication definition: Data status	Logical data	Logical data

Set values to multiple items of communication data together

Using the SCS Simulator, you can set values to multiple communication data items together. The following batch operations can be performed for the communication data from the communication module selected in the Communication Module List View.

- Set values to the communication data.
- Save the set values for the communication data in a file.
- Read values form a file and set them to the communication data.

Note that the number of communication data values set at a time should be 700 or less. If more data values are set at a time, some of the system alarm messages informing the data setting or data status setting may not be transmitted.

Enter the values to be set to communication data

The values can be entered to the "Set Value" items on Communication data list view.
The value can be entered using any of the following operations. After entering the values, you need to set all the values to the communication data.

- Enter a Value Directly
  On Communication Data List View, click "Set Value" items on the line of the communication data that you want to enter the value for. By clicking the data value or data status, they can be entered directly.

  For BOOL type data, each click switches between TRUE, FALSE, and empty (nothing specified).

  For DINT or REAL type data, values can be entered directly from the keyboard.
- Edit multiple data values
  From [Edit] menu or from the pop-up menu after a right clicking, you can use [Cut], [Copy], [Paste] and [Del] commands to edit the values of multiple "Set Value" items.
- Entering values using [Input Values][Input values] on the pop-up menu.
  Right clicking on the Communication Data List View, a pop-up menu will be displayed. Using [Input Values] item on the pop-up menu, the data values and data status for "Set Value" items can be defined.

  For example, if you want to set all communication data to FALSE, you can use [Select All] command on the pop-up menu to select all "Set Value" items, and then you can choose [Set .V=FALSE] of the [Input Values] from the pop-up menu.

Set values to multiple communication data

For the selected communication modules, the values of "Set Value" items on the Communication Data List View can be set together to the communication data.

IMPORTANT

Setting values to communication data cannot be executed while Build or Download is running.

The procedure is as follows:

1. On Communication Module List View, choose a communication module that you want to set the values for.
2. Choose [Set Values] from [Lock] menu or click [Set Values] button on the toolbar so as to display Set Values dialog box.
3. Click [OK] for setting values.
   All the values entered in the "Set Value" items will be set to the communication data. If no values are entered, the communication data will not be changed.
   Click [Cancel] to cancel the operation.

Export the setting values to a file

The values for "Set Value" items of the communication data can be exported to a file.
The procedure is as follows:

1. Choose [Export Values] from [File] menu, or click the [Save (Export Values)] button on the toolbar
   so as to display a dialog box for selecting files.
2. Specify the CSV file for saving the setting values and then click [Save].
   The communication data values and data statuses for all the communication modules on the Communication Module List View will be exported to the file.

IMPORTANT

Do not edit the exported file if you want to import the file later.

Import the setting values from a file

The values for "Set Value" items of the communication data can be imported from a file.

IMPORTANT

Do not import any file other than the file exported from Communication I/O Lock window.

The procedure is as follows:

1. Choose [Import Values] from [File] menu, click the [Open (Import Values)] button on the toolbar
   so as to display a dialog box for selecting files.
2. Choose the CSV file that contains the setting values and then click [Open].
   The communication data values and data statuses of all the communication modules on the Communication Module List View will be displayed with the data values and data statuses imported from the file.

If the values of data statuses differ among communication data in the same communication definition in the CSV file, a warning message is displayed and the data status value of the first communication data in the same communication definition is set to all the communication data within the same communication definition.

F9. Software Configuration Viewer

Software Configuration Viewer is a tool that displays information related to the ProSafe-RS software installed on a PC. Software Configuration Viewer has the following functions.

- Displaying the system release number
- Displaying user names and company name
- Displaying the ID number (System ID license number)
- Displaying intellectual property rights, copyrights and registered trademarks included in the ProSafe-RS software
- Displaying the package names and number of licenses
- Displaying installation logs
- Displaying the program revisions
- Displaying registry information
- Printing information displayed in Software Configuration Viewer

SEE ALSO For more information about Starting Software Configuration Viewer, refer to:

"ProSafe-RS and ProSafe-RS Lite applications that can start from Start menu" in Read Me First (IM 32P01A30-01EN)

Tabs of Software Configuration Viewer

Software Configuration Viewer contains the following tabs.

- All
- Install Log
- Program Information
- Registry

IMPORTANT

The Registry tab is displayed only when you have logged on as an administrative user. It is not displayed when you have logged on as a non-administrative user.

Functions of the tabs in Software Configuration Viewer are explained as follows.

All tab

The All tab displays the following items.

- System release number
- User names and company name
- System ID license number
- Intellectual property rights, copyrights and registered trademarks included in the ProSafe-RS software

Install Log tab

The Install Log tab displays the history of installation tasks.

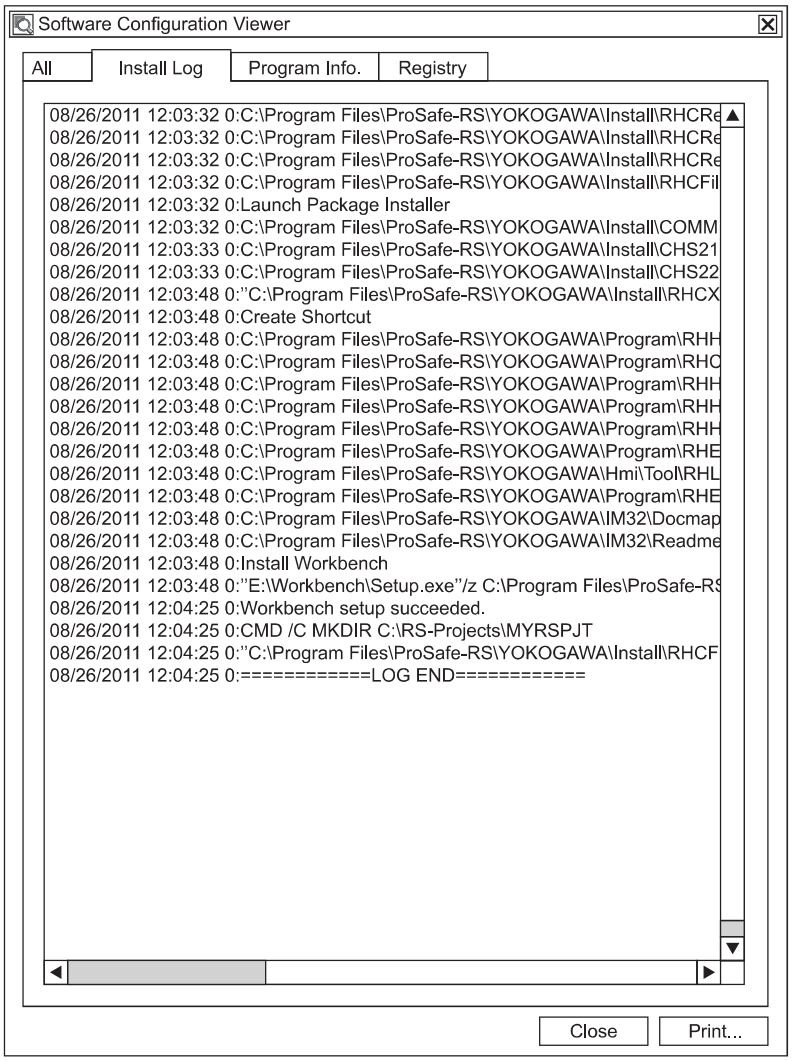


Figure F9-1 Example of Install Log tab

Program Info. tab

The "Program Info." tab displays the detailed information of the ProSafe-RS software installed in the PC. It displays the version information and creation dates of executable modules (*.exe), drivers (*.sys) and libraries (*.dll) of the ProSafe-RS software.

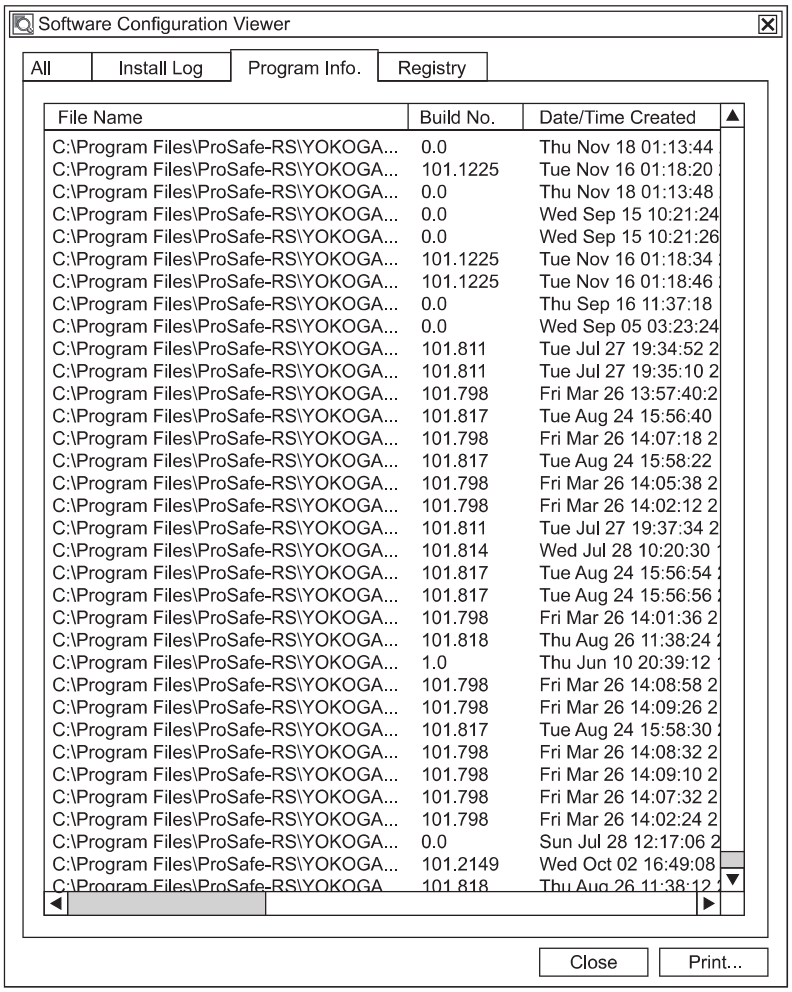


Figure F9-2 Example of Program Info. tab

The information about the Workbench and Multi-Language Editor is not available in "Program Info.". The following section explains how to display detailed information for Workbench and Multi-Language Editor.

1. In Workbench, select [Help] > [About].
   The About dialog box appears.
2. Click the [Info].
   Detailed information regarding Workbench and Multi-Language Editor is displayed.

Registry tab

The Registry tab displays names and values of registry entries set or used by the ProSafe-RS software.

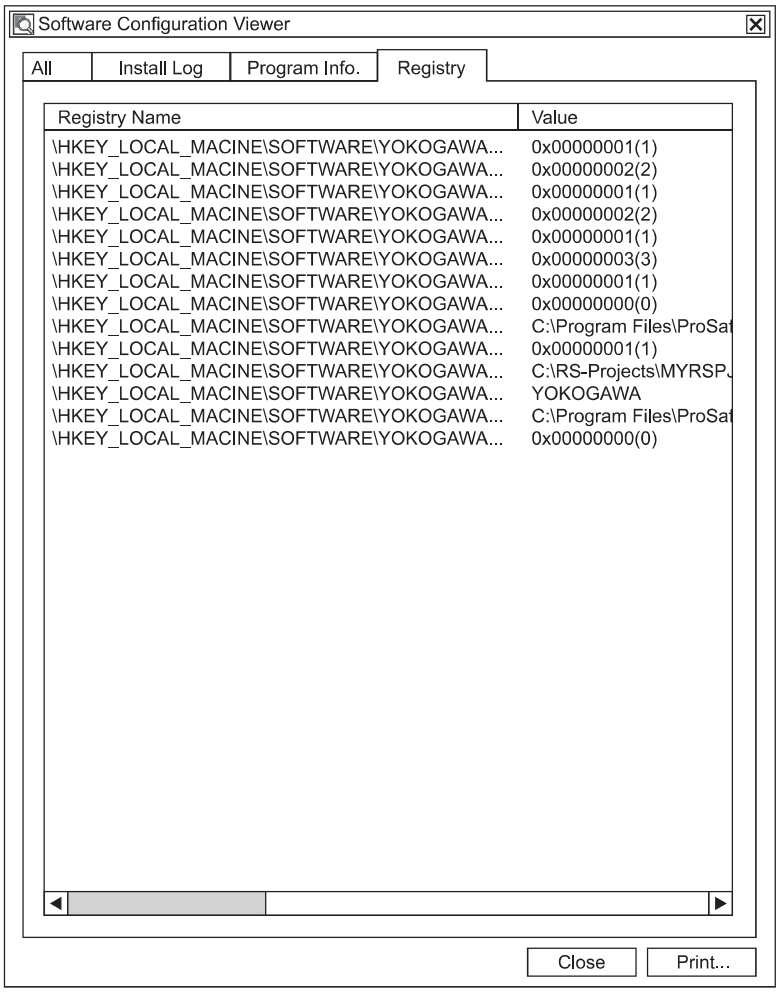


Figure F9-3 Example of Registry tab

IMPORTANT

The Registry tab is displayed only when you have logged on as an administrative user. It is not displayed when you have logged on as a non-administrative user.

Printing displayed information

It is possible to printout the information displayed in a tab through a printer by clicking the [Print] button on the tab.
The displayed information can be printed out with the following steps.

1. Click the [Print] button
   so as to open Create Report dialog box.

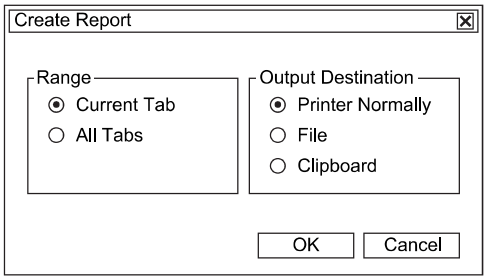


Figure F9-4 Create Report dialog box

2. Select one of the options in the "Range" section.
   By default, [Current Tab] is selected.
   - If you select [Current Tab], only the information displayed in the currently displayed tab is printed out.
   - If you select "All Tabs," the information displayed in all of the tabs is printed out in sequence.
     If you select [All Tabs], the information of the "Registry" tab will be printed out even if the current login user does not have the Administrator privilege.
3. Select one of the options in the "Output Destination" section.
   By default, [Printer Normally] is selected.
   - If you select [Printer Normally], the information is printed out through the default printer of the PC. On each page, the date and time of printing and a sequential page number starting from 1 are added as the header and footer respectively.
   - If you select [File], the Windows standard "Save As" dialog box will appear. Specify the file name and saving destination and save the information. The default file name and extension are "rssoft.txt."
   - If you select [Clipboard], the information will be copied to the clipboard. Then it is possible to paste the information into another application for editing.
4. If you selected [Printer Normally] or [Clipboard] for "Output Destination", click the [OK] button on the Create Report dialog box.
   Printing to the specified destination is started.

F10. Builder Environment Tool

Builder Environment Tool can be used for configuring builder font and other builder environment settings. This section describes how to use the Environment Setting window.

Target builders of Builder Environment Tool

This tool is used as required when customizing builder operations. The use of this tool is not mandatory. The target builders of this tool are shown below.

- SCS Constants Builder
- I/O Parameter Builder
- Tag Name Builder
- Alarm Priority Builder
- Alarm Processing Table Builder
- Modbus Address Builder
- Communication I/O Builder
- DNP3 Communication Builder

Note that settings made in this tool are not applied to SCS Manager and Multi-Language Editor.

Displaying Builder Environment Tool

Builder Environment Tool is opened by selecting [Environment Setting] in the [Tools] menu of each of the builders.
When the Environment Setting window is displayed, the builders of this tool cannot be operated on.

Click [OK] button to reflect the setting when starting up a builder.

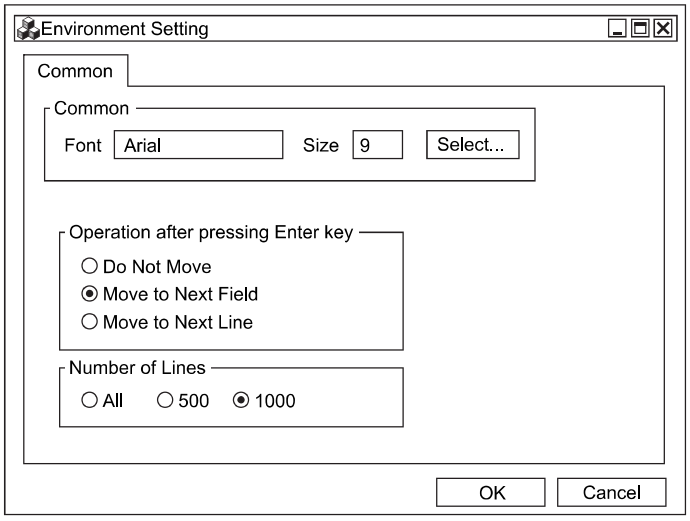


Figure F10-1 Environment Setting window

Common

This section allows setting font type and size for character strings displayed in the workspace. Click [Select] to display the following Font selection dialog box. Select a font type from [Font] and [Script], and specify the size as well. Note that [Font style] cannot be specified with this dialog box.

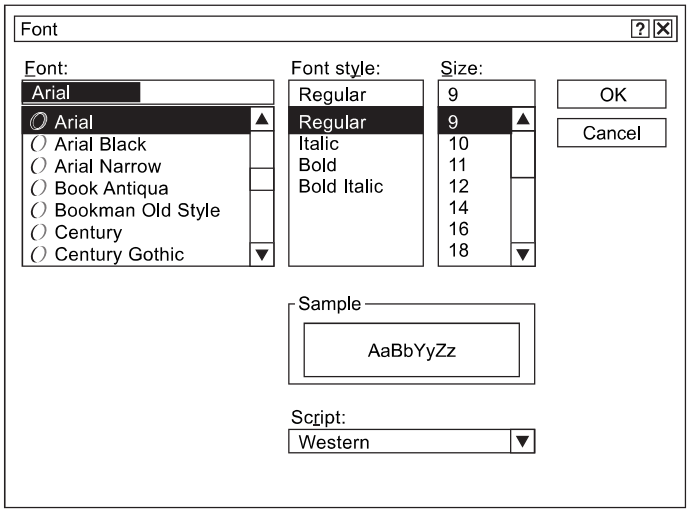


Figure F10-2 Font Selection dialog box

Operation after pressing Enter key

In this section, it is possible to specify the destination field that the cursor jumps to when the [Enter] key is pressed in spread-sheet type windows.

Table F10-1 Destination of the cursor

Item	Description
Do Not Move	Do not move the cursor
Move to Next Field	Move the cursor to the next field
Move to Next Line	Move the cursor to the next line

Number of lines

In this section, it is possible to specify the maximum number of lines that can be displayed in the document window. This setting is applied to Comm. I/O Wiring Tab of Communication I/O Builder and Modbus Address Builder.

If [All] is selected, the maximum number of displayed lines of the builder will be set as the maximum number of lines for each tab. If another value is specified, the value is set as the maximum number of displayed lines. If more lines than the maximum number of displayed lines are to be displayed, a page switch button is displayed on the upper part of the tab.

For example, if 1000 is specified for the maximum number of display lines in a tab that displays 4000 lines, four page switch buttons are displayed.

The default value is 1000.

Revision information

Title : Engineering Reference Manual

Manual No. : IM 32P04B10-01EN

Nov. 2022/9th Edition/R4.08 or later

F1	Added precautions when building.

Jan. 2022/8th Edition/R4.07

C1.1	Added descriptions of password change.
F8.7	Updated the reference of POU Reference Manual.

Feb. 2021/7th Edition/R4.06

Introduction	Added description of Full Names and Simplified Terms.
B3.1.5	Added descriptions of Work Status List window.
B4.2	Added descriptions of automatic check-out/check-in.
B4.3.4	Added column operations.
B4.4	Added descriptions of the common grid rule function, Match Case Type Options, and Match Text Type Options. Changed the number of condition and action definitions to 20. Changed the number of columns that can be changed simultaneously at grid rule execution to 10 columns. Added regular expression usage examples.
C2.9.1	Added descriptions of filtering by range and dates of Change Sets.
C2.9.3	Added descriptions of how to display a list view and detail view of files.
F1, F8	Added SCSL2 to station type.
F8.8.1	Added L1EC402 and L1EC401ESB to the model name of ESB bus coupler module.
F8.11	Added L1SC70 to SCS type.

Dec. 2019/6th Edition/R4.05

Introduction	Updated the description of registered trademarks and trademarks.
A1	Updated the term definitions of I/O list engineering and RS original engineering.
A4, B1, B3.1.1, B3.2, C1.2.2	Added descriptions of the Safety I/O parameter profile.
B4.3	Added descriptions related to the change of display method of AD Organizer.
B4.3.1	Updated descriptions of the search function of AD Organizer.
B4.3.2	Added descriptions of the sort function of AD Organizer.
B4.3.3	Added descriptions of the filter function of AD Organizer.
C1.1.5	Updated descriptions of restoring RS projects.
C1.2.2	Updated descriptions of user roles and access scopes.
F4	Updated descriptions of the procedures for using Master Database Restoring function.
F5.4	Updated descriptions of the procedures for using Version Control Tool.

Aug. 2018/5th Edition/R4.04

Introduction	Updated the description of registered trademarks of YOKOGAWA.

A1	Changed explanations due to changing the SCS Manager start-up method.
A1, B3.1.1, B3.1.2, B3.1.6, B4.3, B4.4	Updated the figure due to adding the SCS Manager start-up button.

Oct. 2017/4th Edition/R4.03.10

Introduction	Added the fire and gas communication module to the description of a term.
A4	Updated application capacity of AD Suite.
B3.1.1, B3.2, B4.2.1, C1.2.2, C2, F1	Added Safety Communication I/O Editor.
B4.4	Added descriptions of grid rule definitions.
C1.2.2	Added descriptions of access rights when the AD server is upgraded.
F1	Updated descriptions to support Safety Communication I/O Editor, and added items displayed on the CENTUM Integration tab.
F2.2, F2.4	Added fire and gas communication definitions and the wiring information as printing targets.
F4, F5	Added descriptions of how to start the tool and differences in behavior.
F5.3, F5.4	Updated descriptions of checking in and checking out project data.
F5.7	Added descriptions of version information.
F6.2, F6.3	Added descriptions of the display of Project Comparing Tool.
F8	Added and updated descriptions of the forcing function. Added new function blocks.
F8.7	Added forcing functions for safety subsystem communication data.
F8.11	Added and updated descriptions of the Communication I/O Lock window.

May 2017/3rd Edition/R4.03

Introduction	Deleted "Windows Vista" from the description of trademarks.
A3	Changed examples of system configurations.
C1.1.7	Changed explanations for ADMDB backup settings and procedures.
C1.2.3	Changed explanations for AD project export settings and procedures.
F6.3	Changed explanations for procedures and adding setting items of the Project comparing tool and changed explanations for examples of printouts.

Oct. 2016/2nd Edition/R4.02

Entire manual	Changed the symbols that indicate warning and caution.
Introduction	Updated descriptions in "■ Safety, Protection, and Modification of the Product," "■ Symbols," and "■ Trademark Acknowledgments." Added a new term in "■ Full Names and Simplified Terms."
A1, B1, B3.1.1, B4.2.2, C1.2.2, C2.1, D1, F2, F5.4, F7, F8, F8.1, F8.3	Added explanations on iDefine
Part B to Part D	Updated screen captures related to iDefine.
C2.8	Updated explanations on label configurations.
D2.5	Changed the title.
D2.7	Added explanations on the test function.

F2 Added explanations on AD Organizer.

Dec. 2015/1st Edition/R4.01

Newly published

■ For Questions and More Information Online Query: A query form is available on the following URL for online query. http://www.yokogawa.com/iss
■ Written by Yokogawa Electric Corporation
■ Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Attachment 9.10 Test Function Guide

IM32P03B30-01EN

General Specifications

GS 32P03B30-01EN

Model RS4F1500
Safety Control Function (for S2SC70☐)
Model RS4F1505
Safety Control Function for SCS Simulator
(for S2SC70☐)

ProSafe-RS

■ GENERAL

*Safety Control Function is a software package that works on a Safety Control Station (SCS). (*1) The Safety Control Function is to monitor a plant and ensure its safe operation. This software package performs preset safety operations whenever safety control is required.*
RS4F1500 Safety Control Function (for S2SC70☐) is applied to S2SC70☐ Safety Control Unit (for Vnet/IP, N-IO/FIO, Rack Mountable Type). The test functions can be performed by using RS4F1500, or under the virtual test environment where the SCS is not connected, RS4F1505 Safety Control Function for SCS Simulator (for S2SC70☐) can also be used.

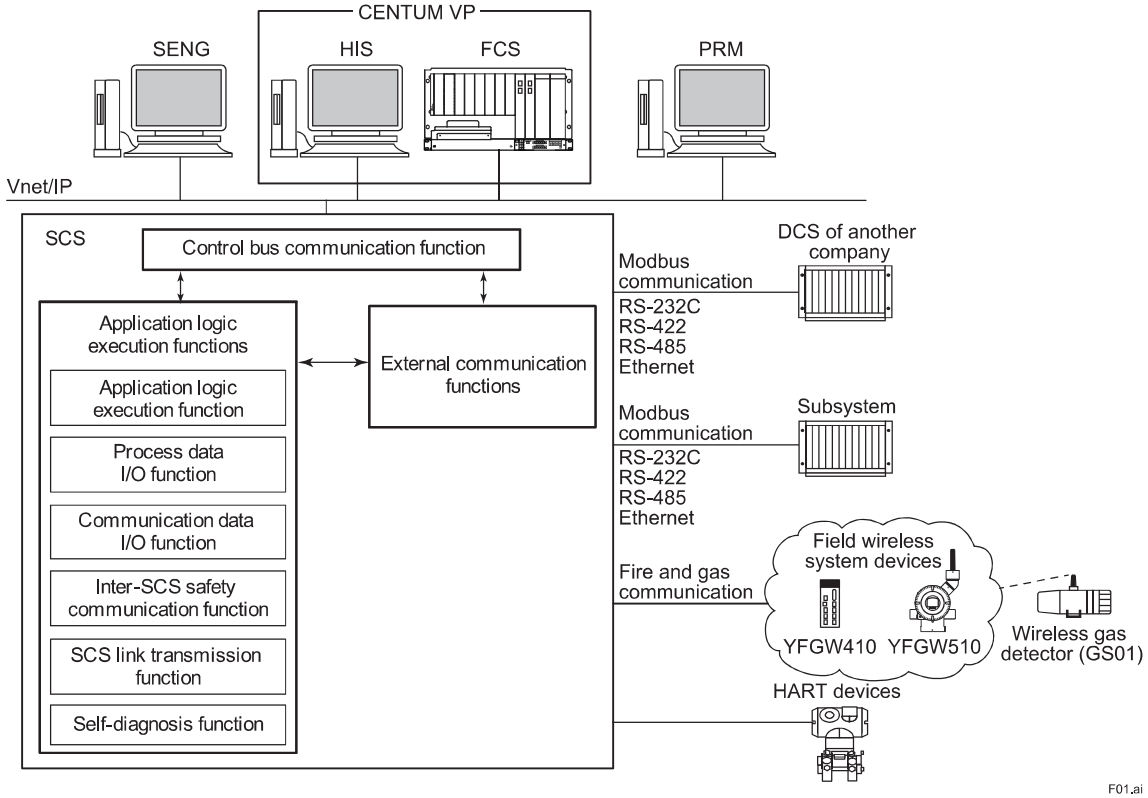
*1: The SCS is composed of a safety control unit, N-IO nodes, and safety node units.

■ FUNCTIONAL SPECIFICATIONS

The following describes the configuration and functions of the package are described as follows:

● Configuration of RS4F1500 Safety Control Function

The functions of the package can be divided into two groups: one is an application logic execution functions group and the other is an external connection functions group.



Application Logic Execution Functions

The following functions compose of the main part of the package that monitors the plant and ensures its safe operation, and performs preset safety operations once an abnormality occurs.

- Application logic execution function
- Process data I/O function
- Communication data I/O function (Subsystem communication function)
- Inter-SCS safety communication function
- SCS link transmission function
- Self-diagnosis function

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

GS 32P03B30-01EN
©Copyright Nov. 2015 (YK)
4th Edition July 24, 2018 (YK)

External Communication Functions

This function group, which performs communications between the application logic execution functions and non-SCS equipment, is composed of the following functions:

- CENTUM VP integration function
- Modbus communication function
- Fire and gas communication function
- Sequence of events recorder (SOER) function
- Diagnosis information collection function
- PRM-supported HART on-demand communication

● Application Logic Execution Functions

Details of Application logic execution function, Process data I/O function, Inter-SCS safety communication function, and SCS link transmission function are given below.

Application logic execution function

Application logics are described by using the Function Block Diagram (FBD), the Ladder Diagram (LD), or Structured Text (ST) compliant to the IEC 61131-3 standard.

The following table shows the functions and function blocks used in the FBD. Some of the elements from LD can also be used to describe FBD.

Table Safety Functions (FU) (1/2)

Function	Details
ABS	Gives the absolute (positive) value of a real value
SQRT	Calculates the square root of a real value
+ADD	+, meaning “addition”
× MUL	×, meaning “multiplication”
–SUB	–, meaning “subtraction”
/ DIV	/, meaning “division”
SHL	Make the bits of an integer shift to the left. Shift is made on 32 bits. Zero is used to replace lowest bit.
SHR	Make the bits of an integer shift to the right. Shift is made on 32 bits. Highest bit is copied at each shift.
ROL	Make the bits of an integer rotate to the left. Rotation is made on 32 bits.
ROR	Make the bits of an integer rotate to the right. Rotation is made on 32 bits.
AND	AND
OR	OR
XOR	Exclusive disjunction (exclusive OR)
NOT	Negation
SEL	Selects one of two input values (INTEGER)
SEL_R	Selects one of two input values (REAL)
SEL_T	Selects one of two input values (TIME)
MAX	Selects the larger of two input values (INTEGER)
MIN	Selects the smaller of two input values (INTEGER)
LIMIT	Limits the range of the input values to output (INTEGER)
MUX4	Selects one of four input values (INTEGER)
MUX8	Selects one of eight input values (INTEGER)
MUXBOOL4	Selects one of four input values (BOOL)
MUXBOOL8	Selects one of eight input values (BOOL)
MUXREAL4	Selects one of four input values (REAL)
MUXREAL8	Selects one of eight input values (REAL)
GT	>, meaning “greater than”
GE	>=, meaning “greater than or equal to”
EQ	=, meaning “equal”
LE	<=, meaning “less than or equal to”
LT	<, meaning “less than”
NE	≠, meaning “unequal”
SCALER	Converts a 0-100 % range of input values into a normalized range for outputting

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Table Safety Functions (FU) (2/2)

Function	Details
1GAIN	Assignment
IB_TO_V	Converts IO_BOOL-type input to data value
IB_TO_S	Converts IO_BOOL-type input to data status
IR_TO_V	Converts IO_REAL-type input to data value
IR_TO_S	Converts IO_REAL-type input to data status

Table Interference-free (*1) Functions (FU)

Function	Details
ANY_TO_BOOL	Converts to BOOL-type
ANY_TO_DINT	Converts to INTEGER-type
ANY_TO_REAL	Converts to REAL-type
ANY_TO_TIME	Converts to TIME-type
POW	Performs power calculation
POWE	Performs calculation of exponential function with base e
ACOS	Calculates the Arc cosine of a real value
ASIN	Calculates the Arc sine of a real value
ATAN	Calculates the Arc tangent of a real value
COS	Calculates the Cosine of a real value
SIN	Calculates the Sine of a real value
TAN	Calculates the Tangent of a real value
LOG	Calculates the Common logarithm of a real value
LOGE	Calculates the Natural logarithm of a real value
MOD	Calculates the Modulo of an integer value

*1: Functions not affecting the safety loop

Table Safety Function Blocks (FB) (1/3)

Function block	Details
SR	Set dominant bistable
RS	Reset dominant bistable
R_TRIG	Detects a rising edge
F_TRIG	Detects a falling edge
CTU	Count up counter
CTD	Count down counter
CTUD	Count up/down counter
TP	Pulse timer which outputs pulses for a specified duration after rising edge detection
TON	On-delay timer
TOF	Off-delay timer
REPEATTIMER	Alternates TRUE and FALSE outputs at specified intervals
FILTER	First-order lag filter
FILTER_S	First-order lag filter with data status analysis capability
ANLG1OO2D	1oo2D analog voter
ANLGVOTER	3-input analog voter (IO_REAL)
BOOLVOTER	3-input BOOL voter (IO_BOOL)
ANLG_S (*1)	Outputs high/low alarm with scale conversion (with data status input)

*1: When the ProSafe-RS system is integrated with CENTUM VP, these function blocks can be used by the HIS of CENTUM VP.

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Table Safety Function Blocks (FB) (2/3)

Function block	Details
ANLGI (*1)	Outputs high/low alarm with scale conversion
VEL (*1)	Detects the velocity limit exceeded
SYS_STAT	Manages the SCS status
SYS_FORCE	Manages forcing
SYS_DIAG	Outputs diagnosis information
SYS_SECURE	Manages Security level
SYS_SEC_CTL	Protects Security level
SYS_IOALLST	Detects fault in all I/O channels
SYS_NODEST	All I/O Channels of FIO Node Status Indicator
SYS_N_NODEST	All I/O Channels of N-IO Node Status Indicator
SYS_OUTST	FIO Output Module 8 Channels Indicator
SYS_OUTST16	FIO Output Module 16 Channels Indicator
SYS_INST	FIO Input Module Status Indicator
SYS_CHST	Status Indicator of FIO Module Channel
SYS_N_IOST16	N-IO I/O Module 16 Channels Indicator
SYS_CERR	Indicates computation errors
SYS_SCANEXT	Indicates the extension of scan period
SYS_OVR	Manages override function blocks
SYS_PSWD	Manages password function blocks
SYS_OUTEN	FIO Output Module Output Status Indicator
SYS_N_OUTEN	N-IO I/O Module Output Status Indicator
SYS_ALLSD	Shuts down Station output
SYS_IOSD	FIO Output Module Output Shutdown
SYS_N_IOSD	N-IO I/O Module Output Shutdown
SYS_FORCE_BD	Manages forcing of inter-SCS safety communication data
SYS_FORCE_LT	Manages forcing of SCS Link Transmission
SYS_LTSTS	Indicates SCS Link Transmission reception status
GOV_B (*1)	Grouping overrides from HIS (BOOL)
GOV_IB (*1)	Grouping overrides from HIS (IO_BOOL)
OVR_B (*1)	Overrides from HIS (BOOL)
OVR_I (*1)	Overrides from HIS (INTEGER)
OVR_R (*1)	Overrides from HIS (REAL)
OVR_IB (*1)	Overrides from HIS (IO_BOOL)
OVR_IR (*1)	Overrides from HIS (IO_REAL)
PASSWD (*1)	Manipulates BOOL-type data using password from HIS
MOB_11 (*1)	Data manual operation with two-position answerback (BOOL)
MOB_21 (*1)	Data manual operation with three-position answerback (BOOL)
MOB_RS (*1)	Auto-reset data manual operation (BOOL)
MOA (*1)	Analog-type data manual operation
CONS_B	Receives data on consumer side for inter-SCS safety communication (BOOL)
CONS_I	Receives data on consumer side for inter-SCS safety communication (INTEGER)
CONS_R	Receives data on consumer side for inter-SCS safety communication(REAL)
PROD_B	Transmits data on producer side for inter-SCS safety communication (BOOL)
PROD_I	Transmits data on producer side for inter-SCS safety communication (INTEGER)

*1: When the ProSafe-RS system is integrated with CENTUM VP, these function blocks can be used by the HIS of CENTUM VP.

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Table Safety Function Blocks (FB) (3/3)

Function block	Details
PROD_R	Transmits data on producer side for inter-SCS safety communication (REAL)
B_TO_IB	Converts data values and status to IO_BOOL-type outputs
R_TO_IR	Converts data values and status to IO_REAL-type outputs
LTRCV	Receives Safety Link Transmission data
LTSND	Sends Link Transmission data
ANN_FUP (*1)	Detects the first-up alarm and transmits the annunciator message
FUP_RST	Resets the first-up alarm annunciator
HSDTR (*1) (*2)	Outputs high alarm of smoke and heat detector with scale conversion (with reset function)
GASDTR (*1) (*2)	Outputs high/low alarm of gas and flame detector with scale conversion (with reset function)
PSI_I (*3)	Fire and gas communication input (INTEGER)
PSI_R (*3)	Fire and gas communication input (REAL)
SCS_FORCE_SF (*3)	Manages forcing of fire and gas communication data

*1: When the ProSafe-RS system is integrated with CENTUM VP, these function blocks can be operated and monitored by the HIS of CENTUM VP.
*2: Supported by ProSafe-RS R4.03.00 or later.
*3: Supported by ProSafe-RS R4.03.10 or later.

Table Interference-free (*1) Function Blocks (FB) (1/2)

Function block	Details
ANN (*2)	Transmits annunciator message
SYS_SCAN	Outputs application logic execution time and percentage of CPU idle time
SYS_IOMDSP	FIO Module Status Indicator
SYS_N_IOMDSP	N-IO Module Status Indicator
SYS_NODEINF	FIO Node Status Indicator
SYS_N_NODEINF	N-IO Node Status Indicator
SYS_ESBINF	Outputs ESB bus status
SYS_NETST	Outputs Control bus status
SYS_ALRDSP	Outputs status of subsystem communication modules
SYS_ALARM	Outputs alarm transmission status
SYS_TIME	Outputs SCS clock information
SYS_FORCE_SC	Manages forcing of subsystem communication data
SYS_STAT_SC	Indicates output enable operation in subsystem communication
SOE_B	BOOL-type data SOER
SOE_I	INTEGER-type data SOER
SOE_R	REAL-type data SOER
ECW_B (*2)	Sets data of a BOOL-type variable from an external device
ECW_I (*2)	Sets data of a INTEGER-type variable from an external device
ECW_R (*2)	Sets data of a REAL-type variable from an external device
AVERAGE	Calculates the average of a specified duration
LIM_ALRM	Hysteresis on a real value for high and low limits
SCI_B (*2)	Input from subsystem (BOOL)
SCI_I (*2)	Input from subsystem (INTEGER)
SCI_R (*2)	Input from subsystem (REAL)
SCO_B (*2)	Output to subsystem (BOOL)
SCO_I (*2)	Output to subsystem (INTEGER)

*1: Functions not affecting the safety loop.
*2: When the ProSafe-RS system is integrated with CENTUM VP, these function blocks can be used by the HIS of CENTUM VP.

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Table Interference-free (*1) Function Blocks (FB) (2/2)

Function block	Details
SCO_R (*2)	Output to subsystem (REAL)
LTFCS	Receives Interference-free Link Transmission data
SYS_SETTIME	Sets the SCS time
SYS_PSUDSP	PSU Status Indicator
PNI_I (*3)	PROFINET communication input (INTEGER)
PNI_R (*3)	PROFINET communication input (REAL)

*1: Functions not affecting the safety loop.
*2: When the ProSafe-RS system is integrated with CENTUM VP, these function blocks can be used by the HIS of CENTUM VP.
*3: Supported by ProSafe-RS R4.03.10 or later.

Table Ladder Elements

Ladder	Details
Direct Contact	Direct contact
Inverted Contact	Inverted contact
Contact with Rising Edge Detection	Contact with rising edge detection
Contact with Falling Edge Detection	Contact with falling edge detection
Direct Coil	Direct coil
Inverted Coil	Inverted coil
SET Coil	SET coil
RESET Coil	RESET coil
Coil with Rising Edge Detection	Coil with rising edge detection
Coil with Falling Edge Detection	Coil with falling edge detection

Scan period of Application Logic Execution Function

50 milliseconds – 1 second (by the unit of 10 – milliseconds within these ranges)

Process Data I/O Function

For process data I/O function, analog I/O modules and digital I/O modules are used. The table below shows the I/O modules that SCSs can employ.

Table I/O Modules

Model	Module Name
SAI143	Analog input module (4 to 20 mA, 16-channel, module isolation)
SAV144	Analog input module (1 to 5 V/1 to 10 V, 16-channel, module isolation)
SAT145	TC/mV input Output (16-channel, isolated channels)
SAR145	RTD input module (16-channel, isolated channels)
SAI533	Analog output module (4 to 20 mA, 8-channel, module isolation)
SDV144	Digital input module (16-channel, dry contact, module isolation)
SDV521	Digital output module (4-channel, 24 V DC/2 A, module isolation)
SDV526	Digital output module (4-channel, 100-120 V AC, module isolation)
SDV531	Digital output module (8-channel, 24 V DC, module isolation)
SDV53A	Digital output module (8-channel, 48 V DC, module isolation)
SDV541	Digital output module (16-channel, 24 V DC, module isolation)
S2MMM843	Analog Digital I/O Module (for N-IO) (16-channel, module isolation)
S2MDV843 (*1)	Digital I/O module (for N-IO) (16-channel, module isolation)

*1: Supported by ProSafe-RS R4.03.00 or later.

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Table Safety Subsystem Communication Modules

Model	Module Name
S2LP131 (*1)	Fire and Gas communication module (1-port)

*1: Supported by ProSafe-RS R4.03.10 or later.

Table Interference-free (*1) Communication Modules

Model	Module Name
ALR111	Serial communication module (RS-232C, 2-port)
ALR121	Serial communication module (RS-422/RS-485, 2-port)
ALE111	Ethernet communication module (1-port)

*1: I/O modules that do not affect the safety loops

Inter-SCS Safety Communication Function

When the inter-SCS safety communication function is employed, a safety loop up to SIL 3 (Safety Integrity Level) can be configured among multiple SCSs via the Vnet/IP. This function ensures authenticity, quality, appropriate sequence, and timelines of the data.

Communication Specifications:

- An SCS is capable of communication up to 16 SCSs. (*1)
- Up to 200 data items can be transmitted per SCS.
- Up to 200 data items can be received per SCS.

*1: In case the SCS performs bi-directional communications or a multiple communications, the number of SCSs becomes less than 16.

For the compatibility of Inter-SCS safety communication by the release numbers of the system programs, refer to the GS “ProSafe-RS Safety Instrumented System Overview (for Vnet/IP)” (GS 32P01B10-01EN).

SCS Link Transmission

Two types of SCS link transmissions are available - SCS Link Transmission Safety Communication and SCS Global Switch Communication.
The SCS Link Transmission Safety Communication is the SIL 3-supported safety communication function to simultaneously transmits data to multiple number of SCSs in a periodic interval. It also receives the data transmitted by other stations and refers them by the application logic.
The SCS Global Switch Communication enables to refer the data transmitted between the SCS and the FCS.
This function is interference-free.

Communication Specifications:

- Communication range: Within to the same domain
- Control bus: Vnet/IP
- Number of communicable stations: Maximum 63
  (The number of stations that can be referred to, depend on the CPU and communication loadings)
- Transmission cycle: 100 ms fixed

Transmission Data Reference/Setting:

- Number of input function block definition: Max. 1000 per SCS
- Number of output function block definition: Max. 128 per SCS
- The number of assignments per receiving station is not limited

Software Requirements:

SCS program: R4.01.00 or later
FCS system program: R3.08.50 or later

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

● External Connection Functions

The CENTUM VP integration function, Modbus communication, sequence of events recorder (SOER), and diagnosis information collection functions are described below:

Scan period of External Connection Function

1 or 2 seconds.

CENTUM VP Integration Function

The SCS can be monitored by CENTUM VP's human interface station (HIS) using the tag name interface in the same way as control tags. When the tag name is defined using the CENTUM VP integration function, the HIS is enabled not only to monitor the SCS but also to perform maintenance override. Annunciator messages assigned with priority levels can be sent from the SCS.

As for the types of SCS data and function blocks to assign tag names, refer to the GS "CENTUM VP Integration Package" (GS 32P04D10-01EN).

Modbus Communication Function

The SCS communicates with external equipment such as sequencers via the Modbus protocol. The SCS acts as the Modbus master which enables to read and write external equipment data. The external equipment also acts as the Modbus master which enables to read and write the SCS data. Connecting with the Modbus communication module is interference-free. ALR121 serial communication module supports ProSafe-SLS communication function which extends the Modbus communication function.

For more details, refer to the GS "ALR111/ALR121 Serial Communication Module" (GS 32P06K50-01EN) or "ALE111 Ethernet Communication Module" (GS 32P06K51-01EN).

Modbus communication function / Communication module	SCS acts as a Modbus master	SCS acts as a Modbus slave
Serial communication module	X	X
Ethernet communication module	X	X

X: Supported

Fire and Gas Communication Function (*1)

SCS acquire the data of wireless gas detector (GS01) using the fire and gas communication function via S2LP131 fire and gas communication module mounted on SCS and field wireless system comply with the ISA100.11a standards. Safety subsystem communication function handles a safety data used in a safety loop and a non-safety data used in an interference-free function. For details of fire and gas communication module, field wireless system, and wireless gas detector, refer to the GS "S2LP131 Fire and gas Communication Module" (GS 32P06K52-01EN).

*1: Supported by ProSafe-RS R4.03.10 or later.

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

● Sequence of Events Recorder (SOER) Function

The SOER function is composed of event collection sub-function, event storage sub-function, and time synchronization sub-functions. When an SOE viewer is used on the CENTUM VP's HIS, the event information can be displayed on the HIS.

- Event collection and storage sub-function
  Event information is collected and stored in a digital input module or a CPU module of an SCS. (*1)
  Time stamp resolution of events collected by a digital input module is 1 ms. (*2)
  Other events are collected by a CPU module by the SCS's scan period as the time stamp resolution.
- Objective event information
  The SCSs collects the following event information when defined by the user definition.

*1: Digital Input Module is a general term of SDV144 Digital Input Module and the channels of defined for digital input by S2MDV843 Digital Input/Output Module or S2MMM843 Analog Digital Input/Output Module.

*2: When utilizing a I.S. barrier for DI, the barrier's delay time is added on to its response time. For details, refer to the I.S. barrier for DI specifications provided by the vendor.

Information to be collected	Trigger for event collection and location for collection
Digital input	Changes in the data value input into the digital input module trigger to collect events. The SOE collection can be enabled or disabled by the channel. (*1) (*3)
Digital output	Changes in the data value output to the digital output module trigger CPU to collect events. The SOE collection can be enabled or disabled by the channel. (*2) (*3)
Analog input	The analog input function block determines the level of the data value to collect events. (*4)
Application logic variable	Each of the SOE event collection function blocks for BOOL-type, INTEGER-type, and REAL-type collects events. (*4)

*1: When the digital input module is dual-redundant, the module with control authority collects events.
*2: When the status of output channel is abnormal (the data status is BAD), no events are collected.
*3: Channel comments (a string composed of a maximum of 32 single-byte characters or 16 double-byte characters) needs to be defined.
*4: A sequential event identifier (a string composed of maximum of 32 single-byte characters or 16 double-byte characters) needs to be defined for the input terminal ID of a function block. Analog output events are to be collected by a function block for SOE event collection for constants.

- Storage of Event Information
  Event information is stored in an event information file in an SCS. Such event information can be seen from multiple SOE viewers.
  Two kinds of event information files are provided – an event log file and a trip signal file. The event log file contains collected event data. The trip signal file contains events before and after a trip signal specified by a user.

Table Event Information File Specification

	Event log file (*1)	Trip signal file (*2)(*3)
Number of events	Max. 15000 events	Max. 1500 events (500 before signal generation and 1000 after signal generation)
Number of files	Max. 1	Max. 2

*1: A diagnosis information message is sent to the user at occurrence of every 12000 events.
*2: Upon completion of collecting trip signal file, a diagnosis information message is sent to a user.
*3: In case the number of events does not reach 1000 in 30 minutes after the trip signal is generated, a trip signal file creation is terminated and a diagnosis information message is sent to a user.

Diagnosis Information Collection Function

An SCS sends a diagnosis information message when an abnormal condition is detected, and the message is stored in the memory of the SCS as the diagnostic information. The message contains the time, location, type, and other information of the abnormality. The SCS can store up to 5000 pieces of information.

PRM-supported HART On-demand Communication

On-demand communication with a HART device is implemented by Plant Resource Manager (PRM) which sends a HART command, and then receives a response from the HART device via the SCS. Analog input/output modules with HART function (SAI143-H and SAI533-H) and Analog Digital I/O modules (S2MMM843) serve as communication relays.

Enhancement of HART function

In the communication among wired-HART devices using Analog Digital I/O Modules (S2MMM843), HART 7 the latest protocol is supported, which enables the S2MMM843 to receive event notification (notifications of change in HART 7 device status).

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

● Test Function

The test function supports performance tests of the user-made applications. Three test modes are available: “target test” employs the actual systems in operation; “virtual test” (SCS simulation test) uses the SCS simulator; and “logic simulation test” uses the logic simulator.

The CENTUM VP test functions and ProSafe-RS test functions constitute the virtual test environment. For details of the CENTUM VP test functions, refer to the GS of CENTUM VP “Test Function” (GS 33J10D50-01EN). Under the virtual test environment, either RS4F1500 safety control function (for S2SC70☐) or RS4F1505 safety control function for SCS simulator (for S2SC70☐) can be used. (*1)

*1: CENTUM VP R6.02 or later is required.

SCS Simulator

The SCS simulator activates the SCS system software that works on the SCS on a computer. Communications with virtual HIS, with FCS simulator, and safety communications among the SCSs can be performed just by the computer.
For operator training, Exatif (*1) DCS interface for training simulator can be used.

*1: Exatif is a product of Omega Simulation Co., Ltd. For the details of its function, refer to the General Specification (GS) issued by Omega Simulation Co., Ltd.

● Connecting to Plant Training System (using Exatif Package)

The Vnet/IP interface to constitute the environment for plant training simulator is supported.

In order to stabilize the performance for longer hours than using it as a test function, configuring the simulator with a following system configuration is required.

For more details, please refer to the GS of CENTUM VP “Expanded Test Functions, FCS Simulator Package, HIS Simulator Package” (GS 33J10D60-01EN).

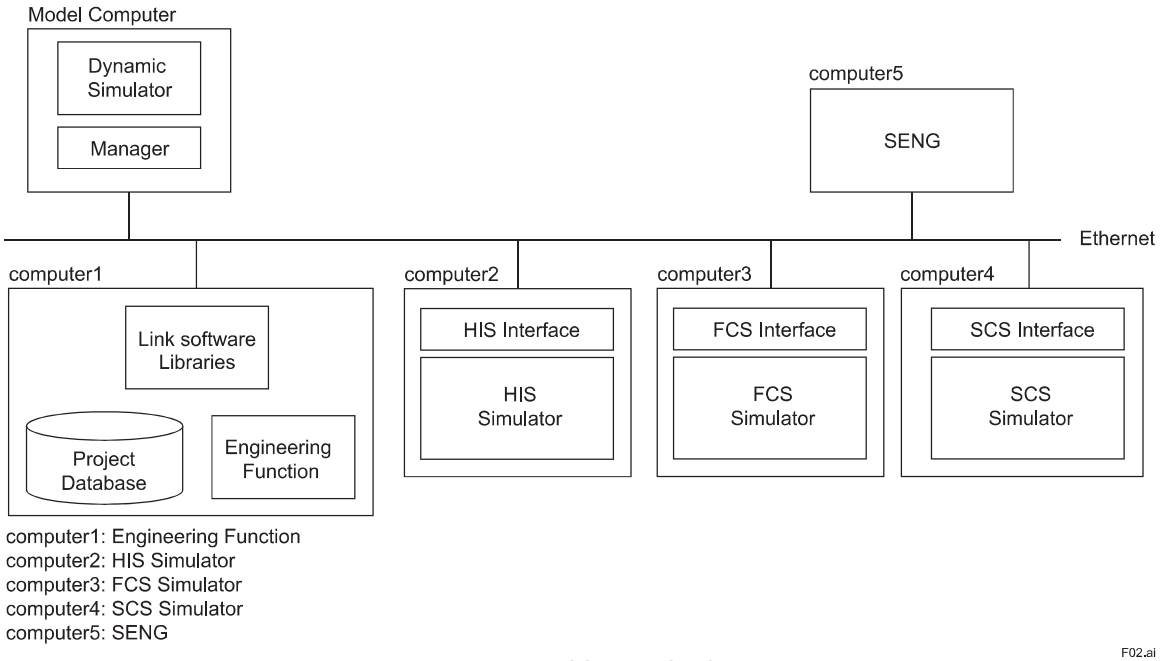


Figure Example of System Configuration

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Table Software Packages required for the Plant Training System

Product	Package	computer1	computer2	computer3	computer4	computer5
ProSafe-RS	RS4F1505 Safety Control Function for SCS Simulator (for S2SC70☐) (*1)	—	—	—	X	—
	RS4E5100 Automation Design Suite (AD Suite), Safety System Engineering and Maintenance Function	—	—	—	—	X
	RS4E5600 CENTUM VP Integration Package	—	—	—	—	X
CENTUM VP (*2)	VP6H1100 Standard Operation and Monitoring Function	—	X	—	—	— (*3)
	VP6E5100 Standard Engineering Function	X	—	—	—	—
	VP6E5420 Test Function (*4)	X	—	—	—	—
	VP6E5425 Expanded Test Function	X	—	—	—	—
	VP6E5426 FCS Simulator Package (*5)	—	—	X	X	—
	VP6E5427 HIS Simulator Package	—	X	—	—	— (*3)
	VP6F1☐05 Control Function for FCS Simulator (*6)	—	—	X	—	—
Plant training system (*7)	Exatif	X				—

X: Required —: Not Required

*1: When using multiple SCS simulators, RS4F1505s of the number same as the SCS simulators are required. RS4F1500 safety control function can be also used.
*2: CENTUM VP R6.02 or later is required.
*3: In order to launch the SCS maintenance support tool, this package must be installed in the computer5.
*4: Including the FCS simulator and HIS simulator.
*5: Including the SCS simulator.
*6: When using multiple FCS simulators, VP6F1☐05s of the number same as the FCS simulators are required. VP6F1☐00 control function can be also used.
*7: Installing this package on each computer is required.

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

■ APPLICATION CAPACITY

A term “application capacity” refers to the capacity to execute SCS’s safety control functions. The application capacity for an SCS differs by the selection of ESB bus coupler modules of SEC401 or SEC402. The same rule applies when calculating the maximum application capacity when RS4F1505 Safety Control Function for SCS Simulator under a virtual test environment.

Table Application Capacity

Category	Item	Maximum capacity
I/O-related items	Number of safety node units	13 (*1)
	Number of N-IO nodes	32
	Number of communication modules (S2LP131) (*2)	8
	Number of communication modules (ALE111/ALR121)	6 (2 modules as slaves and 4 modules as masters)
	Number of I/O points	1500 (*1) (*3)
	Number of subsystem communication data items	2000 (maximum communication data items per SCS) (*4)
	Number of safety subsystem communication I/O data items (*2)	2000 (maximum communication data items in S2LP131 per SCS)
Application logic	Number of POUs (*5)	500
	Number of variables	1500 I/O variables (*3) 4500 internal variables (*3)
Inter-SCS Safety Communication	Number of produced data	200
	Number of consumed data	200
SCS Link Transmission	Number of transmitted data	128
	Number of received data	1000
CENTUM VP integration function	Number of analog input blocks	total 2700
	Number of velocity alarm blocks	
	Number of override blocks	
	Number of password blocks	
	Manual operation function block	
	Number of subsystem communication I/O blocks	2000 (*6)
	Number of safety subsystem communication I/O blocks	2000
	Number of annunciators	2000

*1: The maximum capacity of the SEC401 is up to 9 units of safety node units and 1000 I/O points.
*2: Supported by ProSafe-RS R4.03.10 or later.
*3: The numbers are for reference.
*4: The maximum number of subsystem communication data items per SCS earlier than ProSafe-RS R4.03.10 is up to 500.
*5: POU stands for (Program Organization Unit) representing the programs, user defined function blocks, and user defined functions.
*6: The maximum number of subsystem communication I/O blocks per SCS earlier than ProSafe-RS R4.03.10 is up to 500.

■ OPERATING ENVIRONMENT

RS4F1500 safety control function (for S2SC70□) works on the following safety control units:

S2SC70S, S2SC70D

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

■ MODELS AND SUFFIX CODES

Safety Control Function (for S2SC70☐)

		Description
Model	RS4F1500	Safety Control Function (for S2SC70☐)
Suffix codes	-V	Software License
	1	Always 1
	1	English Version

Safety Control Function for SCS Simulator (for S2SC70☐)

		Description
Model	RS4F1505	Safety Control Function for SCS Simulator (for S2SC70☐)
Suffix codes	-V	Software License
	1	Always 1
	1	English Version

■ ORDERING INFORMATION

Specify the model and suffix code(s).

■ TRADEMARKS

- ProSafe, CENTUM, PRM, STARDOM, FAST/TOOLS, Exaopc, FieldMate, and Vnet/IP are either registered trademarks or trademarks of Yokogawa Electric Corporation.
- Other company and product names appearing in this document are registered trademarks or trademarks of their respective holders.

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation
Subject to change without notice.

Attachment 9.11 Hardware User Guide
IM32P06C10-01EN

User's
Manual

ProSafe-RS
ProSafe-RS Lite

Hardware User's Guide

IM 32P06C10-01EN

YOKOGAWA
Yokogawa Electric Corporation

IM 32P06C10-01EN
9th Edition

Introduction

ProSafe-RS is a safety control system that consists of one or more safety control stations (SCS) and a safety engineering PC (SENG). There are two types of SCSs depending on the safety integrity level (SIL): those that support SIL 3 and those that support SIL 2.

This user's manual describes the hardware configuration, installation, wiring, and maintenance of SCS. Of the devices making up SCS, the safety control unit (SCU) is described for the following models:

- For SCSs that support SIL 3
  - S2SC70S/D
  - SSC60S/D
  - SSC50S/D
- For SCSs that support SIL 2
  - L1SC70S/D

For information about SSC10S/D, refer to Safety Control Stations (Hardware) (IM 32Q06C10-31E).

For information about SSC57S/D, refer to Integration with CI Server (IM 32P04D20-01EN).

Structure of this document

This user's manual consists of the following parts:

- Part A
  System configuration of SCS

  This part describes an example of a system configuration of SCS that comprises a safety control unit, safety node units, a unit for optical bus repeater module, and N-IO nodes.
- Part B
  Components of SCS

  This part describes the devices that make up SCS.
- Part C
  Installing and wiring the SCS

  This part describes the installation of devices, ground wiring, power supply wiring, Vnet/IP cable wiring, and various bus wiring.
- Part D
  Signal wiring between SCS and field devices

  This part describes how to install wiring between I/O modules and field devices.
- Part E
  Maintaining the SCS

  This part describes the routine maintenance, parts with defined life spans, and how to replace devices.

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

Safety Precautions for Use

Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Be sure to confirm the specifications and required settings of the devices that are used in combination with the Product by referring to the instruction manual or other documents of the devices.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:

  
  Indicates that caution is required. This symbol for the Product indicates the possibility of dangers such as electric shock on personnel and equipment, and also indicates that the user must refer to the User’s Manuals for necessary actions. In the User’s Manuals, this symbol is used together with a word “CAUTION” or “WARNING” at the locations where precautions for avoiding dangers are described.

  <French> Signale qu’il faut faire preuve de prudence. Ce symbole pour le produit signale la possibilité d’un danger pour le personnel et l’équipement comme un choc électrique, et signale également que l’utilisateur doit se référer au Manuel de l’utilisateur afin de prendre les mesures nécessaires. Dans le Manuel de l’utilisateur, ce symbole est utilisé conjointement avec la mention «CAUTION» ou «WARNING» aux endroits où sont décrites les précautions pour éviter les dangers.

  
  Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.

  <French> Signale qu'il faut faire preuve de prudence avec la surface brûlante. Les appareils sur lesquels est apposé ce symbole risquent de devenir brûlants. Tout contact physique ou matériel avec ces appareils risque de provoquer des brûlures ou des dommages.

  
  Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.

  
  Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.

  Indicates an AC supply.

  Indicates a DC supply.

I	Indicates that a component such as a power supply switch is turned ON.
◯	Indicates that a component such as a power supply switch is turned OFF.

Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

Warning and Disclaimer

- Except as specified in the warranty terms, YOKOGAWA shall not provide any warranty for the Product.
- YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Product.

Notes on Hardware

Appearance and Accessories

Check the following items when you receive the Product:

- Appearance
- Standard accessories

Contact us or your local distributor in the following cases:

- The Product coating is peeling off.
- The Product itself is damaged.
- Any accessories are missing.

If the following label turns dirty and the information on it becomes illegible, or if the label is peeling off, order a new one with the part number T9029BX to replace it.


: Label attached to the Products such as the power supply module.

Model and Suffix Codes

The name plate on the Product indicates the model and suffix codes. Verify the model and suffix codes with those in the General Specifications (GS) to ensure that the Product matches the order specifications. If you have any questions, contact us or your local distributor.

Style Number

For some products, differences in the functions and usage of the product are distinguished by style number. The style number is indicated in the style number field on the name plate of the product.

Documentation Conventions

Symbols

The following symbols are used in the User's Manuals.

 WARNING	Indicates precautions to avoid a danger that may lead to death or severe injury.
 CAUTION	Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.
IMPORTANT	Indicates important information required to understand operations or functions.
TIP	Indicates additional information.
SEE ALSO	Indicates referenced content. In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.
If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

Full Names and Simplified Terms

In the User's Manuals, simplified terms listed in the following table are used.

Table Info-1 Full Names and Simplified Terms

Full Name	Simplified Term
Automation Design Suite	AD Suite
Automation Design Organizer	AD Organizer
Automation Design Server	AD Server
Automation Design project	AD project
Automation Design Master Database	ADMDB

Continues on the next page

Table Info-1 Full Names and Simplified Terms (Table continued)

Full Name	Simplified Term
Automation Design Suite Administration Tool	ADS Administration Tool
iDefine for ProSafe-RS	iDefine
Modification Package	ModPack
SCSV1-S (SCS supporting the SSC10S/SSC10D safety control units)	SCSV1
SCSP1-S (SCS supporting the SSC50S/SSC50D safety control units)	SCSP1
SCSP2-S (SCS supporting the SSC60S/SSC60D safety control units)	SCSP2
SCSP3-S (SCS supporting the S2SC70S/S2SC70D safety control units)	SCSP3
SCSL2-S (SCS supporting the L1SC70S/L1SC70D safety control units)	SCSL2
SCSU1-S (SCS supporting the SSC57S/SSC57D safety control units)	SCSU1

Installation and Maintenance Notes

Installation Method

Observe the following guidelines to ensure that devices meet safety and performance requirements:

- Install rack-mountable devices, DIN rail-mountable devices, and wall-mountable devices in a lockable metal cabinet. For information about the standards and conditions required of the cabinet, refer to the descriptions of the standards that the Product conforms to.
- If devices are housed in a cabinet, keep the cabinet door closed during operation.
- Ensure that all the empty slots of the devices are covered with the covers provided. Place an order for the required covers.
- Ensure that all cables are firmly fixed with cable ties.
- Install a dedicated breaker in a readily accessible location in the same room as the system so that it can shut off the power supply when an abnormality occurs. Identify and label the breaker with the name of the protected device connected to it. Never allow the breaker to disconnect the grounding cable that is connected to a protective grounding system. Use this breaker to turn off the power supply for the devices of the system when a device abnormality occurs.

WARNING

Be careful not to drop the device while installing it.

SEE ALSO

For more information about SIL3 certified SCS installation method, installation specifications, and measurement categories, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

For more information about SIL2 certified SCS installation method, installation specifications, and measurement categories, refer to:

ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

Tightening Torque of Screws

IMPORTANT

The recommended tightening torque for the Product is shown in the following table. However, if the tightening torque of the screw is specified in the User's Manuals, follow the instructions described in the User's Manuals.

Table Info-2 Recommended Tightening Torque

Nominal diameter of a screw	M2.6	M3	M3.5	M4	M5	M6	M8	M10
Recommended tightening torque (N·m)	0.35	0.6	0.8	1.2	2.8	3.0	12.0	24.0

SEE ALSO For more information about Each nominal diameter of a screw for the device that consists of SIL3 certified SCS, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

For more information about Each nominal diameter of a screw for the device that consists of SIL2 certified SCS, refer to:

ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

Power Cable Wiring

WARNING

- Connect the power cables according to the procedure specified in the User's Manuals of the device.
- Power cables must conform to the safety standards of the country where the device is installed.

SEE ALSO For more information about power cables wiring, refer to:

- C2., "Ground wiring and power supply wiring for SCS" on page C2-1
- User's Manuals of each device

Grounding

WARNING

The Product requires the protective grounding defined by the safety standards.

You must ground the Product according to the procedure specified in the User's Manuals to prevent electric shock and to minimize the effect of noise.

SEE ALSO For more information about grounding, refer to:

- C2., "Ground wiring and power supply wiring for SCS" on page C2-1
- User's Manuals of each device

I/O Cable Wiring

CAUTION

Wire I/O cables according to the procedure specified in the User's Manuals.

SEE ALSO For more information about I/O cable wiring, refer to:

D., “Signal wiring between SCS and field devices” on page D-1

For more information about I/O cables wiring, refer to:

User's Manuals of each device

Connected Devices

IMPORTANT

To ensure CSA standard conformity for the entire system of the Product, all the devices connected to the system of the Product should conform to CSA standards.

Maintenance

CAUTION

During maintenance, wear a wrist strap and follow Electrostatic Discharge (ESD) precautions.

IMPORTANT

- The Product maintenance should be performed only by personnel who have undergone specialized training.
- When a device turns dirty, use a vacuum cleaner or a soft dry cloth to clean it.
- If any existing caution label is peeling off, or is dirty and illegible, order a new one with the part number T9029BX to replace it.

SEE ALSO For more information about maintenance, refer to:

- E., “Maintaining the SCS” on page E-1
- User's Manuals of each device

Modules, Cards, Cables, and Connectors

CAUTION

When the power is on, only modules, cards, cables, and connectors that are allowed in the User's Manuals can be replaced, removed, or installed.

SEE ALSO For more information about replacing, and removing or installing modules, cards, cables, and connectors, refer to:

- E., “Maintaining the SCS” on page E-1
- User's Manuals of each device

Batteries

CAUTION

- You must use only YOKOGAWA-designated batteries.
- When replacing batteries while the power supply is on, do not put your hands inside the device to prevent electric shock.
- When mounting or replacing batteries, you must follow the procedure specified in the User's Manuals of the device.

SEE ALSO For more information about battery, refer to:

- “● Battery” on page B4-7
- E3.1, “Replacing the battery of the processor module” on page E3-4

For more information about batteries, refer to:

User's Manuals of each device

Fuses

WARNING

- Turn off the power supply before replacing the fuses.
- Use only YOKOGAWA-designated fuses for replacement.

SEE ALSO For more information about replacing fuses, refer to:

- “■ Replacing fuse for fan power supply unit” on page E3-10
- E3.3, “Replacing the fuse of digital input module” on page E3-12
- E3.4, “Replacing the fuse of terminal boards (for FIO node)” on page E3-13
- E3.6, “Replacing the fuse of relay boards” on page E3-18
- E3.8, “Replacing the fuses of base plate with disconnecting terminals” on page E3-20

For more information about fuses, refer to:

User's Manuals of each device

■ Fan Unit

CAUTION

When replacing the fan unit while the power supply is on, do not put your hands inside the device to prevent electric shock.

SEE ALSO For more information about fan unit, refer to:

- "■ Replacing fan unit" on page E3-9
- User's Manuals of each device

Copyright and Trademark Notices

All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, PRM, Exaopc, FieldMate Validator, and STARDOM are registered trademarks or trademarks of Yokogawa Electric Corporation.
- The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

Hardware User's Guide

IM 32P06C10-01EN 9th Edition

CONTENTS

PART-A System configuration of SCS..... A-1

Hardware User's Guide

IM 32P06C10-01EN 9th Edition

CONTENTS

PART-B Components of SCS.....B-1

B1. Configuration of SCU..... B1-1

B2. Configuration of SNU..... B2-1

B3. Configuration of unit for optical bus repeater module.....B3-1

B4. FIO node devices..... B4-1

B4.1 Power supply module.....B4-2

B4.2 Processor module.....B4-4

B4.3 ESB bus coupler module.....B4-12

B4.4 ESB bus interface module.....B4-14

B4.5 Optical ESB bus repeater module..... B4-16

B4.6 N-ESB bus coupler module.....B4-19

B4.7 FIO I/O modules and their peripherals.....B4-21

B4.7.1 Analog I/O modules..... B4-22

B4.7.2 Digital I/O modules.....B4-25

B4.7.3 Communication modules..... B4-27

B4.7.4 Pressure clamp terminal blocks..... B4-31

B4.7.5 Connector cover for MIL cable.....B4-32

B4.7.6 Terminal boards (for FIO node).....B4-33

B4.7.7 Relay boards.....B4-38

B4.8 External interface unit..... B4-41

B4.9 Node fan unit..... B4-42

B5. N-IO node devices.....B5-1

B5.1 Node interface unit.....B5-2

B5.2 Base plate for node interface unit..... B5-4

B5.3 Power supply unit..... B5-5

B5.4 N-ESB bus module.....B5-6

B5.5 Base plates..... B5-9

B5.5.1 Base plate with disconnecting terminals..... B5-10

B5.5.2 Base plate for barrier..... B5-14

B5.6 N-IO I/O module.....B5-17

B5.7 Intrinsic safety barriers..... B5-19

B5.8 Terminal board (for N-IO node)..... B5-20

B5.9 N-IO node cables.....B5-21
B6. Other devices.....B6-1
B6.1 Wiring check adapter for digital input.....B6-2

Hardware User's Guide

IM 32P06C10-01EN 9th Edition

CONTENTS

PART-C Installing and wiring the SCS..... C-1

C1. Installing the SCS..... C1-1

C1.1 Installing an FIO node..... C1-2

C1.2 Installing terminal boards and relay boards (for FIO node)..... C1-4

C1.2.1 Installing a rack mountable terminal/relay board..... C1-5

C1.2.2 Installing a DIN rail mountable terminal/relay board..... C1-7

C1.2.3 Precautions when installing a DIN rail mountable terminal/relay board..... C1-11

C1.3 Installing the node interface unit..... C1-12

C1.4 Installing the N-IO I/O unit..... C1-15

C1.4.1 Installing the base plate with disconnecting terminals..... C1-16

C1.4.2 Installing the base plate for barrier..... C1-19

C1.4.3 Mounting N-IO I/O module..... C1-22

C1.4.4 Mounting intrinsic safety barriers..... C1-24

C1.4.5 Mounting the terminal block..... C1-27

C1.5 Installing the terminal board (for N-IO node)..... C1-28

C1.6 Installing the field power supply unit..... C1-29

C2. Ground wiring and power supply wiring for SCS..... C2-1

C2.1 Ground wiring and power supply wiring of the power supply module..... C2-2

C2.2 Connecting the power cable to the power supply unit for fan unit..... C2-3

C2.3 Connecting the field power supply cable to a DIN rail mountable terminal board/relay board (for FIO node)..... C2-4

C2.4 Ground wiring of the FIO node devices..... C2-5

C2.5 Ground and power supply wiring of the node interface unit..... C2-8

C2.5.1 Ground wiring of the base plate for node interface unit..... C2-9

C2.5.2 Ground and power supply wiring of the power supply unit..... C2-10

C2.6 Ground and power supply wiring of the N-IO I/O unit..... C2-13

C3. Bus cable wiring of SCS..... C3-1

C3.1 Connecting cables for Vnet/IP..... C3-2

C3.2 Connecting ESB bus cables..... C3-4

C3.3 Connecting optical ESB bus cables (FIO node)..... C3-5

C3.4 Connecting N-ESB bus cables.....C3-11
C3.5 Connecting optical ESB bus cables (N-IO node)..... C3-13
C3.6 Connecting F-SB bus cables..... C3-17

Hardware User's Guide

IM 32P06C10-01EN 9th Edition

CONTENTS

PART-D Signal wiring between SCS and field devices.... ....D-1

D1. Signal wiring between FIO I/O modules and field devices.....D1-1

D1.1 Types of FIO I/O module signal connection..... D1-2

D1.1.1 Signal connections to the pressure clamp terminal block.....D1-4

D1.1.2 Signal connections to the MIL connectors.....D1-6

D1.1.3 Signal connections to the terminal board/relay board.....D1-7

D1.2 Signal cable connection to analog Input/Output modules.....D1-12

D1.2.1 Terminal numbers and signal names of pressure clamp terminal blocks and the MIL connector of analog I/O modules.....D1-13

D1.2.2 Terminal numbers and signal names of the terminal board for analog I/O modules..... D1-17

D1.3 Signal cable connection to digital I/O modules..... D1-22

D1.3.1 Terminal numbers and signal names of pressure clamp terminal blocks and the MIL connector of digital I/O modules..... D1-23

D1.3.2 Terminal numbers and signal names of the terminal board for digital I/O modules..... D1-27

D1.3.3 Relay board terminal numbers and signal names..... D1-34

D1.4 Connection of communication modules.....D1-41

D1.4.1 Connection of the serial communication module (RS-232C)..... .....D1-42

D1.4.2 Connection of the serial communication module (RS-422/RS-485).... .....D1-48

D1.4.3 Signal connection of the Ethernet communication module.....D1-53

D1.4.4 Connection of the fire and gas communication module.....D1-54

D2. Signal wiring between an N-IO I/O unit and field devices..... D2-1

D2.1 Signal connection to the base plate with disconnecting terminals..... .....D2-5

D2.2 Signal connections of the base plate for barrier: S2BN4D..... D2-9

D2.3 Signal connections to the base plate for barriers: S2BN5D..... D2-10

D3. Signal connection of the external alarm input terminals of the node interface unit..... D3-1

Hardware User's Guide

IM 32P06C10-01EN 9th Edition

CONTENTS

PART-E Maintaining the SCS..... E-1

E1. Precautions during maintenance work..... E1-1

E2. Routine maintenance..... E2-1

E3. Parts with defined life spans and replacement parts of SCS..... E3-1

E3.1 Replacing the battery of the processor module..... E3-4

E3.2 Replacing the parts of the node fan unit..... E3-9

E3.3 Replacing the fuse of digital input module..... E3-12

E3.4 Replacing the fuse of terminal boards (for FIO node)..... E3-13

E3.5 Replacing the relays on relay boards..... E3-15

E3.6 Replacing the fuse of relay boards..... E3-18

E3.7 Replacing the fuses of the base plate for barrier..... E3-19

E3.8 Replacing the fuses of base plate with disconnecting terminals..... E3-20

E4. Replacing FIO node components..... E4-1

E4.1 Replacing power supply module..... E4-2

E4.2 Replacing processor module..... E4-4

E4.3 Replacing ESB bus coupler module..... E4-8

E4.4 Replacing the N-ESB bus coupler module..... E4-9

E4.5 Replacing ESB bus interface module..... E4-10

E4.6 Replacing optical ESB bus repeater module..... E4-11

E4.7 Replacing FIO I/O modules..... E4-13

E4.8 Replacing, adding, and removing the SNU..... E4-18

E4.8.1 Replacing the SNU..... E4-19

E4.8.2 Adding the SNU..... E4-20

E4.8.3 Removing the SNU..... E4-22

E5. Replacing N-IO node components..... E5-1

E5.1 Replacing power supply units..... E5-2

E5.2 Replacing N-ESB bus modules..... E5-4

E5.3 Replacing N-IO I/O modules..... E5-5

E6. Replacing the cables..... E6-1

E6.1 Replacing ESB bus cables..... E6-2

E6.2 Replacing fiber-optic cables for optical ESB bus..... E6-3

E6.3 Replacing N-ESB bus cables..... E6-4

A. System configuration of SCS

This section describes the position and configuration of the safety control station (SCS) in ProSafe-RS. The SCS is connected to a Vnet/IP domain and communicates with other SCSs. There are two types of SCSs depending on the safety integrity level (SIL): those configured with hardware devices that support SIL 3 (such as SCSP3) and those configured with hardware devices that support SIL 2 (such as SCSL2).

The SCS consists of the safety control unit (SCU), safety node units (SNUs), unit for optical ESB repeater module, and N-IO nodes. The SCU, SNU, and unit for optical ESB repeater module are collectively called FIO nodes. An N-IO node consists of a node interface unit and one or more N-IO I/O units.

When connecting the SCU and SNUs, use the ESB bus or optical ESB bus. When connecting the SCU and N-IO nodes, use the ESB bus or optical ESB bus.

The following figure shows an example of a system configuration.

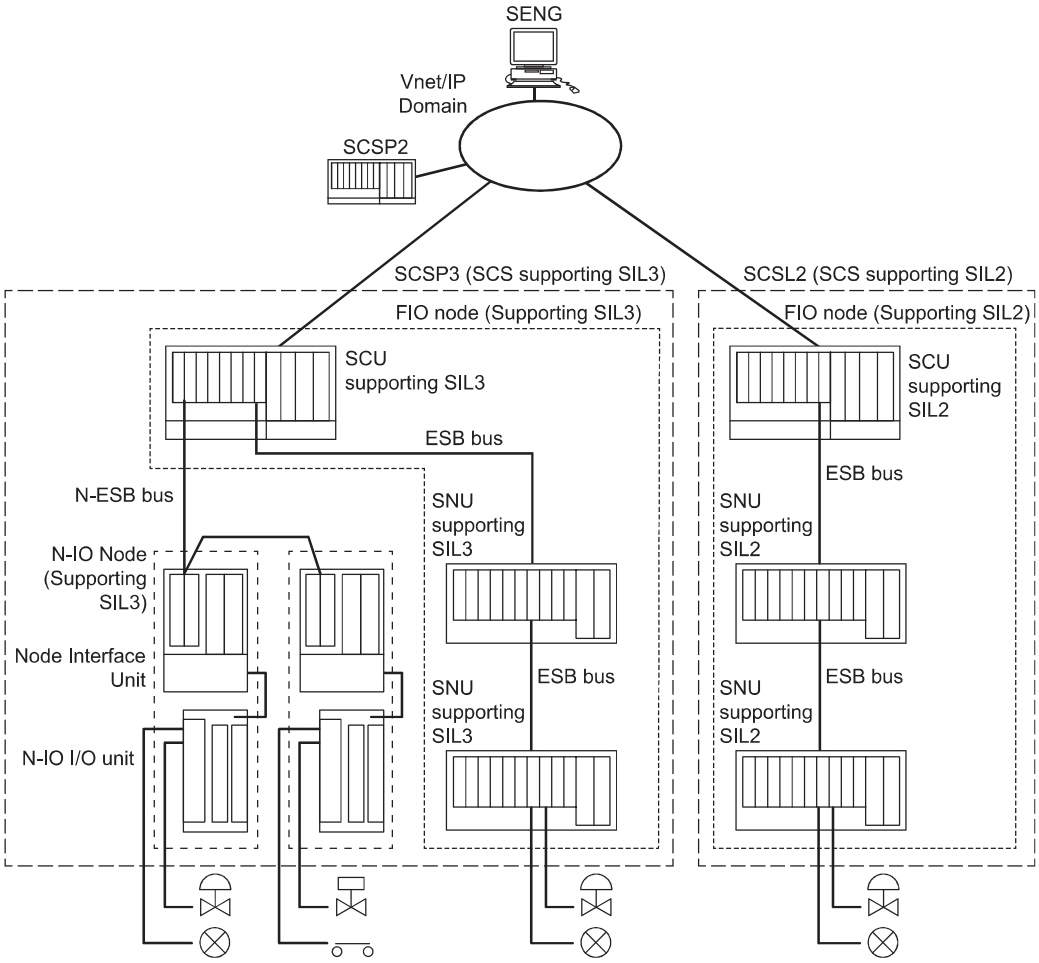


Figure A-1 Example of system configuration

B. Components of SCS

This section describes the components of SCS.

- SCU (FIO node)
- SNU (FIO node)
- Unit for optical bus repeater module (FIO node)
- Devices that make up an FIO node
- N-IO node devices

B1. Configuration of SCU

Processor modules that perform control calculation in the SCS and power supply modules are installed in the SCU. In addition, the SCU has slots for installing FIO I/O modules, N-ESB/ESB bus coupler modules, or optical ESB bus repeater modules.

There are SCUs for SCSs that support SIL 3 and those for SCSs that support SIL 2.

- For SCSs that support SIL 3
  - S2SC70S/D
  - SSC60S/D
  - SSC50S/D
- For SCSs that support SIL 2
  - L1SC70S/D

Each SCU is available in a standard type (ambient temperature: –20 to 40 deg. C) or a wide range temperature type (ambient temperature: –20 to 70 deg. C). A wide range temperature type is configured from a standard type with added node fan units to accommodate a wider ambient temperature range.

Standard type SCU

The following figure shows an example of a duplexed configuration of the standard type SCU.

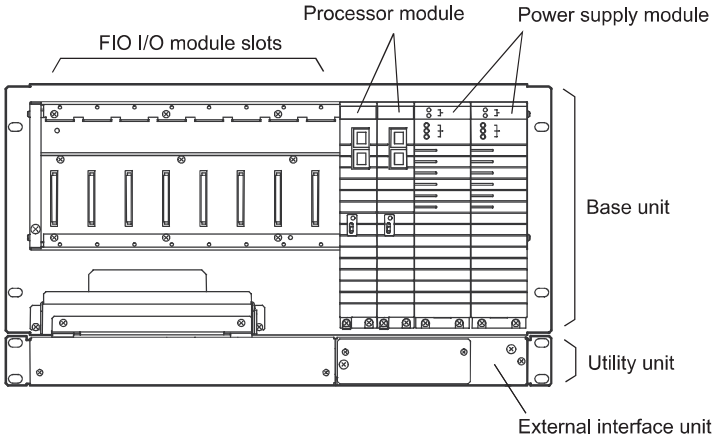


Figure B1-1 Configuration of the standard type SCU

For a single configuration, a processor module is installed in the left slot, and a dummy cover with the following part No. is attached to the right slot:

- SCUs that support SIL 3: T9083VB
- SCUs that support SIL 2: T9085SA

In the FIO I/O module slots, the following modules can also be installed in addition to FIO I/O modules:

- ESB bus coupler module
- Optical ESB bus repeater module
- N-ESB bus coupler module

TIP

N-ESB bus coupler module should be used in S2SC70□.

You must attach a dummy cover to unused FIO I/O module slots. The model names of dummy covers are as follows:

- SCUs that support SIL 3: SDCV01
- SCUs that support SIL 2: L1DCV01

The following tables show the main devices of the standard type SCUs.

Table B1-1 Devices that are installed in S2SC70S-SA/S2SC70D-SA

Name	Model	Specifications	Quantity	
			Single configuration (S2SC70S-SA)	Duplexed configuration (S2SC70D-SA)
Power supply module (*1)	SPW481	Input 100-120 V AC	2	2
	SPW482	Input 220-240 V AC	2	2
	SPW484	Input 24 V DC	2	2
Processor module	S2CP471	-	1	2

*1: One of the following power supply modules is installed: SPW481, SPW482, or SPW484.

Table B1-2 Devices that are installed in S2SC70S-S4/S2SC70D-S4

Name	Model	Specifications	Quantity	
			Single configuration (S2SC70S-S4)	Duplexed configuration (S2SC70D-S4)
Power supply module (*1)	SPW481	Input 100-120 V AC	2	2
	SPW482	Input 220-240 V AC	2	2
	SPW484	Input 24 V DC	2	2
Processor module	SCP461 (*2) (*3)	-	1	2

*1: One of the following power supply modules is installed: SPW481, SPW482, or SPW484.
*2: Use a processor module of style S2 or higher.
*3: Replaceable to S2CP471. If you want to replace, contact YOKOGAWA sales or service agents for replacement.

Table B1-3 Devices that are installed in SSC60S-S/SSC60D-S

Name	Model	Specifications	Quantity	
			Single configuration (SSC60S-S)	Duplexed configuration (SSC60D-S)
Power supply module (*1)	SPW481	Input 100-120 V AC	2	2
	SPW482	Input 220-240 V AC	2	2
	SPW484	Input 24 V DC	2	2
Processor module	SCP461 (*2)	-	1	2

*1: One of the following power supply modules is installed: SPW481, SPW482, or SPW484.
*2: Replaceable to S2CP471. If you want to replace, contact YOKOGAWA sales or service agents for replacement.

Table B1-4 Devices that are installed in SSC50S-S/SSC50D-S

Name	Model	Specifications	Quantity	
			Single configuration (SSC50S-S)	Duplexed configuration (SSC50D-S)
Power supply module (*1)	SPW481	Input 100-120 V AC	2	2
	SPW482	Input 220-240 V AC	2	2
	SPW484	Input 24 V DC	2	2
Processor module	SCP451 (*2)	-	1	2

*1: One of the following power supply modules is installed: SPW481, SPW482, or SPW484.
*2: Use a processor module with firmware revision number (F1) that is 19 or higher.

Table B1-5 Devices that are installed in L1SC70S-S or L1SC70D-S

Name	Model	Specifications	Quantity	
			Single configuration (L1SC70S-S)	Duplexed configuration (L1SC70D-S)
Power supply module (*1)	L1PW481	Input 100-120 V AC	2	2
	L1PW482	Input 220-240 V AC	2	2
	L1PW484	Input 24 V DC	2	2
Processor module	L1CP471	-	1	2

*1: One of the following power supply modules is installed: L1PW481, L1PW482, or L1PW484.

SEE ALSO For more information about restrictions on module installation to SCUs that support SIL 3, refer to:

ProSafe-RS Outline of I/O Modules (for FIO) (GS 32P06K60-01EN)

For more information about restrictions on module installation to SCUs that support SIL 2, refer to:

ProSafe-RS Lite Outline of I/O Modules (GS 32P56K60-01EN)

Wide range temperature type SCU

A wide range temperature type SCU is configured from a standard type SCU with added node fan units to ensure use in a wider ambient temperature range.

The following figure shows an example of a duplexed configuration of a wide range temperature type SCU.

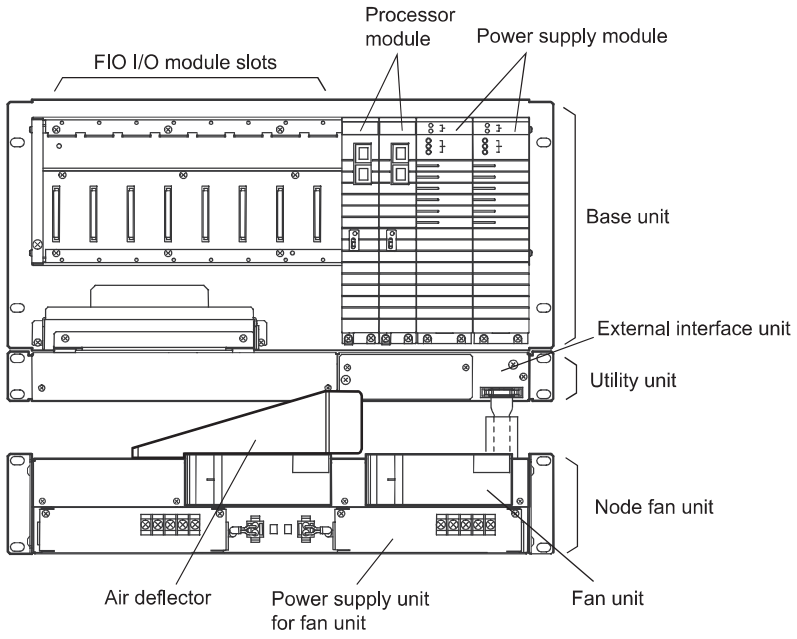


Figure B1-2 Components of the wide range temperature type SCU (example of S2SC70D-FA)

For a single configuration, a processor module is installed in the left slot, and a dummy cover with the following part Nos. is attached to the right slot:

- SCUs that support SIL 3: T9083VB
- SCUs that support SIL 2: T9085SA

In the FIO I/O module slots, you can also install the following modules instead of FIO I/O modules:

- ESB bus coupler module
- Optical ESB bus repeater module
- N-ESB bus coupler module

TIP

N-ESB bus coupler module should be used in S2SC70□.

You must attach a dummy cover to unused FIO I/O module slots. The model names of dummy covers are as follows:

- For SCSs that support SIL 3: SDCV01
- For SCSs that support SIL 2: L1DCV01

The following tables show the main components of the wide range temperature type SCUs.

Table B1-6 Devices that are installed in S2SC70S-FA or S2SC70D-FA

Name	Model/Part	Specifications	Quantity	
			Single configuration (S2SC70S-FA)	Duplexed configuration (S2SC70D-FA)
Power supply module (*1)	SPW481	Input 100-120 V AC	2	2
	SPW482	Input 220-240 V AC	2	2
	SPW484	Input 24 V DC	2	2

Continues on the next page

Table B1-6 Devices that are installed in S2SC70S-FA or S2SC70D-FA (Table continued)

Name	Model/Part	Specifications	Quantity	
			Single configuration (S2SC70S-FA)	Duplexed configuration (S2SC70D-FA)
Processor module	S2CP471	-	1	2
Power supply unit for the fan (*2)	S9159FA	Input 100-120, 220-240 V AC	2	2
	S9160FA	Input 24 V DC	2	2
Fan unit	AIP602	-	2	2
Air deflector	T9085JZ	-	1	1

*1: One of the following power supply modules is installed: SPW481, SPW482, or SPW484.
*2: Either one of the following power supply units is installed for the fan: S9159FA or S9160FA.

Table B1-7 Devices that are installed in S2SC70S-F4 or S2SC70D-F4

Name	Model/Part	Specifications	Quantity	
			Single configuration (S2SC70S-F4)	Duplexed configuration (S2SC70D-F4)
Power supply module (*1)	SPW481	Input 100-120 V AC	2	2
	SPW482	Input 220-240 V AC	2	2
	SPW484	Input 24 V DC	2	2
Processor module	SCP461 (*2) (*3)	-	1	2
Power supply unit for the fan (*4)	S9159FA	Input 100-120, 220-240 V AC	2	2
	S9160FA	Input 24 V DC	2	2
Fan unit	AIP602	-	2	2

*1: One of the following power supply modules is installed: SPW481, SPW482, or SPW484.
*2: Use a processor module of style S2 or higher.
*3: Replaceable to S2CP471. If you want to replace, contact YOKOGAWA sales or service agents for replacement.
*4: Either one of the following power supply units is installed for the fan: S9159FA or S9160FA.

Table B1-8 Devices that are installed in SSC60S-F/SSC60D-F

Name	Model/Part	Specifications	Quantity	
			Single configuration (SSC60S-F)	Duplexed configuration (SSC60D-F)
Power supply module (*1)	SPW481	Input 100-120 V AC	2	2
	SPW482	Input 220-240 V AC	2	2
	SPW484	Input 24 V DC	2	2
Processor module	SCP461 (*2)	-	1	2
Power supply unit for the fan (*3)	S9159FA	Input 100-120, 220-240 V AC	2	2
	S9160FA	Input 24 V DC	2	2
Fan unit	AIP602	-	2	2

*1: One of the following power supply modules is installed: SPW481, SPW482, or SPW484.
*2: Replaceable to S2CP471. If you want to replace, contact YOKOGAWA sales or service agents for replacement.
*3: Either one of the following power supply units is installed for the fan: S9159FA or S9160FA.

Table B1-9 Devices that are installed in SSC50S-F/SSC50D-F

Name	Model/Part	Specifications	Quantity	
			Single configuration (SSC50S-F)	Duplexed configuration (SSC50D-F)
Power supply module (*1)	SPW481	Input 100-120 V AC	2	2
	SPW482	Input 220-240 V AC	2	2
	SPW484	Input 24 V DC	2	2
Processor module	SCP451 (*2)	-	1	2
Power supply unit for the fan (*3)	S9159FA	Input 100-120, 220-240 V AC	2	2
	S9160FA	Input 24 V DC	2	2
Fan unit	AIP602	-	2	2

*1: One of the following power supply modules is installed: SPW481, SPW482, or SPW484.
*2: Use a processor module with firmware revision number (F1) that is 19 or higher.
*3: Either one of the following power supply units is installed for the fan: S9159FA or S9160FA.

Table B1-10 Devices that are installed in L1SC70S-F or L1SC70D-F

Name	Model/Part	Specifications	Quantity	
			Single configuration (L1SC70S-F)	Duplexed configuration (L1SC70D-F)
Power supply module (*1)	L1PW481	Input 100-120 V AC	2	2
	L1PW482	Input 220-240 V AC	2	2
	L1PW484	Input 24 V DC	2	2
Processor module	L1CP471	-	1	2
Power supply unit for the fan (*2)	S9159FA	Input 100-120, 220-240 V AC	2	2
	S9160FA	Input 24 V DC	2	2
Fan unit	AIP602	-	2	2
Air deflector	T9085JZ	-	1	1

*1: One of the following power supply modules is installed: L1PW481, L1PW482, or L1PW484.
*2: Either one of the following power supply units is installed for the fan: S9159FA or S9160FA.

SEE ALSO

For more information about restrictions on module installation to SCUs that support SIL 3, refer to:

ProSafe-RS Outline of I/O Modules (for FIO) (GS 32P06K60-01EN)

For more information about restrictions on module installation to SCUs that support SIL 2, refer to:

ProSafe-RS Lite Outline of I/O Modules (GS 32P56K60-01EN)

B2. Configuration of SNU

SNU sends and receives field device signals through an FIO I/O module and communicates with the SCU through ESB bus or optical ESB bus.

The SNU models are as follows:

- For SCSs that support SIL 3: SNB10D
- For SCSs that support SIL 2: L1NB10D

The following figure shows the configuration of SNU.

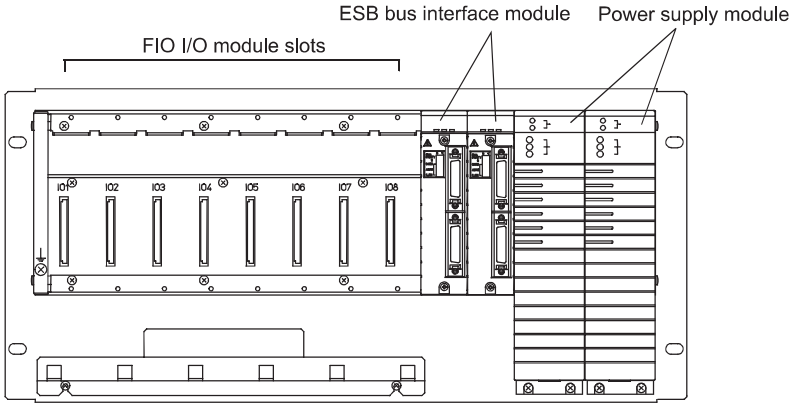


Figure B2-1 Configuration of SNU

In the FIO I/O module slots, you can also install optical ESB bus repeater modules instead of FIO I/O modules. You must attach a dummy cover to unused FIO I/O module slots. The model names of dummy covers are as follows:

- For SCSs that support SIL 3: SDCV01
- For SCSs that support SIL 2: L1DCV01

The following table describes the devices that are installed in SNU.

Table B2-1 Devices that are installed in SNB10D

Name	Model	Specifications	Quantity
Power supply module (*1)	SPW481	100 to 120 V AC input	2
	SPW482	220 to 240 V AC input	2
	SPW484	24 V DC input	2
ESB bus interface module	SSB401	-	2

*1: One of the following power supply modules is installed: SPW481, SPW482, or SPW484.

Table B2-2 Devices that are installed in L1NB10D

Name	Model	Specifications	Quantity
Power supply module (*1)	L1PW481	100 to 120 V AC input	2
	L1PW482	220 to 240 V AC input	2
	L1PW484	24 V DC input	2
ESB bus interface module	L1SB401	-	2

*1: One of the following power supply modules is installed: L1PW481, L1PW482, or L1PW484.

SEE ALSO

For more information about restrictions on module installation to SNUs that support SIL 3, refer to:

ProSafe-RS Outline of I/O Modules (for FIO) (GS 32P06K60-01EN)

For more information about restrictions on module installation to SNUs that support SIL 2, refer to:

ProSafe-RS Lite Outline of I/O Modules (GS 32P56K60-01EN)

B3. Configuration of unit for optical bus repeater module

The unit for optical ESB bus repeater module is used to install the optical ESB bus repeater module.

The SNU models are as follows:

- For SCSs that support SIL 3: SNT10D
- For SCSs that support SIL 2: L1NT10D

The following figure shows the configuration of the unit for optical ESB bus repeater module.

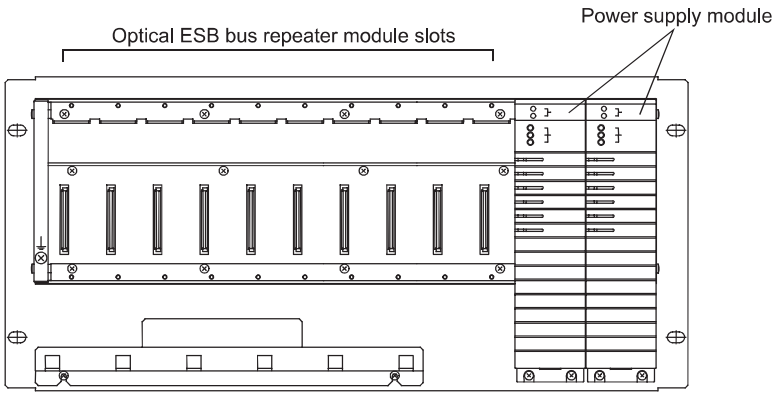


Figure B3-1 Configuration of unit for optical bus repeater module

You must attach a dummy cover to unused optical ESB bus repeater module slots. The model names of dummy covers are as follows:

- For SCSs that support SIL 3: SDCV01
- For SCSs that support SIL 2: L1DCV01

The following table describes the devices that are installed in the unit for optical bus repeater module.

Table B3-1 Devices that are installed in SNT10D

Name	Model	Specifications	Quantity
Power supply module (*1)	SPW481	100 to 120 V AC input	2
	SPW482	220 to 240 V AC input	2
	SPW484	24 V DC input	2

*1: One of the following power supply modules is installed: SPW481, SPW482, or SPW484.

Table B3-2 Devices that are installed in L1NT10D

Name	Model	Specifications	Quantity
Power supply module (*1)	L1PW481	100 to 120 V AC input	2
	L1PW482	220 to 240 V AC input	2
	L1PW484	24 V DC input	2

*1: One of the following power supply modules is installed: L1PW481, L1PW482, or L1PW484.

SEE ALSO

For more information about restrictions on installation of optical ESB bus repeater modules that support SIL 3, refer to:

ProSafe-RS Optical ESB Bus Repeater Module (GS 32Q06L15-31E and GS 32Q06L16-31E)

For more information about restrictions on installation of optical ESB bus repeater modules that support SIL 2, refer to:

ProSafe-RS Lite Optical ESB Bus Repeater Module (GS 32P56L15-01EN and GS 32P56L16-01EN)

B4. FIO node devices

This section describes the devices that constitute an FIO node.

- Power supply module
- Processor module
- ESB bus coupler module
- ESB bus interface module
- Optical ESB bus repeater module
- N-ESB bus coupler module
- FIO I/O modules and their peripherals
  - Analog I/O module
  - Digital I/O module
  - Communication module
  - Pressure clamp terminal block
  - Connector cover for MIL cable
  - Terminal board
  - Relay board
- External interface unit
- Node fan unit

B4.1 Power supply module

The power supply module is installed in the SCU, SNU, or unit for optical bus repeater module and supplies power to the modules in the unit.

There are power supply modules for SCSs that support SIL 3 and those that support SIL 2.

- For SCSs that support SIL 3
  - SPW481: 100-120 V AC input power supply module
  - SPW482: 220-240 V AC input power supply module
  - SPW484: 24 V DC input power supply module
- For SCSs that support SIL 2
  - L1PW481: 100-120 V AC input power supply module
  - L1PW482: 220-240 V AC input power supply module
  - L1PW484: 24 V DC input power supply module

Elements on the power supply module

The following figure shows the elements on the power supply module. Power input terminals are behind the front cover.

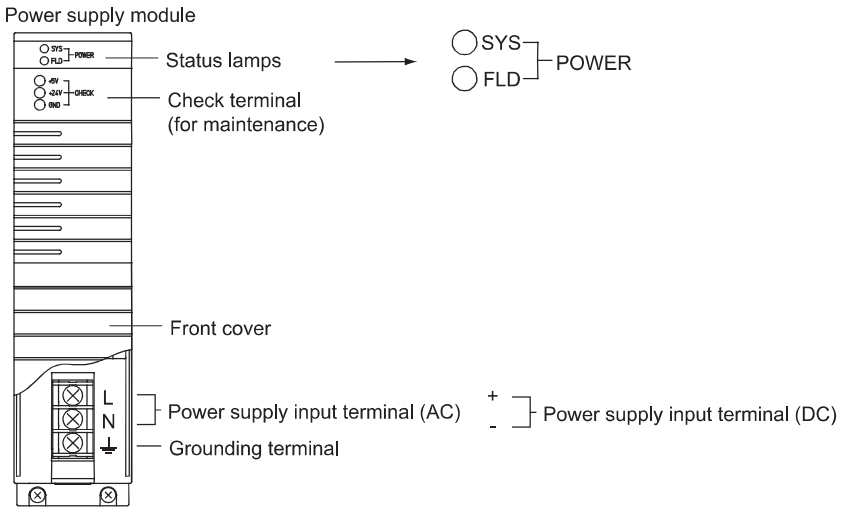


Figure B4.1-1 Power supply module

Status lamps

The power supply module has the following status lamps:

- SYS
  The lamp turns on when the output is +5 V; otherwise, the lamp turns off.
- FLD
  The lamp turns on when the output is +24 V; otherwise, the lamp turns off.

Power input terminals

The power supply module receives power through the power input terminals. You must prepare power cables separately.

SEE ALSO For more information about ground wiring and power supply wiring of the power supply module, refer to:

C2.1, “Ground wiring and power supply wiring of the power supply module” on page C2-2

B4.2 Processor module

The processor module is installed in the SCU and performs control calculations.

There are processor modules for SCUs that support SIL 3 and those that support SIL 2.

- For SCUs that support SIL 3
  - S2CP471: for S2SC70□ and SSC60□
  - SCP461 (style S2 or higher): for S2SC70□-□4 and SSC60□
  - SCP461 (style S1): for SSC60□
  - SCP451: for SSC50□
- For SCUs that support SIL 2
  - L1CP471: for L1SC70□

TIP SCP461 is replaceable to S2CP471. If you want to replace, contact YOKOGAWA sales or service agents for replacement.

Elements on the processor module

The following figures show the elements on the processor modules.

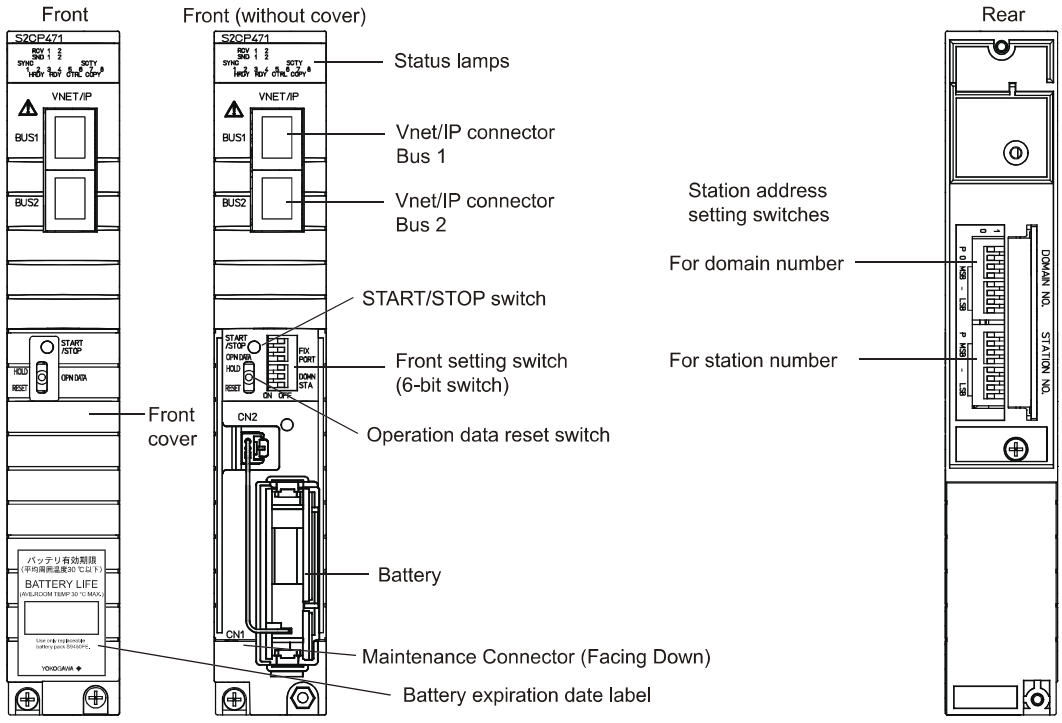


Figure B4.2-1 S2CP471/L1CP471 (The figure shows an example of S2CP471.)

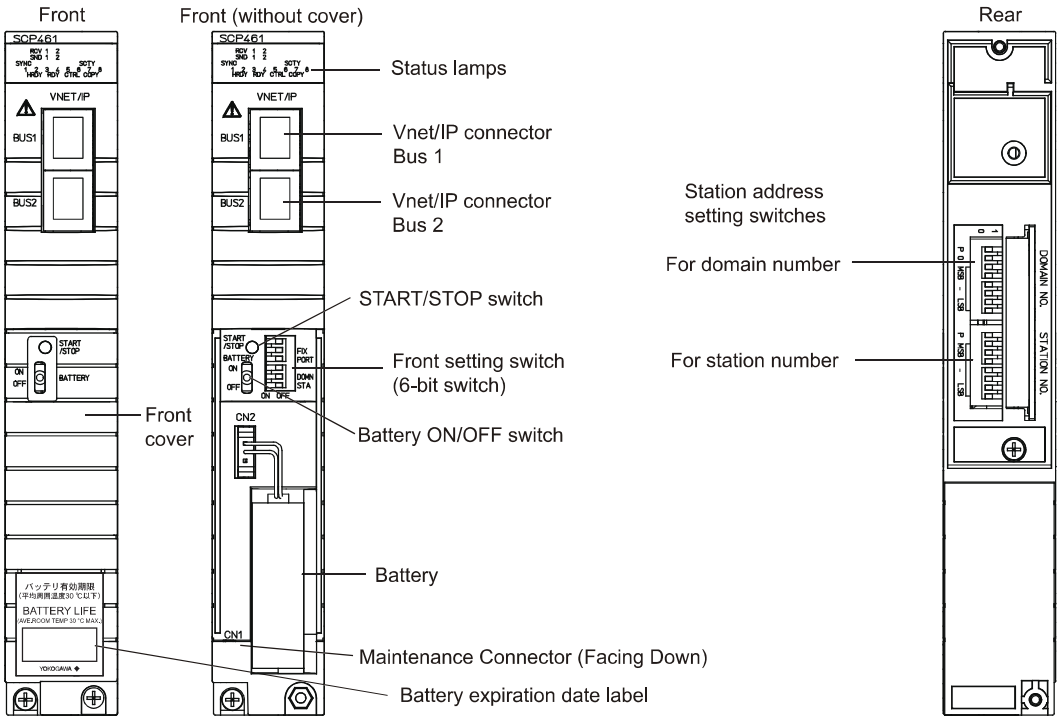


Figure B4.2-2 SCP461

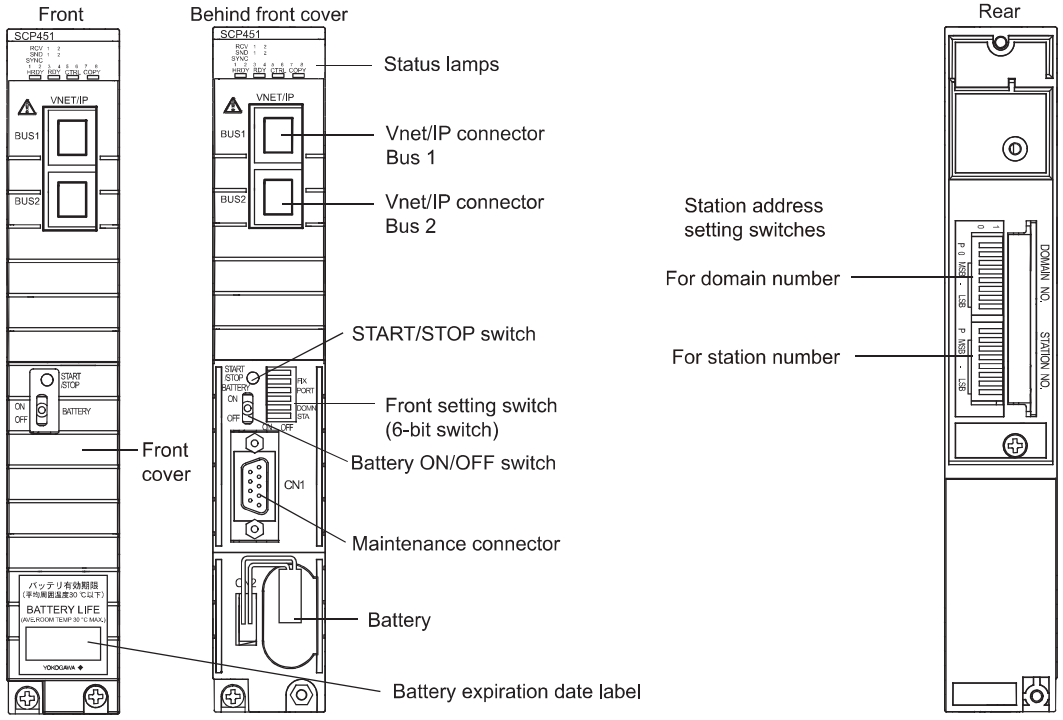


Figure B4.2-3 SCP451

The front setting switches and battery of the processor module are provided behind the front cover. The setting switches for the domain number and station number are provided in the rear of the module, so you must remove the module from the base unit when you configure the switches.

Status lamps

The following figure shows the status lamps of the processor module.

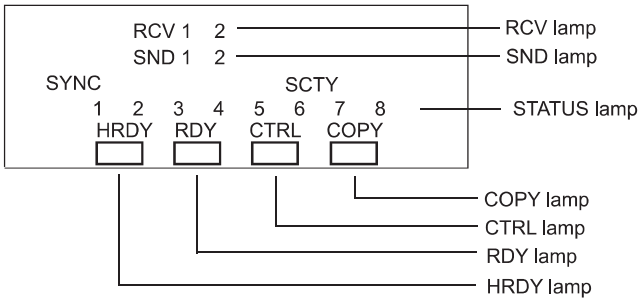


Figure B4.2-4 Status lamps of the processor module

- HRDY
  The processor module diagnoses itself. When the processor module hardware is functioning normally, this lamp turns on; otherwise, the lamp turns off.
- RDY
  This lamp turns on when both the hardware and software are functioning normally; otherwise, the lamp turns off.
- CTRL
  This lamp turns on when the processor module is controlling and turns off when the module is standby in dual-redundant configuration or stopped controlling.
- COPY
  In dual-redundant configuration, this lamp turns on when program copy is running and turns off when program copy is completed. When the standby processor module is replaced in dual-redundant configuration or when the module starts from a stopped state, the program in the active processor module is automatically copied to the standby processor module.
- RCV
  These lamps indicate Vnet/IP communication status. 1 indicates the status of Vnet/IP bus 1 while 2 indicates the status of Vnet/IP bus 2. The lamp flashes when the module is receiving; otherwise, the lamp turns off.
- SND
  These lamps indicate Vnet/IP communication status. 1 indicates the status of Vnet/IP bus 1 while 2 indicates the status of Vnet/IP bus 2. The lamp flashes when the module is sending; otherwise, the lamp turns off.
- SYNC
  This lamp indicates the status of synchronization with the Vnet/IP network time. The lamp turns on when synchronized; otherwise, the lamp turns off.
- SCTY
  This lamp turns on when the security level of the SCS is an online level and turns off otherwise.
- STATUS (1, 2, 3, 4, 5, 6, 7, 8)
  These lamps indicate the status of the processor module. Usually, the lamps indicate an operating mode or error status. However, they indicate the status of the domain number or station number setting switches, depending on the front switch setting.
  - When the DOMN switch is set to ON: Status of the domain number setting switches
  - When the STA switch is set to ON: Status of the station number setting switches

Battery

Even if the power is not supplied to processor modules for example in a power outage, batteries helps to maintain the management information of the modules. The maintained management information varies depending on the type of modules.

- S2CP471 or L1CP471: Real time data of the real time clock (RTC)
- SCP461 or SCP451: Operation data and the real time data of RTC

TIP

- S2CP471/L1CP471 stores the operation data in the non-volatile memory (NVRAM) and stores application programs in the flash memory, so both of them are not initialized in the event of a power outage.
- SCP461 or SCP451 stores application programs in the flash memory and they are not initialized in the event of a power outage.

CAUTION

Use batteries specified by Yokogawa Electric.

A label indicating the expiration date of the battery is attached on the lower part of the processor module front cover.

This expiration date is valid when the ambient temperature is less than 30 degree Celsius.

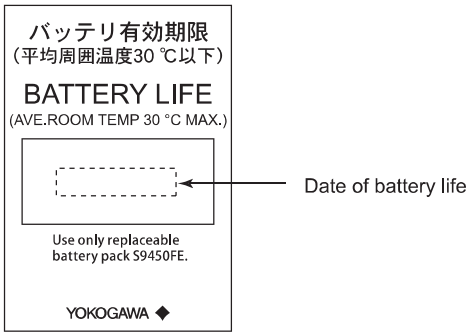


Figure B4.2-5 Example of the battery expiration date label

SEE ALSO For more information about how to replace the battery, refer to:

E3.1, “Replacing the battery of the processor module” on page E3-4

Front switches of the processor module

The following figure shows the switches in the front of the processor module.

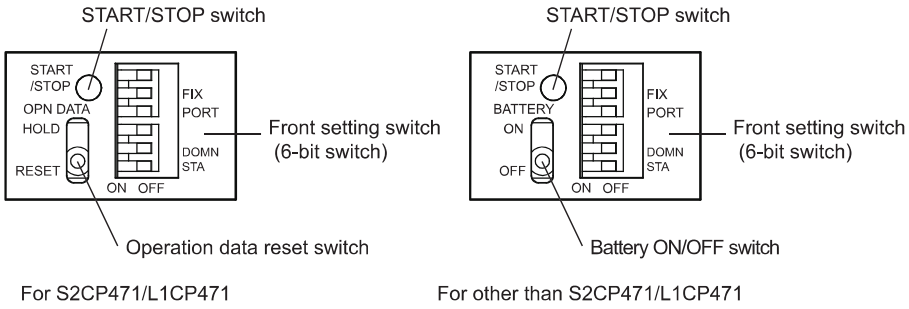


Figure B4.2-6 Front switches of the processor module

IMPORTANT

Note that the operation data reset switch of S2CP471/L1CP471 and the battery ON/OFF switch of other processor modules have the same appearance but different functions.

- START/STOP switch
  This switch is used for maintenance. If this switch is pressed when the processor module is operating, the CPU of the module is stopped forcibly. If this switch is pressed when the processor module is not operating, the CPU restarts.

  This switch is located inside a hole next to the START/STOP sign. Gently push the switch by using a slender non-conductive bar with a diameter of 1 to 2 mm.
- Operation data reset switch (for S2CP471/L1CP471)
  This switch initializes the operation data that is stored in NVRAM when the processor module is turned on.
  - HOLD: The operation data is maintained. Select this position during normal operation.
  - RESET: The operation data is initialized. When the HRDY lamp of the processor module is lit, turn the switch to the HOLD position.
- Battery ON/OFF switch (for SCP461 or SCP451)
  This switch selects whether or not to maintain the module management information (the operation data of NVRAM and the real time data of RTC) while the power is not supplied to processor modules for example in a power outage.
  - ON: The module information is maintained. Select this position during normal operation.
  - OFF: The module information is initialized.
- Front setting switches
  - DOMN: Set to OFF during normal operation. When set to ON, the STATUS lamps indicate the status of the domain number setting switches.
  - STA: Set to OFF during normal operation. When set to ON, the STATUS lamps indicate the status of the station number setting switches.
  - Switches other than above: Set to OFF.

The following figure is an example of STATUS lamp indication when the station number 5 (10000101) is set and the STA switch in the front is set to ON.

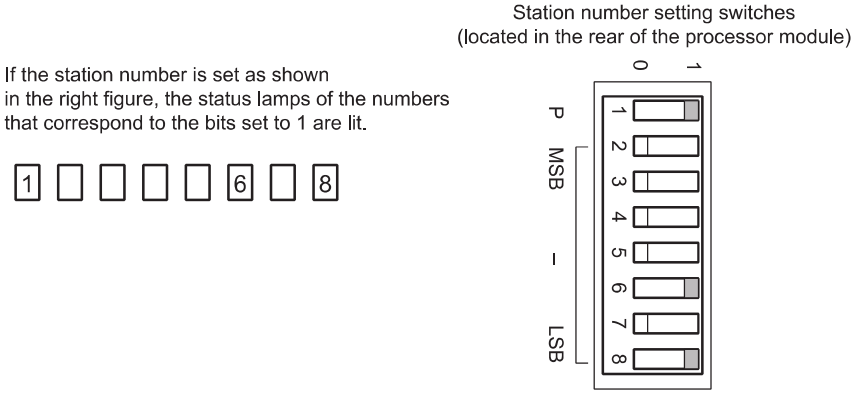


Figure B4.2-7 STATUS lamp indication when station number 5 is set

The following table describes the indication on the STATUS lamps when both DOMN and STA switches are set to OFF.

Table B4.2-1 STATUS lamp indication

STATUS lamps	Display	Description
1, 2	Operating Mode	• Running mode: 1 and 2 on • Waiting mode: 1 off, 2 on • Others: 1 and 2 off
3	Security level	Turns on when the security level is 2 (*1) and turns off otherwise.
4	SCS error status(*2)	Turns off when the system has an error and turns on otherwise.
5, 6, 7	Unused	Always on
8	Writing to flash memories	Turns off during writing and turns on otherwise.

*1: Security level 0 corresponds to offline level and security levels 1 and 2 correspond to online level.
*2: This lamp may be linked to the SYS_DIAG output.

SEE ALSO For more information about SYS_DIAG function block, refer to:

11.7, “SYS_DIAG (diagnostic information output)” in POU Reference Manual (IM 32P03B20-01EN)

For more information about the negotiation setting on the Vnet/IP interface card, refer to:

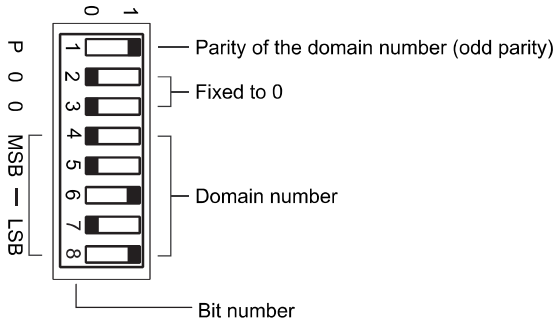
“■ Setting Up the Vnet/IP Interface Card” in B3.1, “Setting Up the Hardware” in Installation Guide (IM 32P01C50-01EN)

Station address setting switches: For domain numbers

A domain stands for a range of stations in a network connected by control bus. You can set the domain number in the range from 1 to 31. To set a required domain number, configure the switches as shown in the tables.

- Setting the switches
  0: In the orientation shown in the following figure, the switch is slid to the left.
  1: In the orientation shown in the following figure, the switch is slid to the right.

Bits 2 and 3 must always be set to 0.



MSB: Most Significant Bit
LSB: Least Significant Bit

Figure B4.2-8 Station address setting switches: For domain numbers

Table B4.2-2 Domain number and switch positions (1/2)

Domain number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit 1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0
Bit 2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Continues on the next page

Table B4.2-2 Domain number and switch positions (1/2) (Table continued)

Domain number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit 4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Bit 5	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
Bit 6	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0
Bit 7	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
Bit 8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

Table B4.2-3 Domain number and switch positions (2/2)

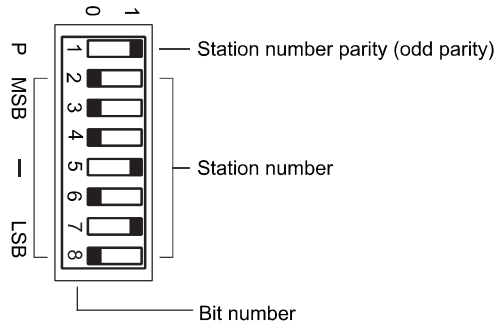
Domain number	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Bit 1	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0
Bit 2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit 4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Bit 5	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
Bit 6	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
Bit 7	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
Bit 8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Station address setting switches: For station numbers

You can set the station number in the range from 1 to 64. To set a required station number, configure the switches as shown in the following tables.

- Setting the switches
  0: In the orientation shown in the following figure, the switch is slid to the left.

  1: In the orientation shown in the following figure, the switch is slid to the right.



MSB : Most Significant Bit
LSB : Least Significant Bit

Figure B4.2-9 Station address setting switches: For station numbers

Table B4.2-4 Station number and switch positions (1/2)

Station number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit 1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0
Bit 2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Continues on the next page

Table B4.2-4 Station number and switch positions (1/2) (Table continued)

Station number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit 4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Bit 5	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
Bit 6	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0
Bit 7	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
Bit 8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

Table B4.2-5 Station number and switch positions (2/2)

Station number	17	18	-----	30	31	32	33	--------	60	61	62	63	64
Bit 1	1	1		1	0	0	1		1	0	0	1	0
Bit 2	0	0		0	0	0	0		0	0	0	0	1
Bit 3	0	0		0	0	1	1		1	1	1	1	0
Bit 4	1	1	-----	1	1	0	0	--------	1	1	1	1	0
Bit 5	0	0		1	1	0	0		1	1	1	1	0
Bit 6	0	0		1	1	0	0		1	1	1	1	0
Bit 7	0	1		1	1	0	0		0	0	1	1	0
Bit 8	1	0		0	1	0	1		0	1	0	1	0

B4.3 ESB bus coupler module

The ESB bus coupler module is installed in the SCU and communicates with the ESB bus interface module in the SNU.

There are ESB bus coupler modules for SCSs that support SIL 3 and those that support SIL 2.

- For SCSs that support SIL 3: SEC401/SEC402
- For SCSs that support SIL 2: L1EC401/L1EC402

SEC401/L1EC401 has one ESB bus port while SEC402/L1EC402 has two ESB bus ports. The ESB bus coupler module is always used in dual-redundant configuration.

Elements on the ESB bus coupler module

The following figure shows the elements on the ESB bus module.

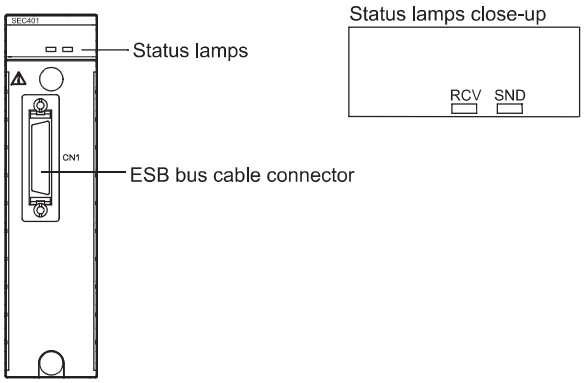


Figure B4.3-1 ESB bus coupler module (1 port)

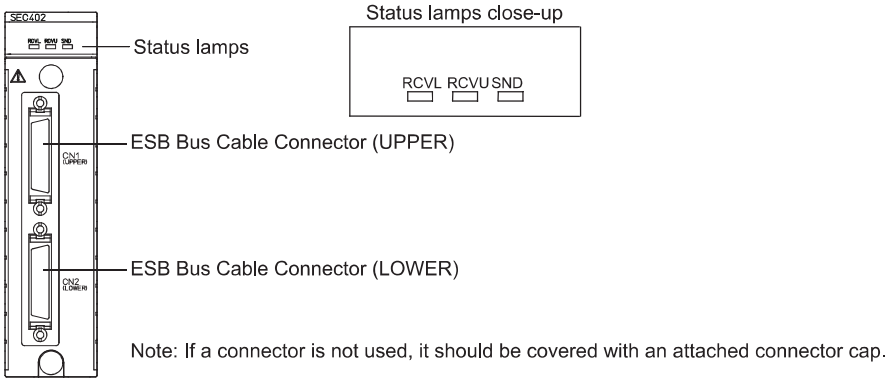


Figure B4.3-2 ESB bus coupler module (2 ports)

Status lamps (SEC401/L1EC401)

The status lamps indicate the device status as follows:

- RCV
  The lamp turns on when the module is receiving; otherwise, the lamp turns off.
- SND
  The lamp turns on when the module is sending; otherwise, the lamp turns off.

Status lamps (SEC402/L1EC402)

The status lamps indicate the device status as follows:

- RCVL
  The lamp turns on when the module is receiving through the ESB bus cable connector (LOWER); otherwise, the lamp turns off.
- RCVU
  The lamp turns on when the module is receiving through the ESB bus cable connector (UPPER); otherwise, the lamp turns off.
- SND
  The lamp turns on when the module is sending through the ESB bus cable connector (LOWER or UPPER); otherwise, the lamp turns off.

ESB bus cable connector

This connector is used to connect the ESB bus cable (Model: YCB301). Because the ESB bus coupler module comes at one end of the ESB bus, the module has a terminating resistor inside.

B4.4 ESB bus interface module

The ESB bus interface module is installed in SNU and communicates with the ESB bus coupler module in the SCU.

There are ESB bus interface modules for SCSs that support SIL 3 and those that support SIL 2.

- For SCSs that support SIL 3: SSB401
- For SCSs that support SIL 2: L1SB401

The ESB bus coupler module is always used in dual-redundant configuration.

Elements on the ESB bus interface module

The following figure shows the elements on the ESB bus interface module.

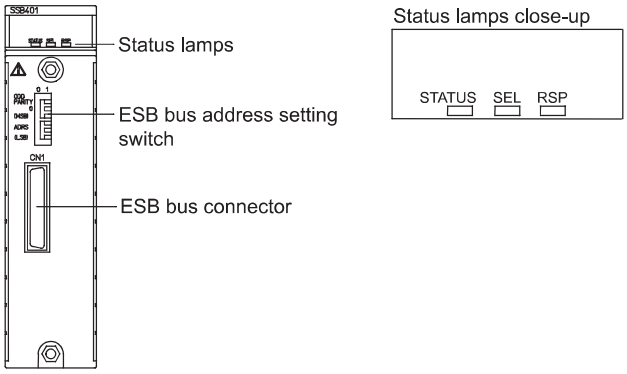


Figure B4.4-1 ESB bus interface module

Status lamps

The status lamps indicate the device status as follows:

- STATUS
  The lamp turns on when the module is normal; otherwise, the lamp turns off.
- SEL
  The lamp turns on when the module is sending data to an I/O module; otherwise, the lamp turns off.
- RSP
  The lamp turns on when the module is receiving data from an I/O module; otherwise, the lamp turns off.

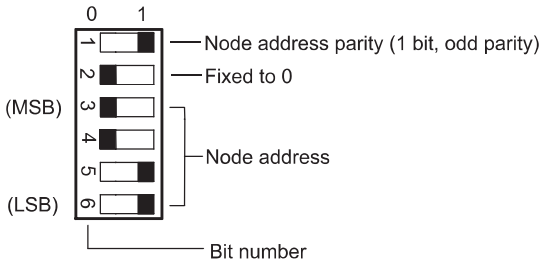
ESB bus address setting switches

When multiple SNUs are connected to the ESB bus, you can select an SNU to be accessed by setting the node number with these switches. For SCSP1, set the node number in the range of 2 to 10. For SCSP2/SCSP3/SCSL2, set the node number in the range of 2 to 14. Node number 1 is assigned to the SCU.

To set a required node number, configure the switches as shown in the table.

- Setting the switches
  0: In the orientation shown in the following figure, the switch is slid to the left.

  1: In the orientation shown in the following figure, the switch is slid to the right.



MSB : Most Significant Bit
LSB : Least Significant Bit

Figure B4.4-2 ESB bus address setting switches

Table B4.4-1 ESB bus address and switch positions

Node number	2	3	4	5	6	7	8	9	10	11	12	13	14
Bit 1	0	1	0	1	1	0	0	1	1	0	1	0	0
Bit 2	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit 3	0	0	0	0	0	0	1	1	1	1	1	1	1
Bit 4	0	0	1	1	1	1	0	0	0	0	1	1	1
Bit 5	1	1	0	0	1	1	0	0	1	1	0	0	1
Bit 6	0	1	0	1	0	1	0	1	0	1	0	1	0

ESB bus connector

This connector is used to connect the connector unit for ESB bus.

Connect the ESB bus cable (YCB301) to the connector unit for ESB bus. If the module comes at the end of the ESB bus, connect the ESB bus cable to the connector unit with terminator for ESB bus.

The following figure shows the connector unit for ESB bus and the connector unit with terminator for ESB bus.

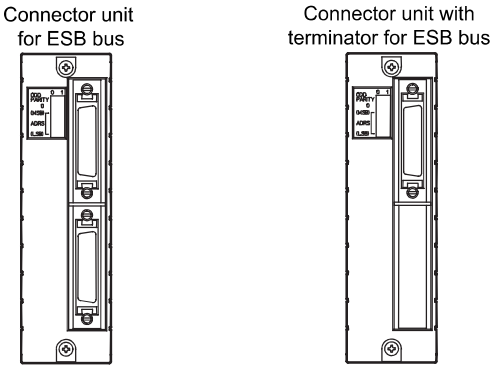


Figure B4.4-3 Connector unit for ESB bus

B4.5 Optical ESB bus repeater module

The optical ESB bus repeater module converts electric signals to optical signals, extending the transmission distance. The optical ESB bus repeater modules are installed in the SCU, SNU, and unit for optical bus repeater module. The unit where the module can be installed depends on the module type (master or slave).

There are optical ESB bus repeater modules for SCSs that support SIL 3 and those that support SIL 2. The optical ESB bus repeater module is always used in dual-redundant configuration. The following table describes the types of optical ESB bus repeater modules.

Table B4.5-1 Types of optical ESB bus repeater modules

Model	Name	Description
For SCSs that support SIL 3 • SNT401 • SNT411 For SCSs that support SIL 2 • L1NT401 • L1NT411	Optical ESB bus repeater master module	• Mountable units: SCU SNU Unit for optical bus repeater module
		• Module types: With ESB bus branch connector With ESB bus terminator
		• Maximum transmission distance of fiber-optic cables(*1) 5 km: SNT401/L1NT401 50 km: SNT411/L1NT411(*2)
For SCSs that support SIL 3 • SNT501 • SNT511 For SCSs that support SIL 2 • L1NT501 • L1NT511	Optical ESB bus repeater slave module	• Mountable units: SNU Unit for optical bus repeater module
		• Module types: With ESB bus terminator
		• Maximum transmission distance of fiber-optic cables(*1) 5 km: SNT501/L1NT501 50 km: SNT511/L1NT511(*2)

*1: The maximum transmission distance is 50 km even if repeated for two times by the optical ESB bus repeater modules.
*2: The minimum distance is 5 km.

Elements on the optical ESB bus repeater module

The following figure shows the elements on the optical ESB bus repeater modules.

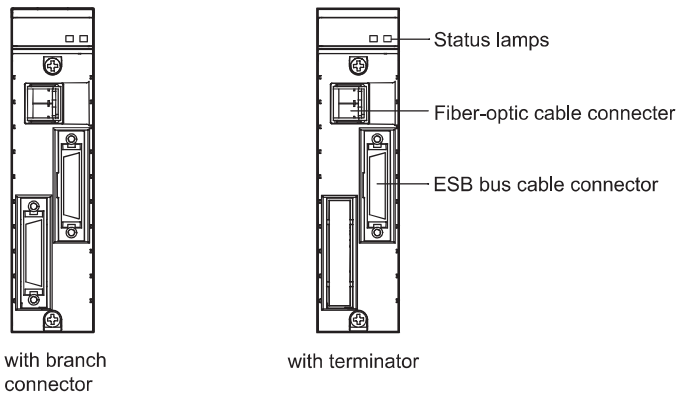


Figure B4.5-1 Optical ESB bus repeater module

Status lamps

The following figure shows the status lamps of the optical ESB bus repeater module.

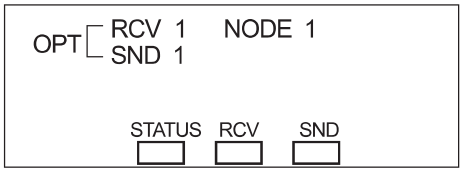


Figure B4.5-2 Status lamps

The status lamps indicate the device status as follows:

- STATUS
  The lamp turns on when the module is normal; otherwise, the lamp turns off.
- RCV
  The lamp turns on when the module is receiving electrical signal. Otherwise, the lamp turns off.
- SND
  The lamp turns on when the module is sending electrical signal. Otherwise, the lamp turns off.
- OPT RCV
  The figure “1” lamp turns on when the module is receiving optical signal. Otherwise, the lamp turns off.
- OPT SND
  The figure “1” lamp turns on when the module is sending optical signal. Otherwise, the lamp turns off.
- NODE
  This lamp indicates the operation mode setting. The figure “1” lamp turns on when bit 1 of the unit type setting switch is set to "1." Otherwise, the lamp turns off.

Fiber-Optic cable connector

This connector is used to connect the fiber-optic cable.

SEE ALSO For more information about the specifications of fiber-optic cables, refer to:

- ProSafe-RS Installation Guidance (TI 32P01J10-01EN)
- ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

ESB bus cable connector

This connector is used to connect the ESB bus cable (Model: YCB301).

The optical ESB bus repeater slave module is always at the end of the ESB bus, so a connector unit with ESB bus terminator is provided.

Unit type setting switch

Set this switch according to the type of the unit where the optical ESB bus repeater module is installed. When you change the switch setting, you must remove the connector unit for ESB bus.

The following figure shows the unit type setting switch.

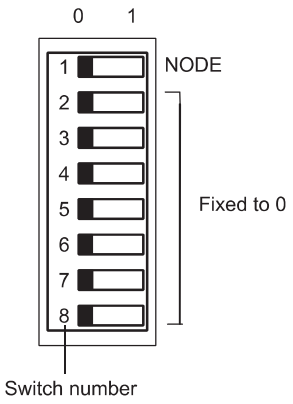


Figure B4.5-3 Unit type setting switch

- Switch 1
  Set to 0 if you install the module to the unit for optical bus repeater module. Set to 1 if you install the module to SCU or SNU.
- Switches 2 to 5
  Always set to 0.
- Switches 6 to 8
  Set to 0 during normal operation. These switches are used for maintenance.

B4.6 N-ESB bus coupler module

The N-ESB bus coupler module (Model: S2EN402, S2EN404) is installed in the SCU and communicates with the N-ESB bus modules (Model: S2EN501) in N-IO nodes. S2EN402 has two N-ESB bus ports, whereas S2EN404 has four N-ESB bus ports. The N-ESB bus coupler module can be used in SCSP3.

The N-ESB bus coupler module is always used in dual-redundant configuration.

Elements on the N-ESB bus coupler module

The following figures show the elements on the N-ESB bus coupler modules.

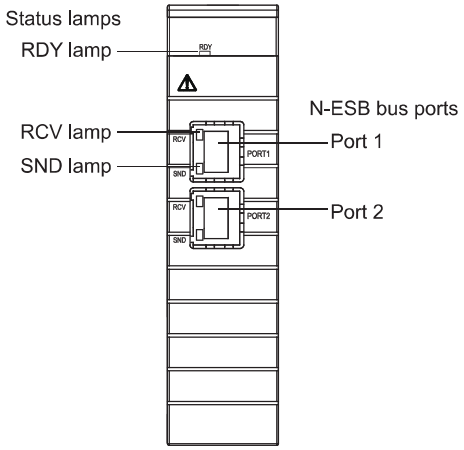


Figure B4.6-1 S2EN402

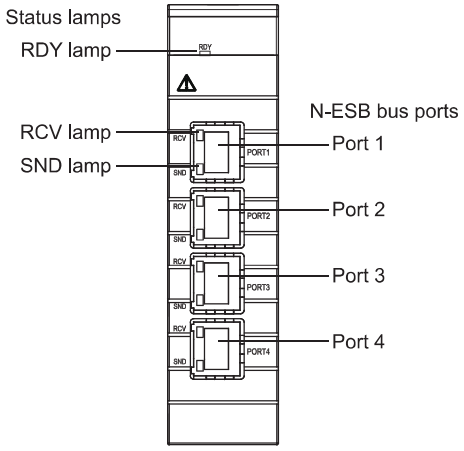


Figure B4.6-2 S2EN404

Status lamps

The N-ESB bus coupler module has the following status lamps.

- RDY
  The lamp turns on when the module is normal; otherwise, the lamp turns off.
- RCV
  The lamp turns on when the module is receiving; otherwise, the lamp turns off. The RCV lamp is provided for each port.
- SND

The lamp turns on when the module is sending; otherwise, the lamp turns off. The SND lamp is provided for each port.

- **N-ESB bus ports**

  Cables for N-ESB bus are connected to these ports. For unused ports, put the cover that came with the module.

B4.7 FIO I/O modules and their peripherals

The following types of FIO I/O modules are available:

- Analog I/O modules
- Digital I/O modules
- Communication modules

Peripherals for the FIO I/O modules are as follows:

- Pressure clamp terminal block
- Connector cover for MIL cable
- Terminal board
- Relay board

SEE ALSO

For more information about restrictions on FIO I/O module installation to SCSs that support SIL 3, refer to:

ProSafe-RS Outline of I/O Modules (for FIO) (GS 32P06K60-01EN)

For more information about restrictions on FIO I/O module installation to SCSs that support SIL 2, refer to:

ProSafe-RS Lite Outline of I/O Modules (GS 32P56K60-01EN)

B4.7.1 Analog I/O modules

An analog input module receives analog signals and converts them into internal data of SCU. An analog output module converts the internal data of SCU into analog signals and outputs them. There are analog I/O modules for SCSs that support SIL 3 and those that support SIL 2.

- For SCSs that support SIL 3
  - SAI143: Analog input module (4 to 20 mA input, 16 channels, module isolation)
  - SAV144: Analog input module (1 to 5 V DC/1 to 10 V DC input, 16 channels, module isolation)
  - SAT145: TC/mV input module (16 channels, isolated channels)
  - SAR145: RTD input module (16 channels, isolated channels)
  - SAI533 : Analog output module (4 to 20 mA output, 8 channels, module isolation)
- For SCSs that support SIL 2
  - L1AI143: Analog input module (4 to 20 mA input, 16 channels, module isolation)
  - L1AV144: Analog input module (1 to 5 V DC/1 to 10 V DC input, 16 channels, module isolation)
  - L1AT145: TC/mV input module (16 channels, isolated channels)
  - L1AR145: RTD input module (16 channels, isolated channels)
  - L1AI533: Analog output module (4 to 20 mA output, 8 channels, module isolation)

Elements on the analog I/O modules

An analog I/O module and field devices are connected through a pressure clamp terminal block, MIL cable, or signal cable. The available connection methods differ for each module.

The following figure shows the elements on the module that supports connection through pressure clamp terminals and a MIL cable and the module that has a signal cable interface adapter.

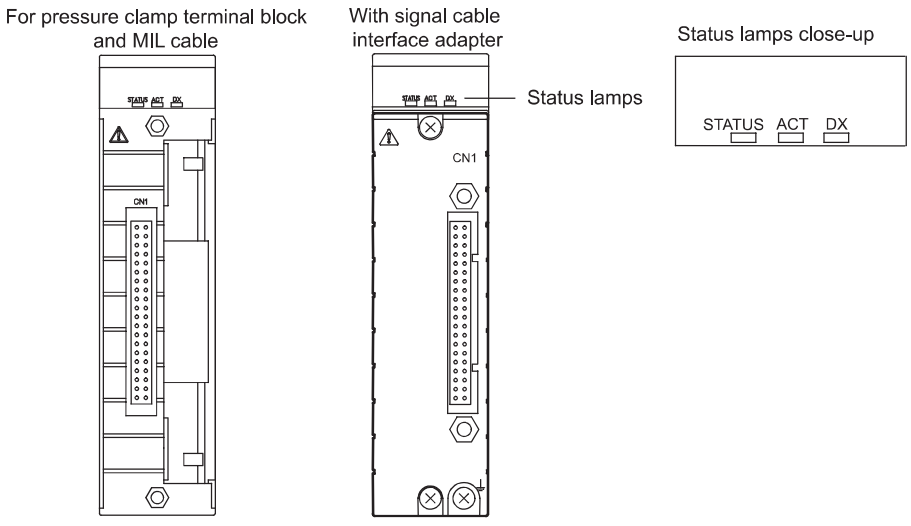


Figure B4.7.1-1 Analog I/O modules

SEE ALSO For more information about pressure clamp terminal blocks, refer to:

B4.7.4, “Pressure clamp terminal blocks” on page B4-31

For more information about the connector cover for MIL cable, refer to:

B4.7.5, “Connector cover for MIL cable” on page B4-32

For more information about how to connect analog I/O modules and field devices, refer to:

D1.1, “Types of FIO I/O module signal connection” on page D1-2

Status lamps

The status lamps indicate the device status as follows:

- STATUS
  On: Hardware normal

  Off: Other than the above
- ACT
  On: Operating

  Off: Stopped operating, or standby in dual-redundant configuration

TIP SAI143 (style S4 or later) and L1AI143 can reset the error detection status of smoke and heat detectors. The ACT lamp is off while SAI143/L1AI143 is resetting the error detection status of detectors.

- DX
  On: In dual-redundant configuration

  Off: Other than the above

SEE ALSO For more information about the function to reset the error detection status of Smoke and Heat Detector by SAI143 (style S4 or later) and L1AI143, refer to:

A3.4.1, “Device reset function with FIO” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

Setting pins of the current input module

In the case of current input module (Model: SAI143/L1AI143), there is an option to select whether to supply power to the transmitter for each channel by using the setting pins, depending on the type of the transmitter. The following figure shows the right side view of the current input module and the jumper positions on the setting pins when supplying power (2-wire) and not supplying power (4-wire) to the transmitter.

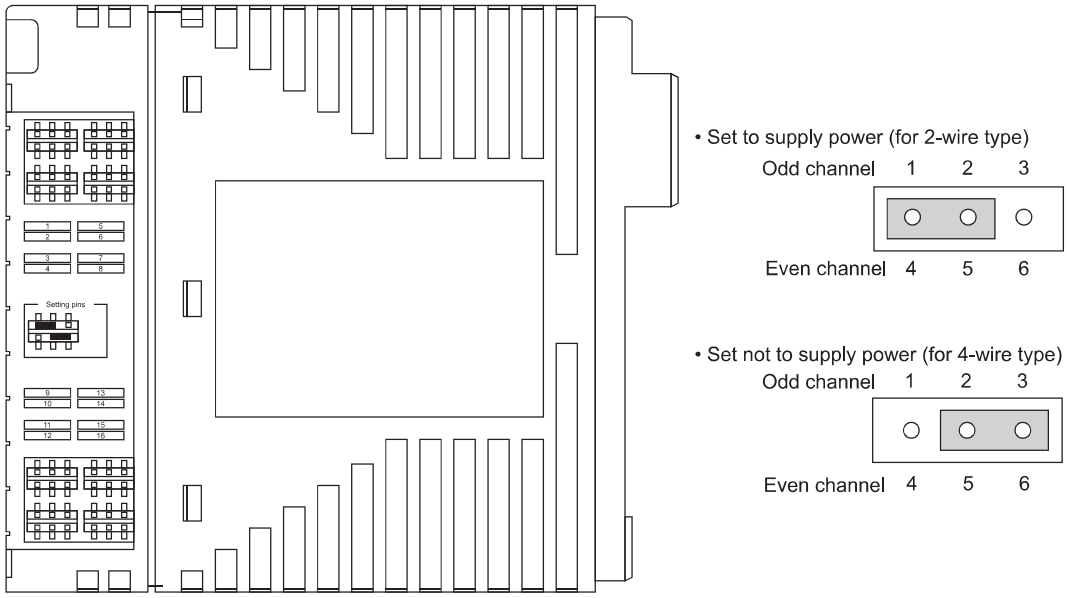


Figure B4.7.1-2 Setting pins of the current input module

The following figure shows the relationship between the setting pins and channel numbers. The factory-set default is “Yes”, meaning supply power to a 2-wire type transmitter.

Display of setting pins	Setting pin	Power supply to transmitter		Remarks	Setting pin	Power supply to transmitter		Remarks
		Yes (2-wire)	No (4-wire)	Channel No.		Yes (2-wire)	No (4-wire)	Channel No.
S1 to S16 1 2 3 4 5 6	S1	1 2	2 3	1	S5	1 2	2 3	5
	S2	4 5	5 6	2	S6	4 5	5 6	6
	S3	1 2	2 3	3	S7	1 2	2 3	7
	S4	4 5	5 6	4	S8	4 5	5 6	8
	S9	1 2	2 3	9	S13	1 2	2 3	13
	S10	4 5	5 6	10	S14	4 5	5 6	14
	S11	1 2	2 3	11	S15	1 2	2 3	15
	S12	4 5	5 6	12	S16	4 5	5 6	16

Figure B4.7.1-3 Setting pins of the current input module

B4.7.2 Digital I/O modules

A digital input module receives digital (discrete) signals and converts them into internal data of SCU. A digital output module converts the internal data of SCU into digital (discrete) signals and outputs them.

There are digital I/O modules for SCSs that support SIL 3 and those that support SIL 2.

- For SCSs that support SIL 3
  - SDV144: Digital input module (16 channels, module isolation)
  - SDV521: Digital output module (24 V DC/2 A, 4 channels, module isolation)
  - SDV526: Digital output module (100-120 V AC, 4 channels, module isolation)
  - SDV531: Digital output module (8 channels, module isolation)
  - SDV53A: Digital output module (48 V DC, 8 channels, module isolation)
  - SDV541: Digital output module (16 channels, module isolation)
- For SCSs that support SIL 2
  - L1DV144: Digital input module (16 channels, module isolation)
  - L1DV521: Digital output module (24 V DC/2 A, 4 channels, module isolation)
  - L1DV526: Digital output module (100 to 120 V AC, 4 channels, module isolation)
  - L1DV531: Digital output module (8 channels, module isolation)
  - L1DV53A: Digital output module (48 V DC, 8 channels, module isolation)
  - L1DV541: Digital output module (16 channels, module isolation)

Elements on the digital I/O modules

A digital I/O module and field devices are connected through a pressure clamp terminal block, MIL cable, or signal cable. The available connection methods differ for each module.

The following figure shows the elements on the module that supports connection through pressure clamp terminals and a MIL cable and the module that has a signal cable interface adapter.

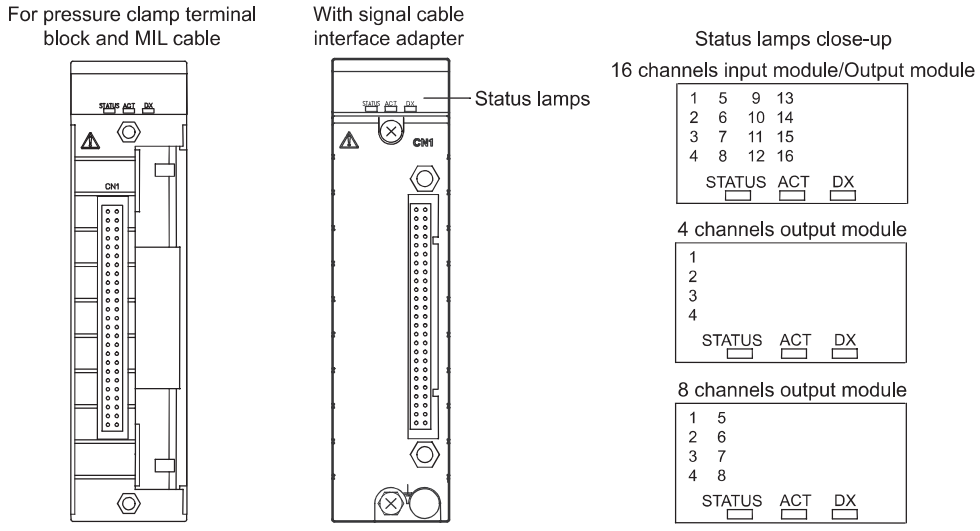


Figure B4.7.2-1 Digital I/O modules

SEE ALSO For more information about pressure clamp terminal blocks, refer to:

B4.7.4, “Pressure clamp terminal blocks” on page B4-31

For more information about the connector cover for MIL cable, refer to:

B4.7.5, “Connector cover for MIL cable” on page B4-32

For more information about how to connect analog I/O modules and field devices, refer to:

D1.1, “Types of FIO I/O module signal connection” on page D1-2

Status lamps

The status lamps indicate the device status as follows:

- STATUS
  The lamp turns on when the hardware is functioning normally; otherwise, the lamp turns off.
- ACT
  The lamp turns on when the module is operating and turns off when the module is stand-by in dual-redundant configuration or not operating.
- DX
  The lamp turns on when the module is in dual-redundant configuration; otherwise, the lamp turns off.
- Channel numbers
  The lamp turns on when the input or output on the channel is ON; otherwise the lamp turns off.

Behavior of SDV531/L1DV531 on short-circuit error

When a short-circuit occurs on the field side, SDV531 and L1DV531 behave as follows:

- SDV531 (other than SDV531-S13) and L1DV531
  When a short circuit occurs on the field side, only the output on the relevant channel becomes OFF. When the failure on the field side is resolved, the output channel can be recovered by performing the Output Enable Operation for that channel. Then, the recovered channel outputs the application logic value. The channel continues to output the failsafe value until the Output Enable Operation is performed.
- SDV531-S13
  The Output Shutoff Switch is activated by a short circuit on the field side, and the output on all channels of the module becomes OFF. When the failure on the field side is resolved, the outputs can be recovered by starting the output module from the SCS Status Management Window and performing the Output Enable Operation. Then, the recovered channels output the application logic value. All the outputs remain OFF until the Output Enable Operation is performed.

B4.7.3 Communication modules

Communication modules are used for communication between the SCS and external devices. The communication modules support Modbus slave communication, subsystem communication, and safety subsystem communication.

The following types of communication modules are available:

- ALR111: Serial communication module (RS-232C, 2 ports)
- ALR121: Serial communication module (RS-422/RS-485, 2 ports)
- ALE111: Ethernet communication module
- S2LP131: Fire and gas communication module

ALR111, ALR121, and ALE111 can be used with SCSs that support SIL 3 and those that support SIL 2. S2LP131 can be used in SCSP3 (SCS supporting SIL 3 which is configured with S2SC70□).

IMPORTANT

When using ALE111, you must use the style S1 module with unit revision U:2 or later. The unit revision is indicated on the top of the module. However, the unit revision is not indicated if it is U:0.

TIP

The fire and gas communication mode communicates with YFGW410. YFGW410 is called a PROFINET IO-device.

Elements on the serial communication module

The following figure shows the elements on the serial communication modules.

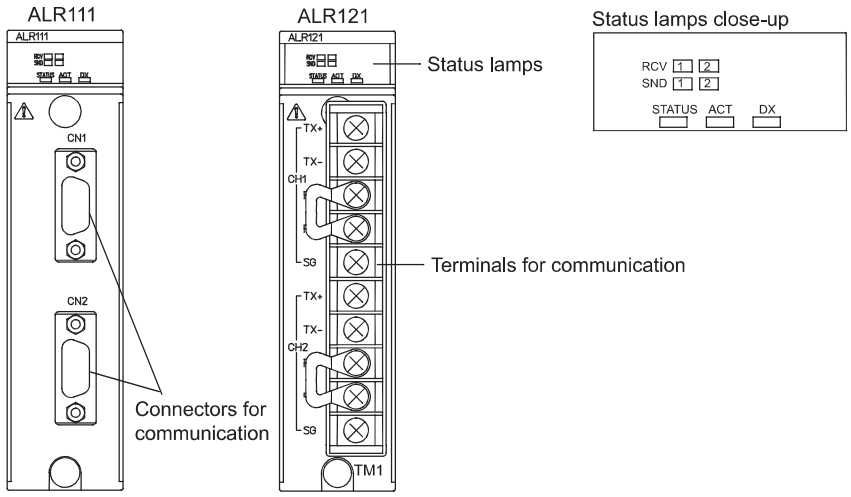


Figure B4.7.3-1 Serial communication module

Status lamps

The status lamps indicate the device status as follows:

- STATUS
  On: Hardware normal

  Off: Other than the above

- ACT
  On: Operating

  Off: Standby in dual-redundant configuration, or not operating
- DX
  On: Normal in dual-redundant configuration

  Off: Error in dual-redundant configuration, or operating in non-redundant configuration
- RCV-1
  On: CH1 is receiving data

  Off: Other than the above
- SND-1
  On: CH1 is sending data

  Off: Other than the above
- RCV-2
  On: CH2 is receiving data

  Off: Other than the above
- SND-2
  On: CH2 is sending data

  Off: Other than the above

Elements on the Ethernet communication module

The following figure shows the elements on the Ethernet communication module.

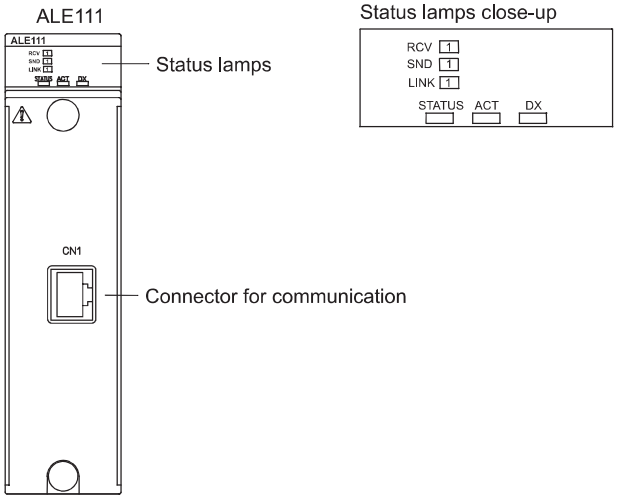


Figure B4.7.3-2 Ethernet communication module

Status lamps

The status lamps indicate the device status as follows:

- STATUS
  On: Hardware normal

  Off: Other than the above
- ACT
  On: Operating

  Off: Standby in dual-redundant configuration, or not operating

- DX
  On: Normal in dual-redundant configuration

  Off: Error in dual-redundant configuration, or operating in non-redundant configuration
- RCV
  On: Receiving data

  Off: Other than the above
- SND
  On: Sending data

  Off: Other than the above
- LINK
  On: Link is established

  Off: Other than the above

Elements on the fire and gas communication module

The following figure shows the elements on the fire and gas communication module.

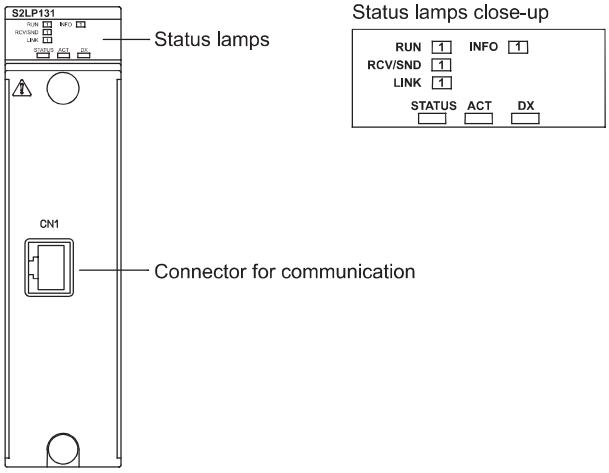


Figure B4.7.3-3 Fire and gas communication module

Status lamps

The status lamps indicate the device status as follows:

- STATUS
  On: Hardware normal

  Off: Other than the above
- ACT
  On: Operating

  Off: Other than the above
- DX
  Always off
- RUN
  On: Communicating normally

  Off: Other than the above
- RCV/SND
  Flashing: Sending or receiving data

Off: Other than the above

- LINK
  On: Link is normal

  Off: Other than the above

- INFO
  On: Configuration information that matches the configuration of the PROFINET IO-device connected to S2LP131 is not loaded on S2LP131. (*1)

  Flashing: Duplicate address between S2LP131 and PROFINET IO-device. (*2)

  Off: Configuration information that matches the configuration of the PROFINET IO-device connected to S2LP131 is loaded on S2LP131.

*1: If YFGW410 is used as a PROFINET IO-device, the lamp does not turn on although the configuration information that matches the configuration is not loaded.
*2: If YFGW410 is used as a PROFINET IO-device, the lamp does not flash although the address duplicates.

SEE ALSO For more information about configuration of S2LP131, refer to:

E1.5, “Engineering for fire and gas communication” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

B4.7.4 Pressure clamp terminal blocks

The pressure clamp terminal block is used to connect the signal cables of field devices directly to the I/O module. There are pressure clamp terminal blocks for SCSs that support SIL 3 and those that support SIL 2.

- For SCSs that support SIL 3
  - STA4S: Pressure clamp terminal block for analog I/O
  - STB4S: Pressure clamp terminal block for digital I/O
  - STA4D: Dual-redundant pressure clamp terminal block for analog I/O
  - STB4D: Dual-redundant pressure clamp terminal block for digital I/O
- For SCSs that support SIL 2
  - L1TA4S: Pressure clamp terminal block for analog I/O
  - L1TB4S: Pressure clamp terminal block for digital I/O
  - L1TA4D: Dual-redundant pressure clamp terminal block for analog I/O
  - L1TB4D: Dual-redundant pressure clamp terminal block for digital I/O

The following figure shows the appearance of the pressure clamp terminal blocks for single and dual-redundant configurations. The pressure clamp terminal blocks for analog I/O and digital I/O are functionally different but have the same appearance.

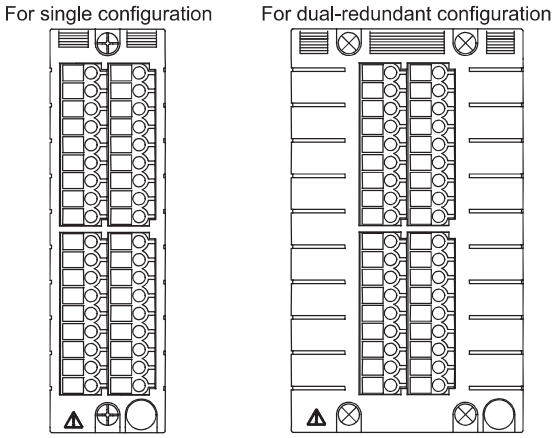


Figure B4.7.4-1 Pressure clamp terminal blocks

B4.7.5 Connector cover for MIL cable

A connector cover for MIL cable over the I/O modules is used to connect the MIL cable to the connector securely. There are connector covers for MIL cable for SCSs that support SIL 3 and those that support SIL 2.

- For SCSs that support SIL 3
  - SCCC01: For flat ribbon cables
  - SCCC02: For discrete wire cables (DI, DO cables)
- For SCSs that support SIL 2
  - L1CCC01: For flat ribbon cables
  - L1CCC02: For discrete wire cables (DI, DO cables)

The following figure shows the appearance of the connector cover for MIL cable.



Figure B4.7.5-1 Example of a connector cover for MIL cable (flat ribbon cables)

B4.7.6 Terminal boards (for FIO node)

The terminal boards are used to pass field device signals to I/O modules. Terminal boards can be used with SCSs that support SIL 3 and those that support SIL 2. All models support the single and dual-redundant configurations of I/O modules.

Table B4.7.6-1 Types of rack mountable terminal boards

Terminal board	Name	Connectable I/O module	
		For SCSs that support SIL 3	For SCSs that support SIL 2
SEA4D	Terminal board for analog I/O (single and dual-redundant)	SAI143, SAI533, SAV144	L1AI143, L1AI533, L1AV144
SED2D	Terminal board for digital I/O (single and dual-redundant)	SDV521	L1DV521
SED3D	Terminal board for digital output (single and dual-redundant)	SDV53A	L1DV53A
SED4D	Terminal board for digital I/O (single and dual-redundant)	SDV144, SDV531, SDV541	L1DV144, L1DV531, L1DV541
SWD2D	Terminal board for digital output (single and dual-redundant)	SDV526	L1DV526

Table B4.7.6-2 Types of DIN rail mountable terminal boards

Terminal board	Name	Connectable I/O module	
		For SCSs that support SIL 3	For SCSs that support SIL 2
SBA4D	Terminal board for analog I/O (single and dual-redundant)	SAI143, SAI533, SAV144	L1AI143, L1AI533, L1AV144
SBT4D	Terminal board for TC/mV (single and dual-redundant)	SAT145	L1AT145
SBR4D	Terminal board for RTD input (single and dual-redundant)	SAR145	L1AR145
SBD2D	Terminal board for digital output (single and dual-redundant)	SDV521	L1DV521
SBD3D	Terminal board for digital output (single and dual-redundant)	SDV531, SDV53A	L1DV531, L1DV53A
SBD4D	Terminal board for digital I/O (single and dual-redundant)	SDV144, SDV541	L1DV144, L1DV541
S1BB4D	Terminal board for analog input (3-wire, single and dual-redundant)	SAI143	L1AI143

Elements on rack mountable terminal boards

The following figures show the elements on the rack mountable terminal boards.

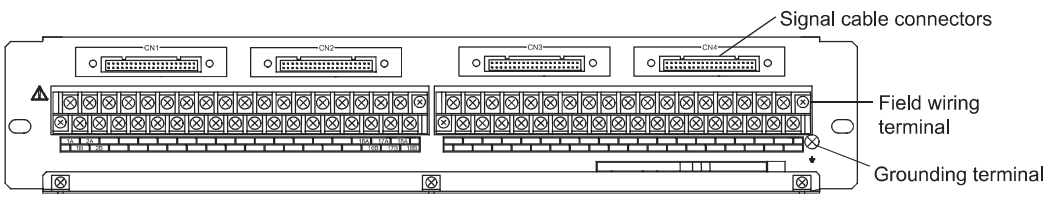


Figure B4.7.6-1 SEA4D

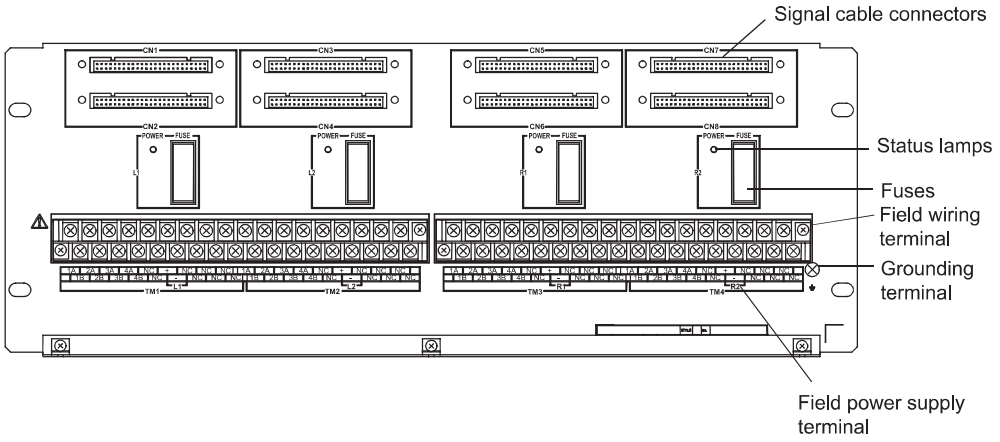


Figure B4.7.6-2 SED2D

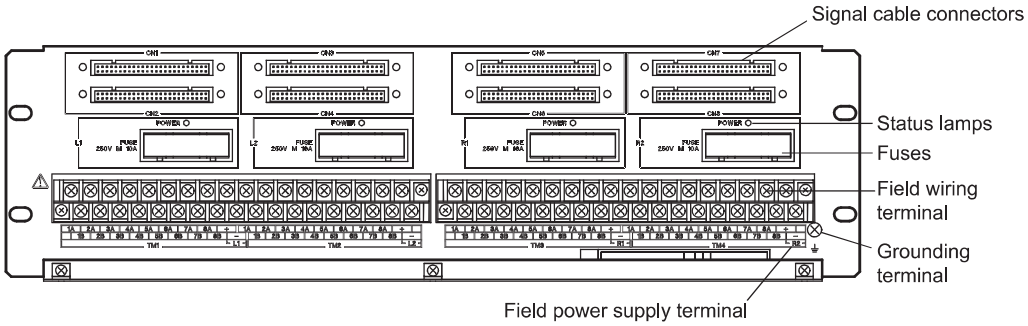


Figure B4.7.6-3 SED3D

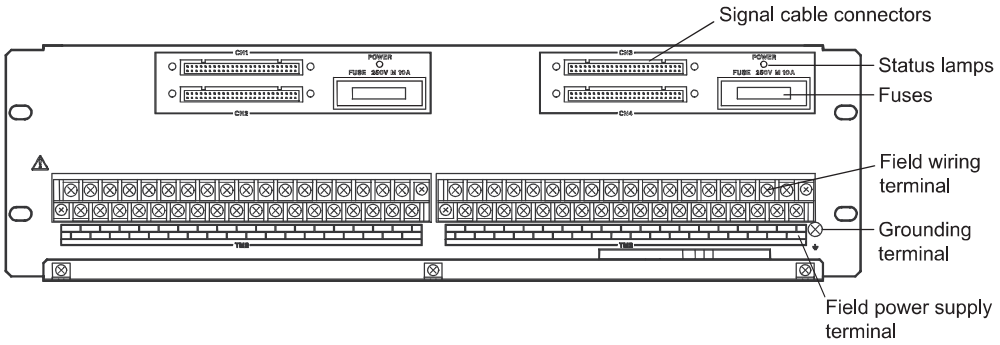


Figure B4.7.6-4 SED4D

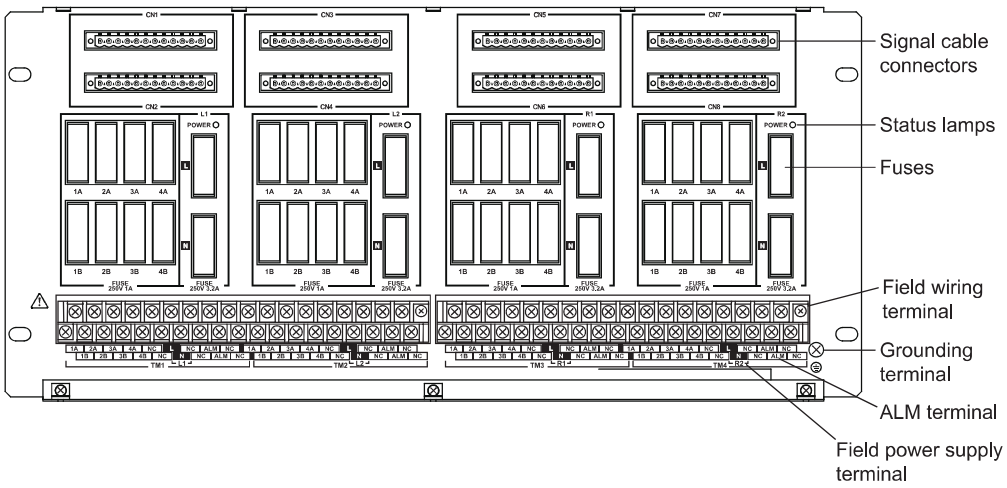


Figure B4.7.6-5 SWD2D

Status lamps

SED2D, SED3D, SED4D, and SWD2D have status lamps.

The status lamps indicate the device status as follows:

- POWER
  The lamp turns on when the field power is supplied and also the fuse is not blown; otherwise, the lamp turns off.

ALM terminals

SWD2D has ALM terminals. Each of the terminal groups TM1 to TM4 has a pair of ALM terminals for sending a contact signal when fuse is blown. When any fuse (1A to 4A, 1B to 4B, L and N) of a terminal group is blown, the contact of the ALM terminals becomes closed.

When the external relays are connected, a surge absorber should be used for inhibiting the noises.

SEE ALSO For more information about the alarm terminals of SWD2D, refer to:

- ProSafe-RS Field Device Connection (for FIO) (GS 32Q06J10-31E)
- ProSafe-RS Lite Field Device Connection (GS 32P56J10-01EN)

Elements on DIN rail mountable terminal boards

The following figures show the elements on DIN rail mountable terminal boards.

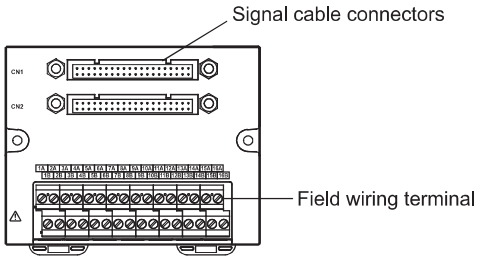


Figure B4.7.6-6 SBA4D

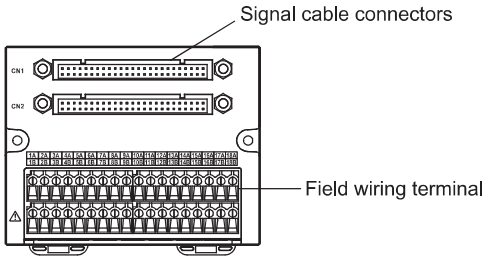


Figure B4.7.6-7 SBT4D

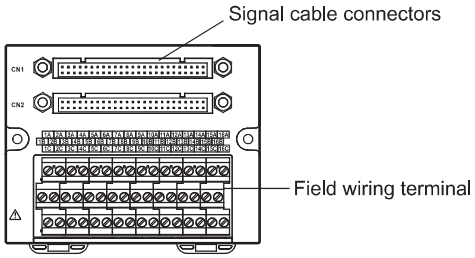


Figure B4.7.6-8 SBR4D

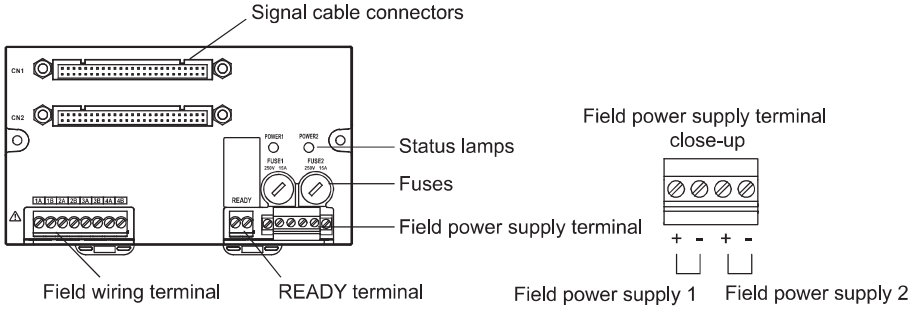


Figure B4.7.6-9 SBD2D

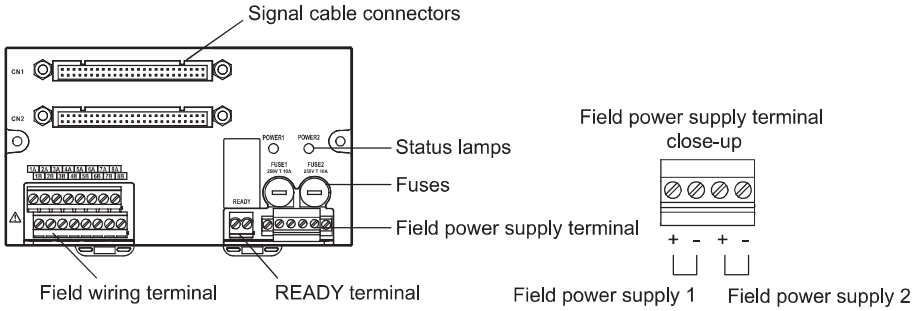


Figure B4.7.6-10 SBD3D

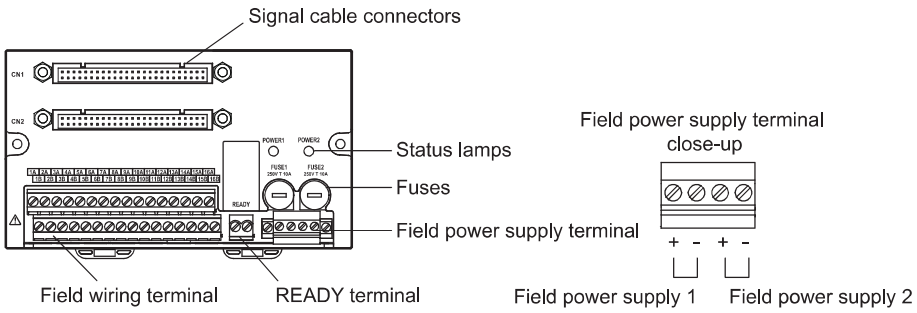


Figure B4.7.6-11 SBD4D

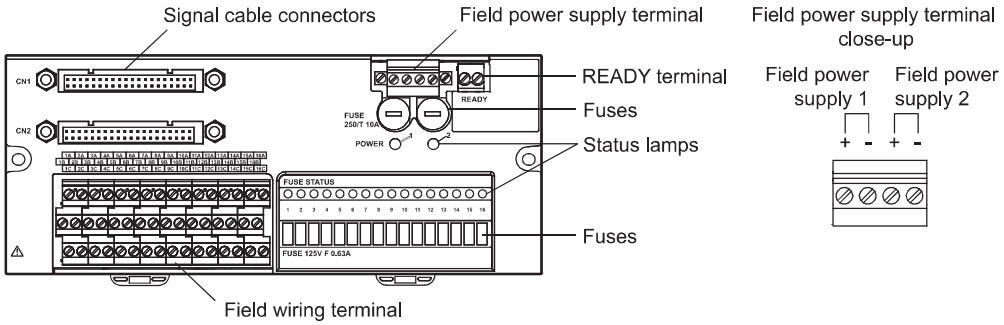


Figure B4.7.6-12 S1BB4D

Status lamps

SBD2D, SBD3D, SBD4D, and S1BB4D have status lamps.

The status lamps indicate the device status as follows:

- POWER1
  The lamp turns on when field power 1 is supplied and also fuse 1 is not blown; otherwise, the lamp turns off.
- POWER2
  The lamp turns on when field power 2 is supplied and also fuse 2 is not blown; otherwise, the lamp turns off.
- FUSE STATUS
  This lamp is provided for each channel of S1BB4D. The lamp turns on when the fuse is normal; otherwise, the lamp turns off. If this lamp is off, power is not supplied to the field device.

READY terminals

SBD2D, SBD3D, SBD4D, and S1BB4D have READY terminals. The contact between the READY terminals becomes closed when field powers 1 and 2 are supplied and also the two fuses are not blown. Otherwise, the contact between the READY terminals is open.

If an external relay is used, a surge absorber should be used for noise prevention.

B4.7.7 Relay boards

The output voltage of a digital output module is applied to the relay coils on the relay board to produce relay contact signals. Relay boards can be used with SCSs that support SIL 3 and those that support SIL 2.

The following table describes the available models of rack mountable relay boards. The relay output status can be read back by connecting the digital input module (SDV144/L1DV144).

Table B4.7.7-1 Types of 19-inch rack mountable relay boards

Relay board	Name	Connectable I/O module	
		For SCSs that support SIL 3	For SCSs that support SIL 2
SRM53D	Relay board (8 x 2 dry contact outputs)	SDV531	L1DV531
		SDV144 (readback)	L1DV144 (readback)
SRM54D	Relay board (16 x 1 dry contact outputs)	SDV541	L1DV541
		SDV144 (readback)	L1DV144 (readback)

The following table describes the available model of DIN rail mountable relay board.

Table B4.7.7-2 Types of DIN rail mountable relay boards

Relay board	Name	Connectable I/O module	
		For SCSs that support SIL 3	For SCSs that support SIL 2
SBM54D	Relay board for digital output	SDV541	L1DV541

Elements on rack mountable relay boards

The following figure shows the elements on SRM53D.

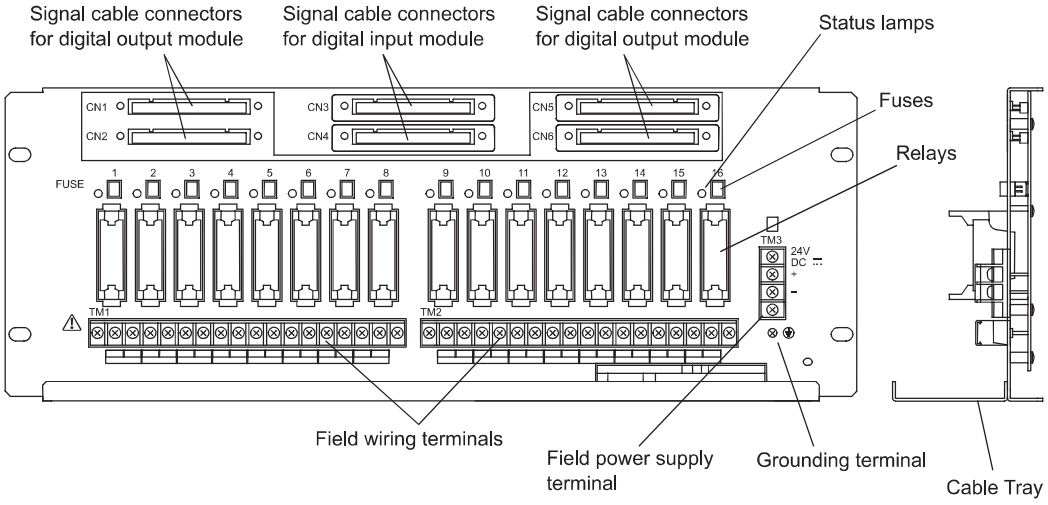


Figure B4.7.7-1 SRM53D (with cable tray)

The following figure shows the elements on SRM54D.

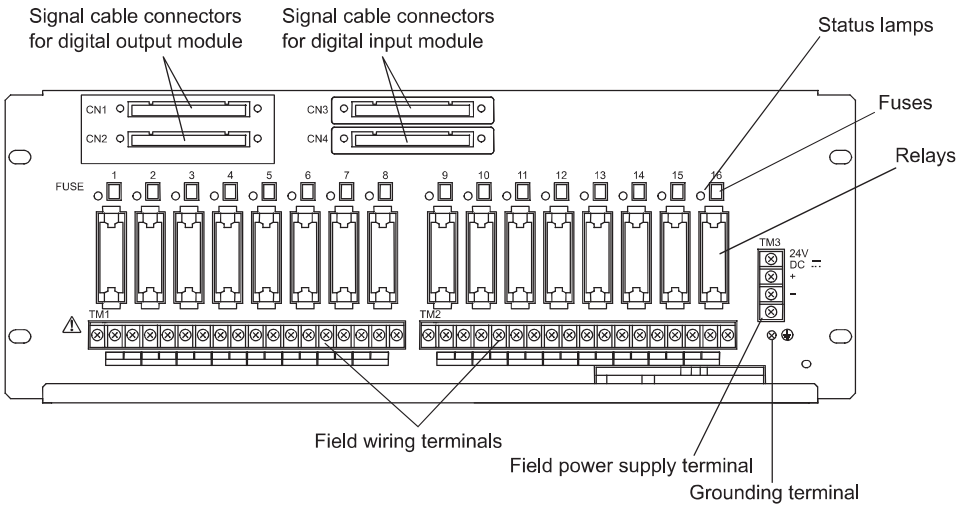


Figure B4.7.7-2 SRM54D

● Status lamps

The status lamps indicate the device status as follows:

- Status lamps (1 to 16)
  The lamp turns on when the signal from the digital output module is ON; otherwise, the lamp turns off.

SEE ALSO For more information about the status lamps of SRM53D, refer to:

"● Signal connection between SRM53D and digital I/O modules" on page D1-34

For more information about the status lamps of SRM54D, refer to:

"● Signal connection between the SRM54D and digital I/O modules" on page D1-37

■ Elements on DIN rail mountable relay boards

The following figure shows the elements on SBM54D.

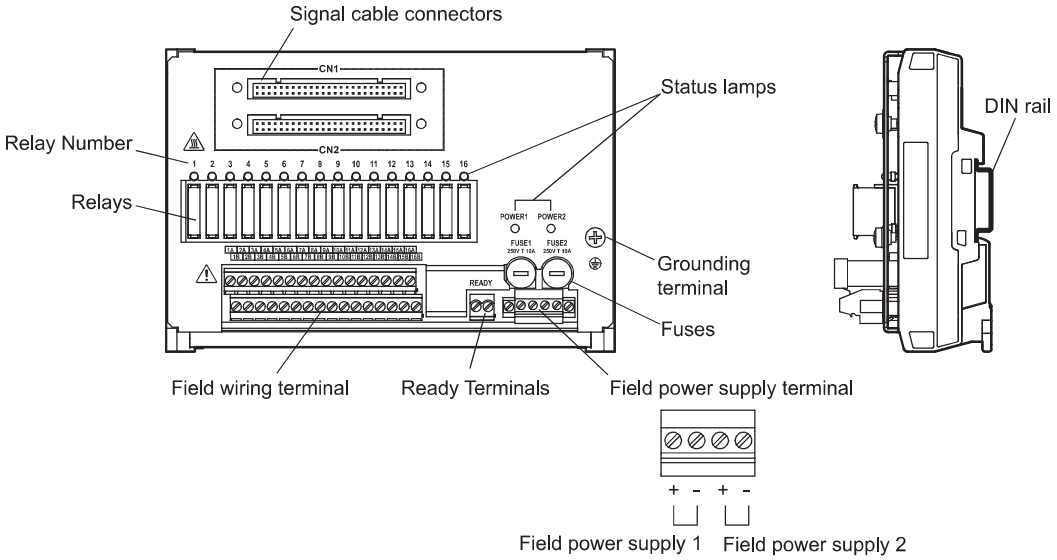


Figure B4.7.7-3 SBM54D

Status lamps

The status lamps indicate the device status as follows:

- POWER1
  The lamp turns on when field power 1 is supplied and also fuse 1 is not blown; otherwise, the lamp turns off.
- POWER2
  The lamp turns on when field power 2 is supplied and also fuse 2 is not blown; otherwise, the lamp turns off.
- Status lamps (1 to 16)
  The lamp turns on when the signal from the digital output module is ON; otherwise, the lamp turns off.

SEE ALSO For more information about status lamps, refer to:

"● Signal connections between SBM54D and digital I/O modules" on page D1-39

READY terminals

The contact between the READY terminals becomes closed when field powers 1 and 2 are supplied and also the two fuses are not blown. Otherwise, the contact between the READY terminals is open.

If an external relay is connected to the terminals, a surge absorber must be connected for noise prevention.

B4.8 External interface unit

The external interface unit is one of the units that constitute the SCU and transmits temperature signals and fan control signals to the processor module.

The external interface units are available in two types: one for standard type SCU and the other for wide range temperature type SCU.

Elements on the external interface unit

The following figure shows the elements on the external interface units for standard type SCU and wide range temperature type SCU.

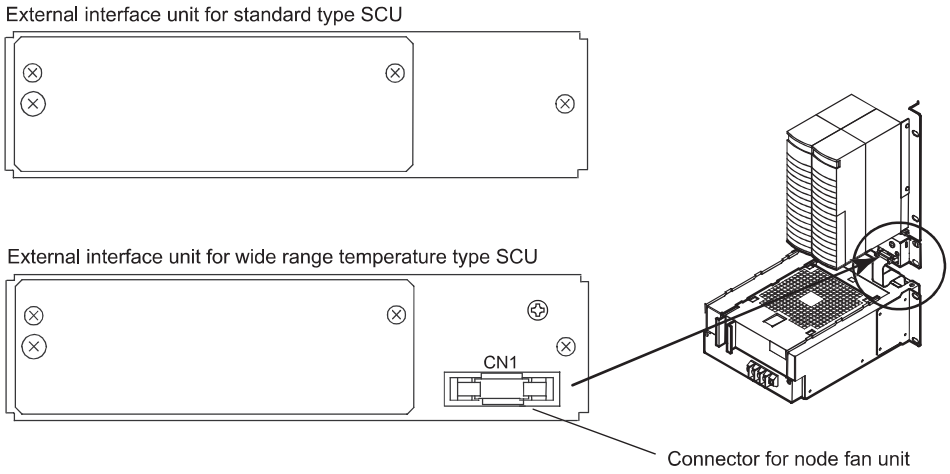


Figure B4.8-1 External interface unit

External interface unit for standard type safety control unit

The external interface unit for standard type SCU has a built-in temperature sensor (thermometer) for monitoring the ambient temperature of the SCU. The sensor signals are converted into the temperature information by the HKU (House Keeping Unit) function in the processor module. When the ambient temperature abnormality occurs it can be monitored through the SCS status management window on SENG, using the SCS maintenance Support Tools.

SEE ALSO For more information about the SCS State Management window, refer to:

H1.2, “SCS State Management window” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

External interface unit for wide range temperature type safety control unit

The external interface unit for wide range temperature type SCU is used when connecting node fan units to the SCU. Same as the external interface unit for standard type SCU, a temperature sensor is built-in.

The following signals that indicate the status of fans are passed to the HKU function in the processor module:

- Fan speed signal
- Fan speed control signal

B4.9 Node fan unit

The wide range temperature type SCU has a node fan unit. These fan units reduce the temperature increase to prevent malfunctions and the component fatigues that may be caused by the high temperature.

■ Configuration of the node fan unit

The following figure shows the configuration of the node fan unit.

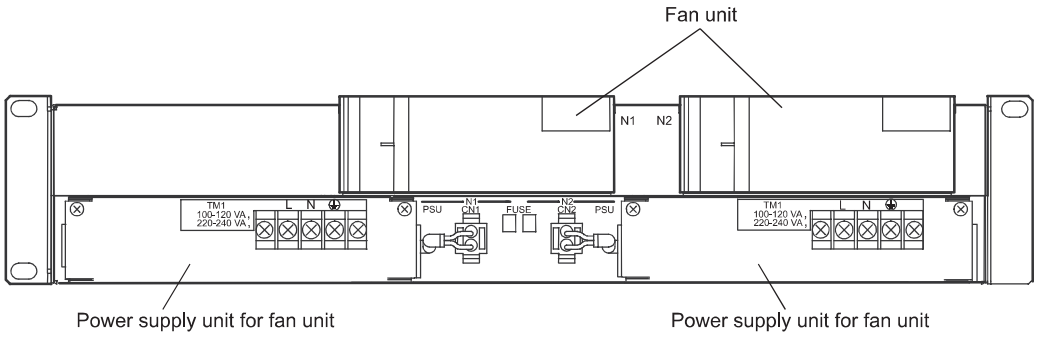


Figure B4.9-1 Node fan unit

● Fan unit

The fan revolution varies with the ambient temperature for two levels. When the ambient temperature is higher than 35 degree C, or when the other fan is abnormal, the fan revolves at high speed. When a fan revolves at an abnormally very low speed, the abnormality can be monitored through the SCS status management window on SENG.

The following figure shows the appearance of the fan unit.

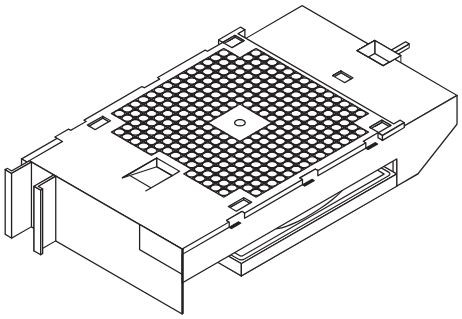


Figure B4.9-2 Fan unit

SEE ALSO For more information about replacing the fan unit, refer to:

"■ Replacing fan unit" on page E3-9

● Power supply unit for fan unit

The power supply unit for fan unit receives the designated power supply through the power input terminals and produces 12 V DC for running the fan. The left and right power supply units for fan unit supply power to the left and right fan units, respectively.

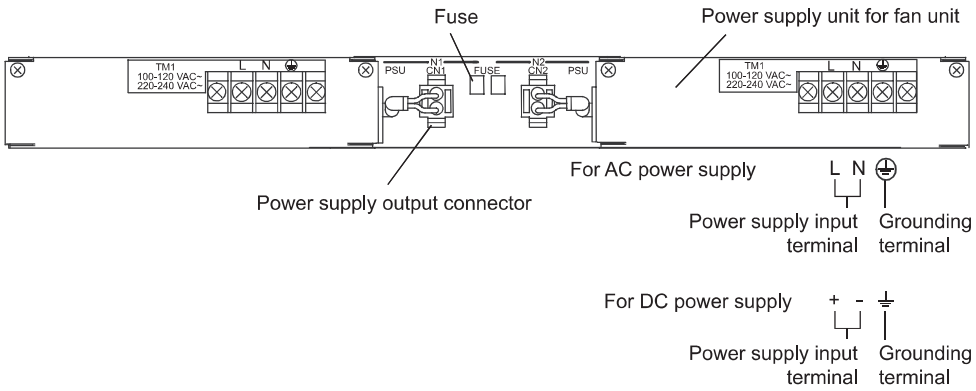


Figure B4.9-3 Power supply unit for fan unit

SEE ALSO For more information about replacing the power supply unit for fans, refer to:

"■ Replacing power supply unit for fan unit" on page E3-11

● Fuse for fan power supply unit

A fuse is used for protecting the power supply unit for fan unit.

SEE ALSO For more information about replacing the fuse for fan power supply unit, refer to:

"■ Replacing fuse for fan power supply unit" on page E3-10

B5. N-IO node devices

This section describes the devices that constitute an N-IO node. The node interface unit and the N-IO I/O unit, which are components of an N-IO node, consist of a base plate and devices that are mounted on the base plate. N-IO nodes can be used in SCSP3.

- Node interface unit
  - Base plate for node interface unit
  - Power supply unit
  - N-ESB bus module
- N-IO I/O unit
  - Base plate
  - N-IO I/O module
  - Intrinsic safety barrier
- Terminal board
- Cables
  - F-SB bus cable
  - Power supply cable for base plates

TIP

For legal conformity in some regions, a generic name called “system model name” is given to a specific set of products that make up an N-IO I/O unit. There are following system model names:

- S2ZN1D
- S2ZN4D
- S2ZN5D

SEE ALSO

For more information about Products that constitute an S2ZN1D, S2ZN4D, or S2ZN5D, refer to:

- ProSafe-RS Base Plate (for N-IO) (GS 32P06K20-01EN)
- ProSafe-RS Base Plates for Barrier (for N-IO) (GS 32P06P10-01EN)

B5.1 Node interface unit

The node interface unit (Model: S2NN30D) passes the field device signals that the N-IO I/O units received to the SCU and passes the signals from the SCU to the N-IO I/O unit. The node interface unit also distributes the power that is supplied by the power supply unit to the N-IO I/O units.

Configuration of the node interface unit

The node interface unit consists of the following components:

- Base plate for node interface unit
- Power supply unit
- N-ESB bus module

The following figure shows the configuration of the node interface unit.

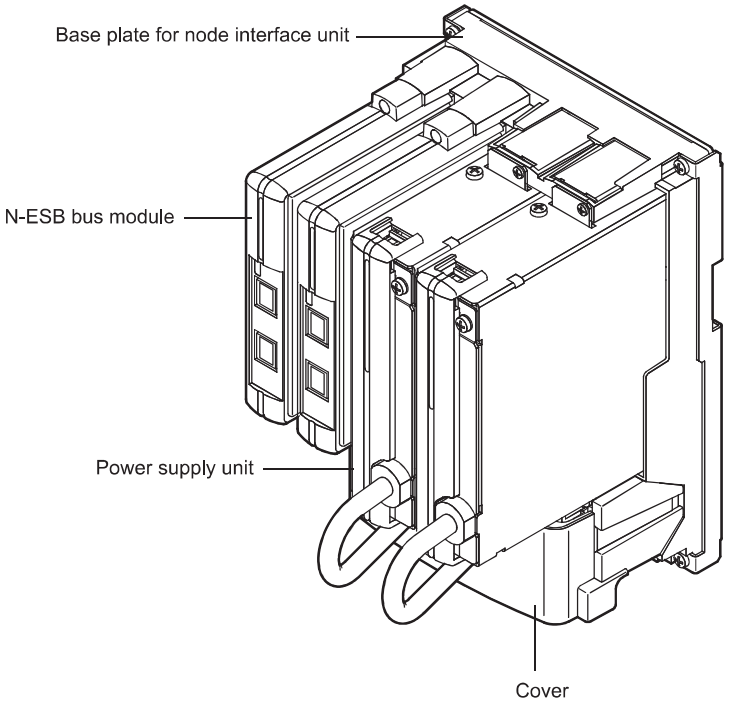


Figure B5.1-1 Node interface unit

Cover

A cover for protecting wiring connectors and terminals is provided.

Follow these steps to remove and attach the cover:

- Removing the cover
  1. Pinch the bottom-right part of the cover as shown in the figure, move it outward so that the cover expands. The hook on the cover leaves the groove of the base plate for node interface unit.
  2. Remove the cover toward you.
- Attaching the cover
  Put back the cover along the guide. Ensure that the wiring does not touch the cover.

The following figure shows how to remove and attach the cover.

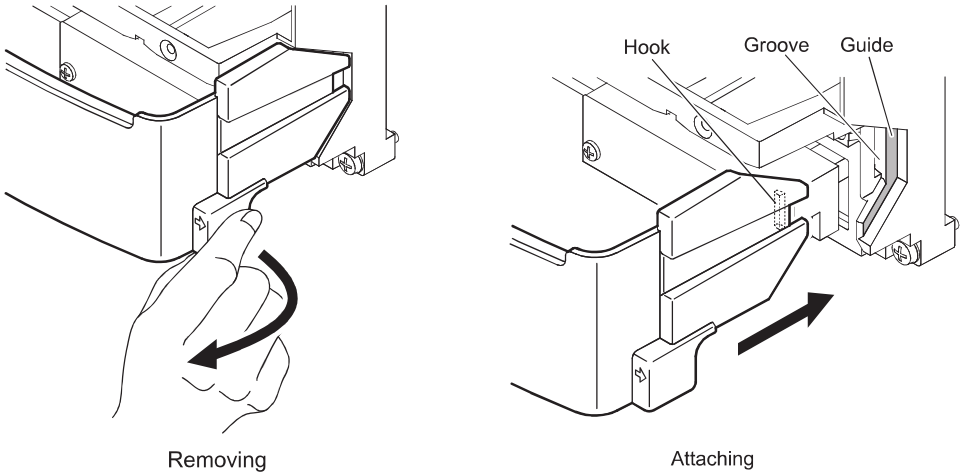


Figure B5.1-2 Removing and attaching the cover

B5.2 Base plate for node interface unit

The base plate for node interface unit is the base plate where you mount power supply units and N-ESB bus modules.

Elements on the base plate for node interface unit

The following figure shows the elements on the base plate for node interface unit.

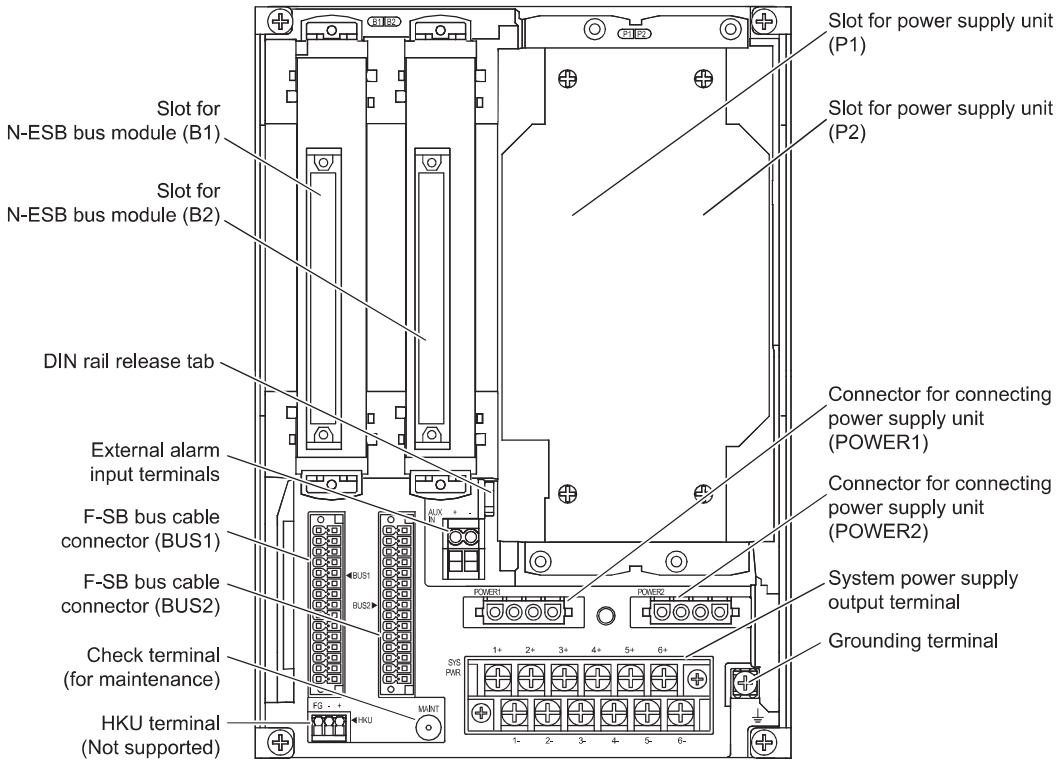


Figure B5.2-1 Base plate for node interface unit (DIN rail mountable type)

External alarm input terminals

These terminals are provided for connecting a voltage input signal from an external device. The terminals are pressure clamp terminals.

SEE ALSO For more information about signal wiring of the external alarm input terminals, refer to:

D3., “Signal connection of the external alarm input terminals of the node interface unit” on page D3-1

For more information about the software setting for the external alarm input terminals, refer to:

Appendix 1.1, “Setting items for nodes” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Connectors for connecting power supply unit

To the connectors for connecting power supply unit, connect only the device specified by YOKOGAWA.

B5.3 Power supply unit

The power supply unit supplies power to the node interface unit and N-IO I/O units. The power supply units are mounted in pair on a base plate for node interface unit.

The following power supply units are available:

- S2PW503: 24 V DC output power supply unit (120 W output, 100-240 V AC input)
- S2PW504: 24 V DC output power supply unit (120 W output, 24 V DC input)

Elements on the power supply unit

The following figure shows the elements on the power supply unit.

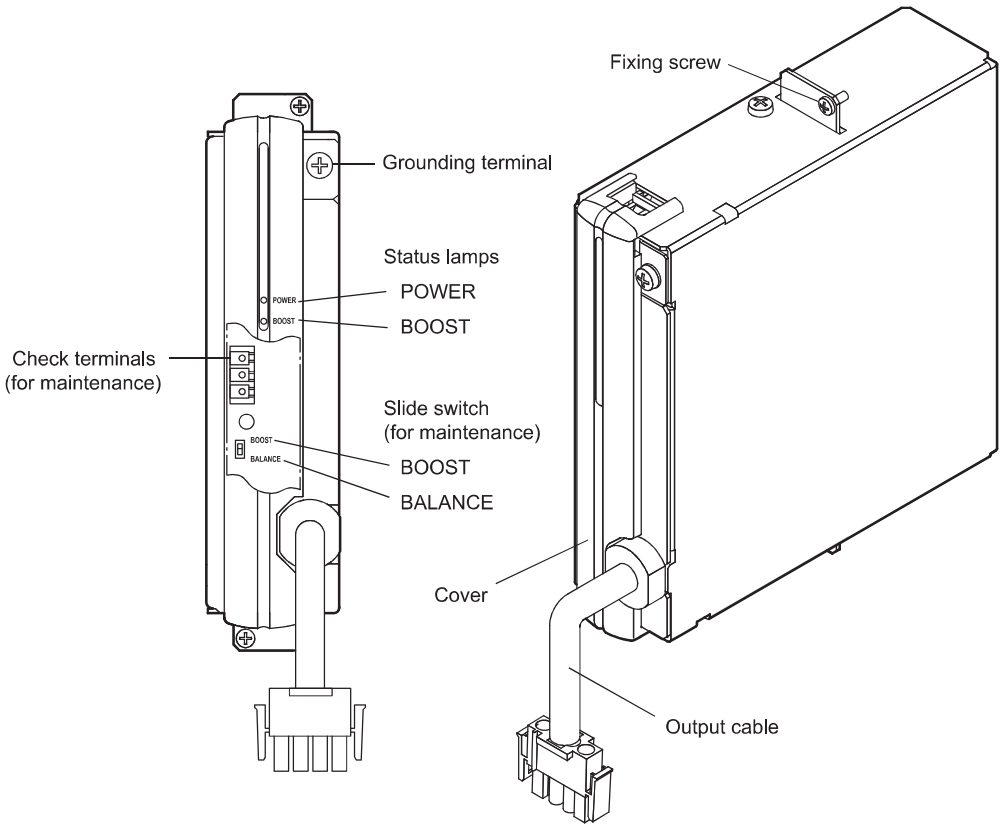


Figure B5.3-1 Power supply unit

Status lamps

Each lamp indicates the device status as follows:

- POWER
  This lamp is on while the power is applied.
- BOOST
  This lamp is for maintenance. The lamp is off during normal operation.

Slide switch

Set this switch to the BALANCE position during normal operation. This switch is for maintenance.

B5.4 N-ESB bus module

The N-ESB bus module (Model: S2EN501) communicates with the SCU through N-ESB bus or optical ESB bus. The N-ESB bus modules are mounted in pair on a base plate for node interface unit.

Elements on the N-ESB bus module

The N-ESB/optical ESB ports have different shapes, depending on the type of the bus to be connected. The following figure shows the elements on the N-ESB bus modules.

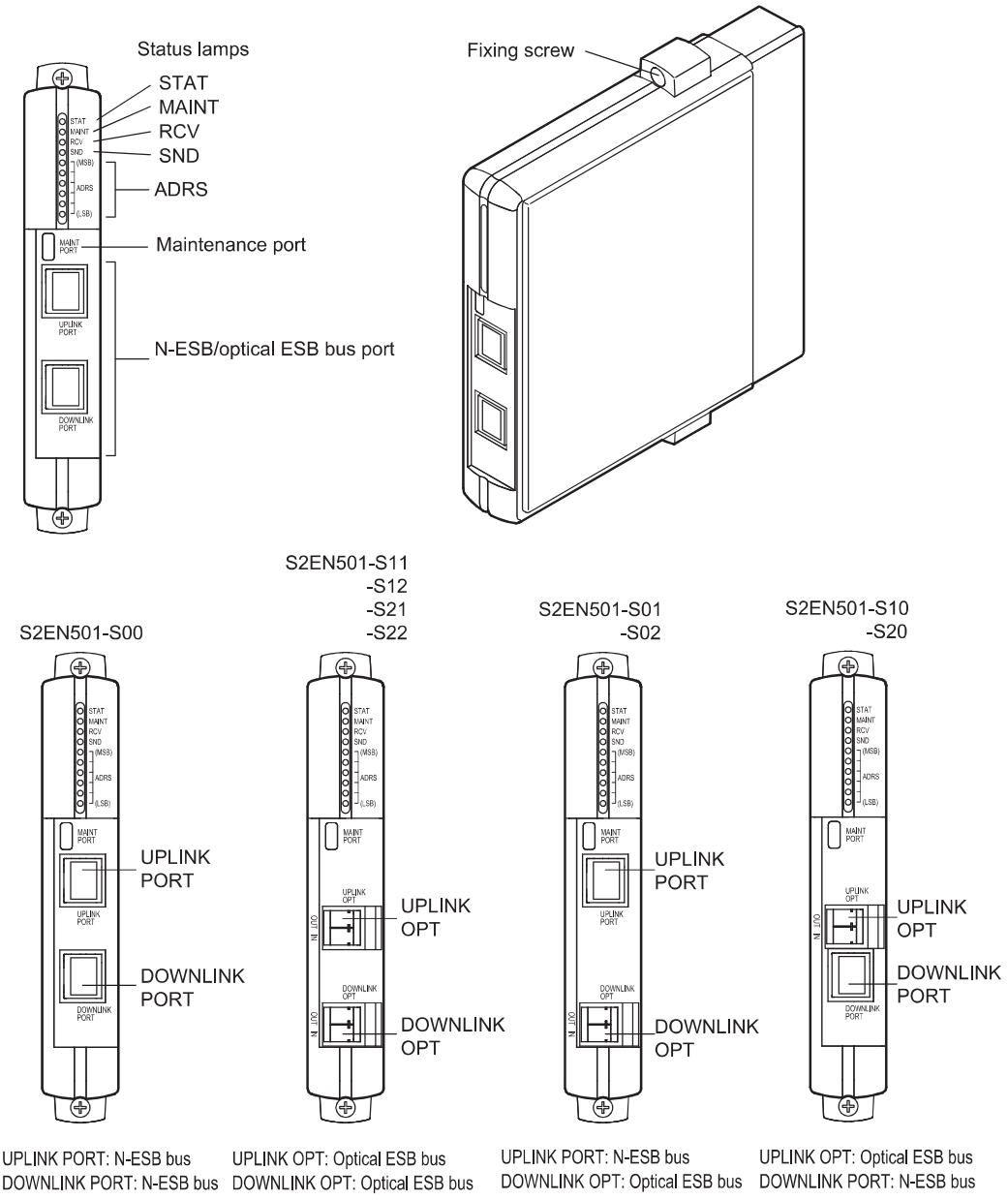


Figure B5.4-1 N-ESB bus module

Status lamps

Each lamp indicates the device status as follows:

- STAT
  The lamp turns on when the hardware is functioning normally; otherwise, the lamp turns off.
- MAINT
  The lamp turns on in maintenance mode; otherwise, the lamp turns off.
- RCV
  The lamp turns on when the module is receiving; otherwise, the lamp turns off.
- SND
  The lamp turns on when the module is sending response frames for a signal addressed to the module; otherwise, the lamp turns off.
- ADRS
  These lamps indicate the node number in 6-bit binary code.

  The following table shows the correspondence between the node number and the lamp status.

Table B5.4-1 Node number and lamp status

ADRS	Node number(*1)							
	1	2	3	...	16	...	31	32
MSB(*2)	○	○	○		○		○	●
|	○	○	○		●		●	○
|	○	○	○	...	○	...	●	○
|	○	○	○		○		●	○
|	○	●	●		○		●	○
LSB(*3)	●	○	●		○		●	○

*1: The symbols denote the lamp status as follows:
●: On
○: Off
*2: Most significant bit
*3: Least significant bit

TIP

The ADRS lamps are all off when the node number is not set.

Maintenance port

The maintenance port is used to set the node number of the N-IO node. This is a micro USB port. When the port is not used, put the cover that came with the module.

IMPORTANT

You must set the node number of the N-IO node before you connect the bus cables.

SEE ALSO

For more information about the node number setting of N-IO nodes, refer to:

F2.1.1, “Using the Node Number Setting Tool” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

N-ESB bus/optical ESB bus ports

To these ports, you connect N-ESB or optical ESB bus cables in a daisy chain.

- UP LINK PORT/OPT
  Connect the cable to the SCU or to the N-IO node or SNU that is closer to the SCU in the daisy chain.

- DOWN LINK PORT/OPT
  Connect the cable to the N-IO node or SNU that is farther from the SCU in the daisy chain.

For unused ports, put the cover that came with the module.

B5.5 Base plates

The base plate for N-IO I/O unit is where you can mount N-IO I/O modules to connect up to 16 I/O signals.

The following types of base plates are available:

- Base plate with disconnecting terminals
- Base plate for barrier

B5.5.1 Base plate with disconnecting terminals

The base plate with disconnecting terminals (Model: S2BN1D) is where you can mount N-IO I/O modules to connect up to 16 I/O signals. To the base plate with disconnecting terminals, you can connect a field power supply that supplies power to the field devices.

The base plate with disconnecting terminals comes in the terminal type (S2BN1D-□1□□□ or S2BN1D-□2□□□) and the connector type (S2BN1D-□9□□□). You can use the terminal type when you connect I/O signals directly and you can use the connector type when you connect I/O signals through a terminal board.

Elements on the base plate with disconnecting terminals: Terminal type

The following figure shows the elements on the terminal type of base plate with disconnecting terminals.

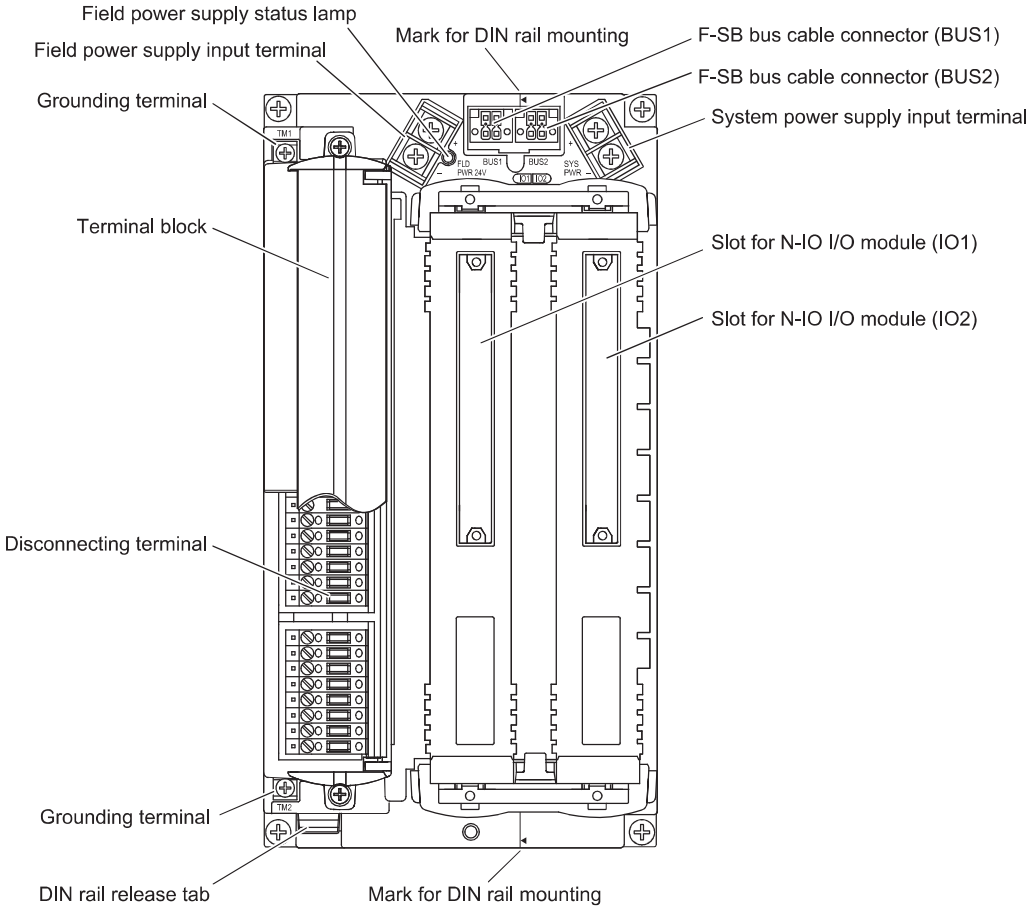


Figure B5.5.1-1 Base plate with disconnecting terminals (DIN rail mountable and terminal type)

The terminal block may be either pressure clamp terminal type or spring clamp terminal type. The terminal block has a cover. Because the terminal block is detachable from the base plate, you can detach it when you perform wiring works.

You must mount a dummy cover for I/O module (Model: S2DCV02) to unused N-IO I/O module slots.

SEE ALSO For more information about Signal connection to the base plate with disconnecting terminal, refer to:

D2.1, “Signal connection to the base plate with disconnecting terminals” on page D2-5

Disconnecting terminals

Disconnecting terminals are used to facilitate disconnecting and connecting of the signal cables between field devices and the N-IO I/O module. By disconnecting terminals, the N-IO I/O module can be protected from any overvoltage that may occur when maintaining field devices or performing wiring work.

- Tab is pulled out: The signal wire is disconnected.
- Tab is pressed in: The signal wire is connected.

During normal operation, all tabs should be pressed in. Pull out the tab when disconnection is required. Tabs of unused channels should be pressed in.

IMPORTANT

Do not disconnect the signal cables by using disconnecting terminals while the status of the digital output signal (DO) is ON.

When you pull out the tabs, use the dedicated tool (TZ 0306704 from Phoenix Contact Corporation).

The following figure shows the pulled out or pressed in disconnecting terminals.

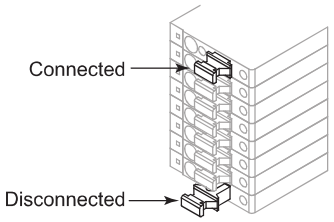


Figure B5.5.1-2 Disconnecting terminals

System power supply input terminals

To the system power supply input terminals, connect only the device specified by YOKOGAWA.

Field power supply status lamp

The lamp turns on when the field power is supplied; otherwise, the lamp turns off.

Elements on the base plate with disconnecting terminals: Connector type

The following figure shows the elements on the connector type of base plate with disconnecting terminals.

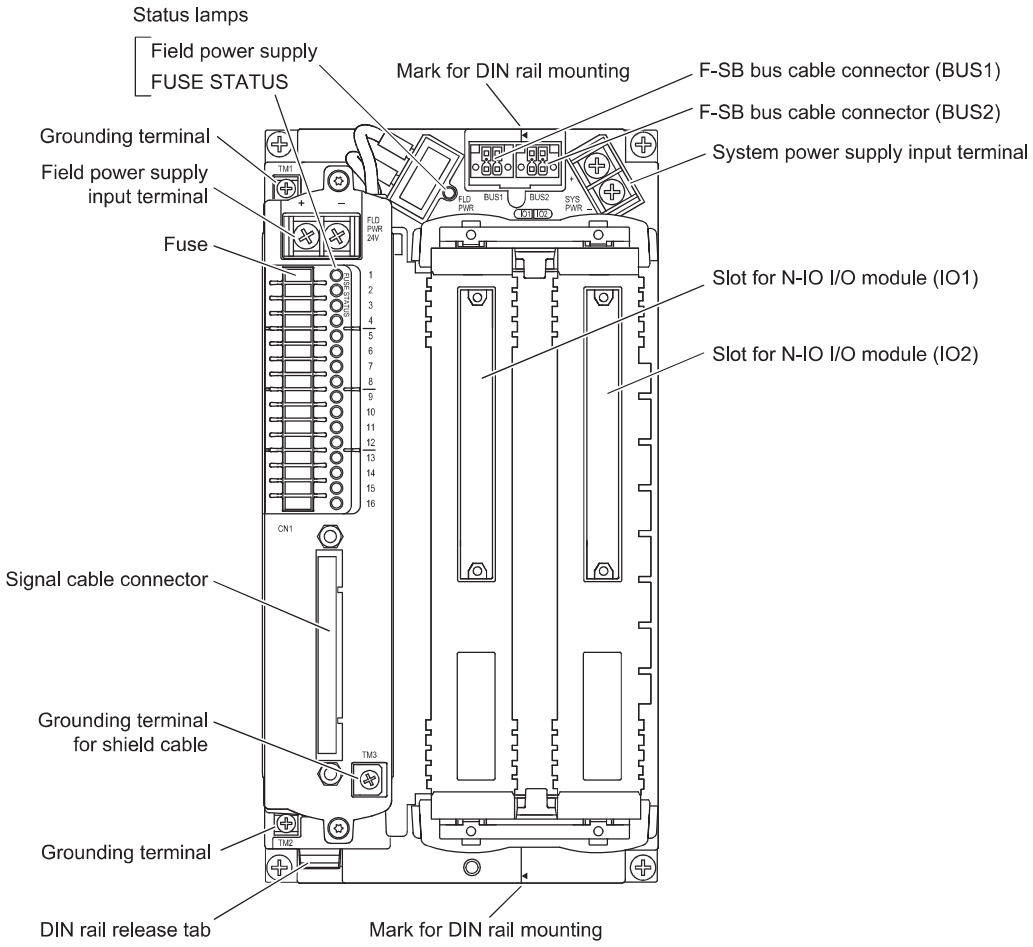


Figure B5.5.1-3 Base plate with disconnecting terminals (DIN rail mountable and connector type)

You must mount a dummy cover for I/O module (Model: S2DCV02) to unused N-IO I/O module slots.

Do not remove the cover next to the field power supply status lamp.

SEE ALSO For more information about Signal connection to the base plate with disconnecting terminal, refer to:

D2.1, “Signal connection to the base plate with disconnecting terminals” on page D2-5

System power supply input terminals

To the system power supply input terminals, connect only the device specified by YOKOGAWA.

Status lamps

Each lamp indicates the device status as follows:

- Field power supply
  The lamp turns on when the field power is supplied; otherwise, the lamp turns off.
- FUSE STATUS
  This lamp is checked when a 3-wire current input device is used.

  The lamp turns on if the fuse blows while the field power is supplied; otherwise, the lamp turns off.

TIP If a device except for 3-wire current input is used, FUSE STATUS lamp is always off.

Signal cable connector

You must connect dedicated signal cables (Model: AKB331, AKB651) to the signal cable connector.

SEE ALSO For more information about the signal cable specifications, refer to:

- ProSafe-RS/ProSafe-RS Lite Cables (GS 32Q06M10-31E)
- ProSafe-RS Base Plate (for N-IO) (GS 32P06K20-01EN)

B5.5.2 Base plate for barrier

The base plate for barrier (Model: S2BN4D, S2BN5D) is where you can mount N-IO I/O modules and intrinsic safety barriers to connect up to 16 I/O signals.

For each I/O signal channel, mount an intrinsic safety barrier that you selected according to the type of the signal.

You need to connect a power supply to the base plate for barrier to supply power to the intrinsic safety barriers.

The following table lists the different types of base plates for barrier.

Table B5.5.2-1 Different types of base plates for barrier

Model	Position of intrinsic safety wiring terminals	Position of intrinsic safety wiring
S2BN4D-10□C0	Intrinsic safety barrier	Left on the base plate
S2BN4D-10□D0	Intrinsic safety barrier	Right on the base plate
S2BN5D-121C0	Base plates	Left on the base plate
S2BN5D-121D0	Base plates	Right on the base plate

Elements on the base plate for barrier: S2BN4D

The following figure shows the elements on the base plate for barrier S2BN4D.

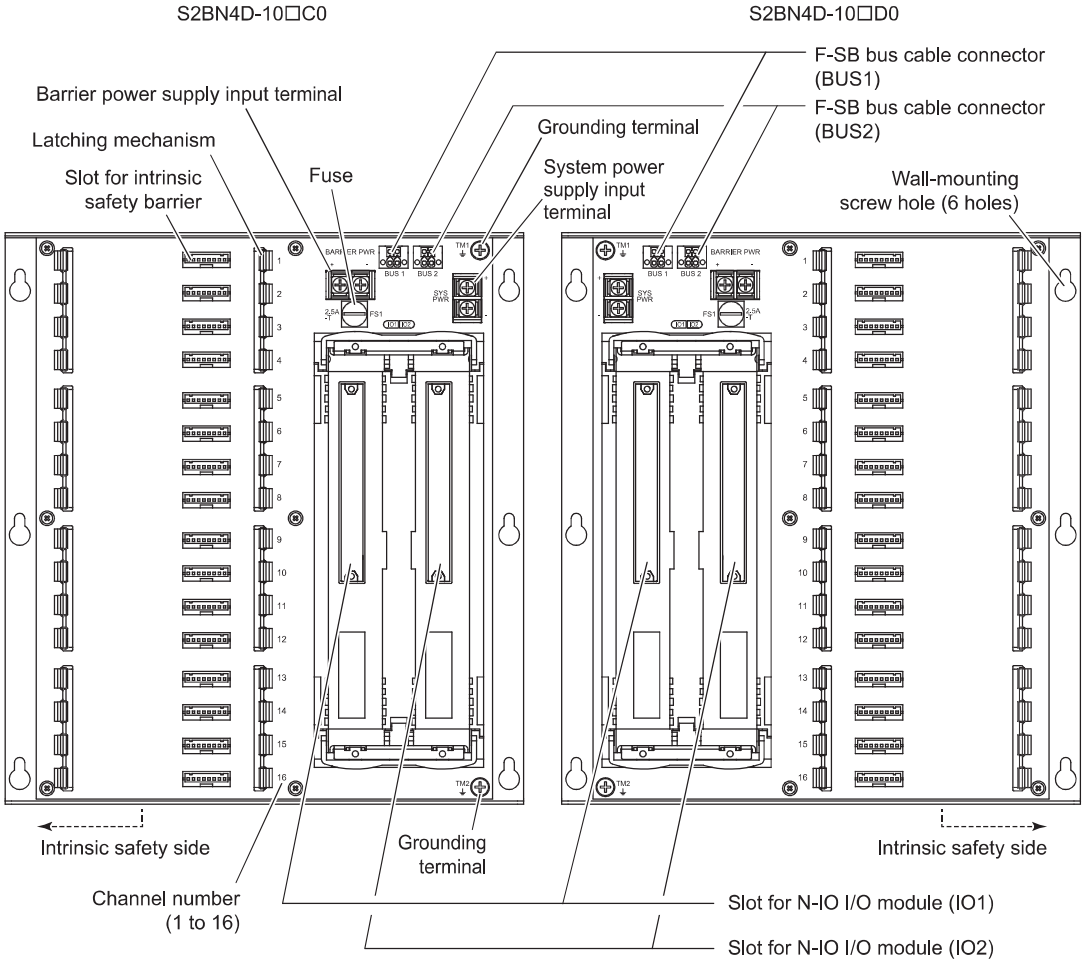


Figure B5.5.2-1 Base plate for barrier S2BN4D

The wiring from the intrinsic safety barriers to the field devices becomes intrinsic safety wiring. S2BN4D-10□C0 has intrinsic safety wiring on the left side of the mounted barriers, while S2BN4D-10□D0 has intrinsic safety wiring on the right side. These base plates do not have signal terminals because signal terminals are provided on intrinsic safety barriers.

You must mount a dummy cover for I/O module (Model: S2DCV02) to unused N-IO I/O module slots.

SEE ALSO For more information about signal connection to S2BN4D, refer to:

D2.2, “Signal connections of the base plate for barrier: S2BN4D” on page D2-9

System power supply input terminals

To the system power supply input terminals, connect only the device specified by YOKOGAWA.

Elements on the base plate for barrier: S2BN5D

The following figure shows the elements on the base plate for barrier S2BN5D.

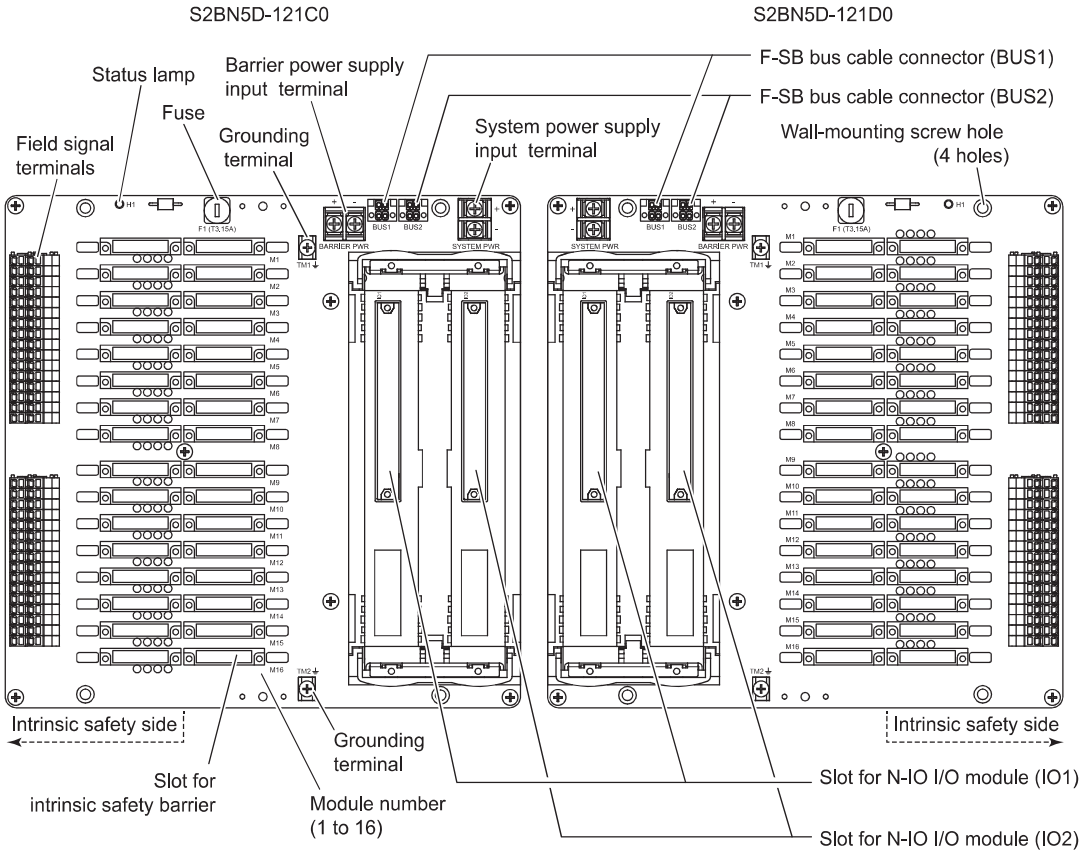


Figure B5.5.2-2 Base plate for barrier S2BN5D

The wiring from the intrinsic safety barriers to the field devices becomes intrinsic safety wiring. S2BN5D-121C0 has signal terminals for connection to the field devices in the left of the base plate, while S2BN5D-121D0 has the signal terminals in the right. The signal terminals for connection to the field devices are spring clamp terminals.

You must mount a dummy cover for I/O module (Model: S2DCV02) to unused N-IO I/O module slots.

SEE ALSO For more information about signal connection to S2BN5D, refer to:

D2.3, “Signal connections to the base plate for barriers: S2BN5D” on page D2-10

System power supply input terminals

To the system power supply input terminals, connect only the device specified by YOKOGAWA.

Status lamp

The lamp turns on when the barrier power is supplied and also the fuse is not blown; otherwise, the lamp turns off.

B5.6 N-IO I/O module

The N-IO I/O module converts process input signals from field devices into internal data of the SCU and also converts the internal data of the SCU into process output signals and sends them to the field devices. The signal category is defined for each channel.

The N-IO I/O module is mounted on a base plate with disconnecting terminals or a base plate for barrier.

The following types of N-IO I/O modules are available:

Table B5.6-1 Types of N-IO I/O modules

Model	Name	Settable signal category
S2MMM843	Analog digital I/O module	Analog input, analog output, digital input, digital output
S2MDV843	Digital I/O module	Digital input, digital output

Elements on the N-IO I/O module

The following figure shows the elements on the N-IO I/O module.

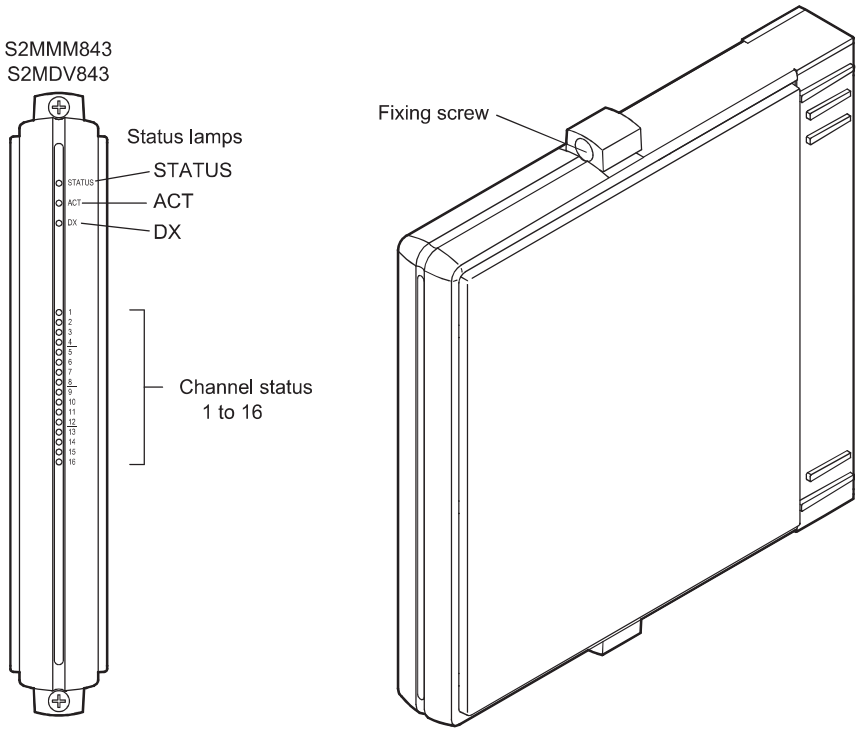


Figure B5.6-1 N-IO I/O module

Status lamps

Each lamp indicates the device status as follows:

- STATUS
  On: Hardware normal

  Flashing: In non-redundant configuration, a channel failure occurred. In dual-redundant configuration, a channel failure occurred while the standby module has a hardware error.

  Off: Hardware error
- ACT
  On: In dual-redundant or non-redundant configuration, the module is operating.

Off: In non-redundant configuration, the module stopped operation. In dual-redundant configuration, the module is standby or stopped operation.

- DX
  On: The module is in dual-redundant configuration.

  Off: The module is in non-redundant configuration.

- Channel status
  Error in the wiring to the field device or the on/off status of digital input (DI) or digital output (DO) is indicated for each channel.

  On: DI or DO signal is ON in non-redundant module or active module in dual-redundant configuration, without wiring error.

  Flashing: Wiring error in non-redundant module or active module in dual-redundant configuration

  Off: Other than above

TIP

The channel status lamps flash at a frequency of 2 Hz. If the DI or DO signal turns on and off at a cycle near this frequency, you cannot discriminate it from the flashing that indicates a wiring error. For this reason, you must check the I/O module report from the status display view on SENG.

B5.7 Intrinsic safety barriers

Intrinsic safety barriers are mounted on a base plate for barrier and electrically isolate intrinsic safety circuits from non-intrinsic safety circuits.

For each channel of the N-IO I/O module, use an appropriate intrinsic safety barrier based on the type of the I/O signal.

SEE ALSO For more information about the signal types and specifications of intrinsic safety barriers, refer to:

ProSafe-RS Baseplates for Barrier (for N-IO) (GS 32P06P10-01EN)

B5.8 Terminal board (for N-IO node)

The terminal board for analog digital I/O (Model: A2BM4) relays signals of field devices to N-IO I/O unit.

The following figure shows the appearance of the terminal board for analog digital I/O.

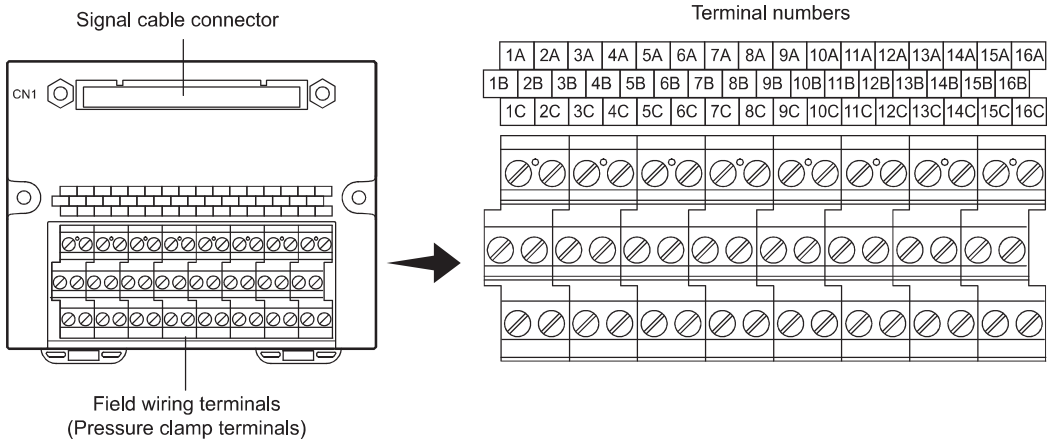


Figure B5.8-1 Terminal board for analog digital I/O

B5.9 N-IO node cables

This section describes the cables that are used in an N-IO node.

- F-SB bus cable
- Power supply cable for base plates

F-SB bus cable

The F-SB bus cable (Model: S2KLF10) is a dedicated cable assembly that is used to connect multiple N-IO I/O units to a node interface unit. At each cable end on the N-IO I/O unit side, a unit number is indicated on a tag, showing to which unit it should be connected. The following figure shows the appearance of the F-SB bus cable.

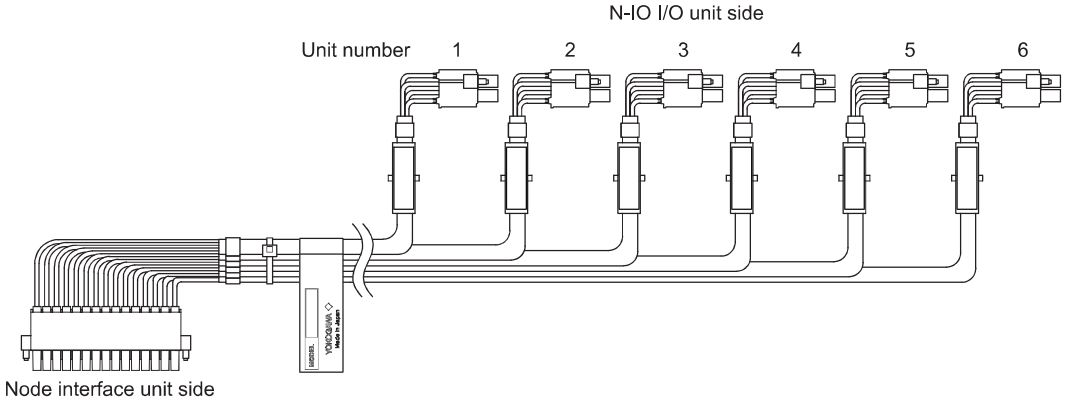


Figure B5.9-1 Appearance of F-SB bus cable

Power supply cable for base plates

The power supply cable for base plates (Model: S2KPB10) is a dedicated cable that is connected between a node interface unit and an N-IO I/O unit. Connect the red cable to the plus terminal and the blue cable to the minus terminal.

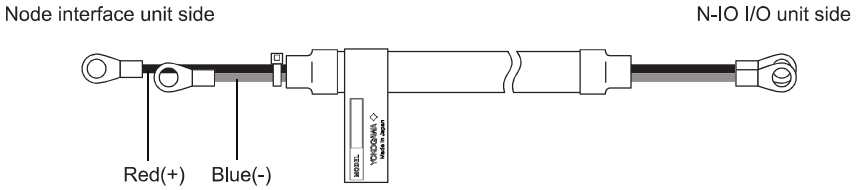


Figure B5.9-2 Appearance of the power supply cable for base plates

B6. Other devices

This section describes the following SCS device:

- Wiring check adapter

B6.1 Wiring check adapter for digital input

The wiring check adapter to detect open circuits or short circuits in the field wiring is used for the digital input (DI) channels of the FIO digital input module and the N-IO I/O module.

The following models of wiring check adapters are available:

- SCB100: For open circuit detection
  By connecting this adapter in parallel with the field device switch, an open circuit can be detected while the DI channel is receiving an OFF signal.
- SCB110: For short circuit detection
  By connecting this adapter in series with the field device switch, short circuits with the power line or other channels can be detected while the DI channel is receiving an ON signal.

In order to detect open circuits or short circuits, you must also enable the diagnostic feature of the DI channel in addition to installing the wiring check adapters.

SEE ALSO For more information about Diagnostic function of DI channel, refer to:

Appendix 1.3.4, “Settings for the DI channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Appearance of the wiring check adapter

The following figure shows the appearance of SCB100 and SCB110.



Figure B6.1-1 External view of SCB100/SCB110 wiring check adapter

Usage of wiring check adapter

The following figure shows how the wiring check adapter is connected. DCn and INn of the digital input module (SDV144/L1DV144), and nA and nB of N-IO I/O modules (S2MMM843 and S2MDV843) are signal names of the n-th channel.

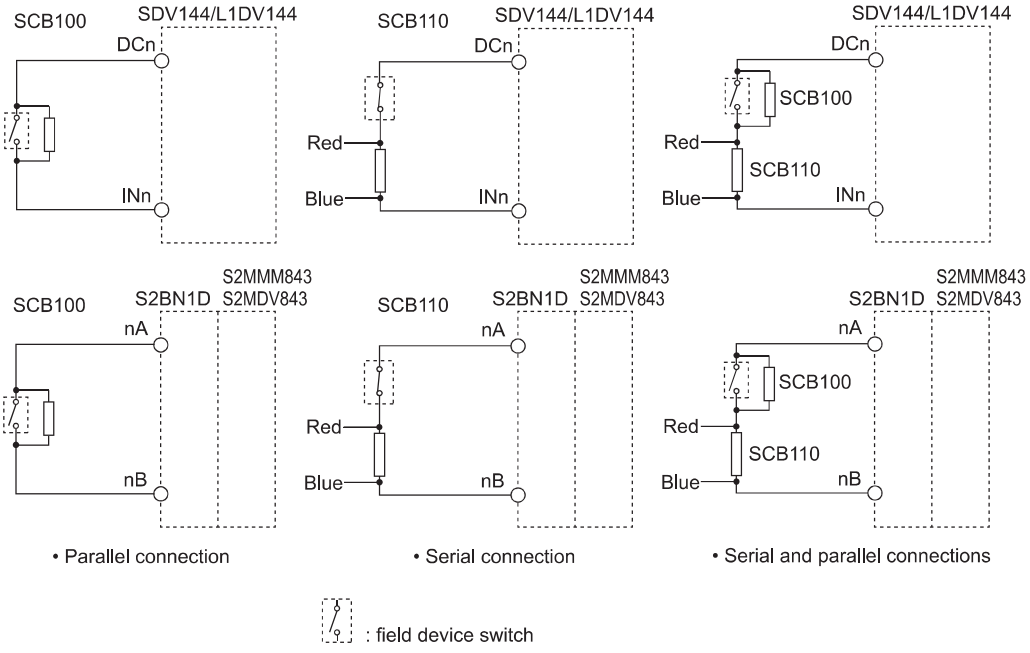


Figure B6.1-2 Usage of wiring check adapter

IMPORTANT

Do not stress the wiring check adapter.

SCB110 has a polarity. It does not work properly if you install it wrongly.

SEE ALSO For more information about I/O channel number of SDV144/L1DV144, refer to:

- "■ SED4D signal cable connection" on page D1-28
- "■ SBD4D signal cable connection" on page D1-32
- "■ Input terminal numbers and signal names of SDV144/L1DV144" on page D1-23

C. Installing and wiring the SCS

This section describes how to install and wire SCS components.

- Installing the SCS
- Grounding and power supply wiring of SCS
- Bus cable wiring of SCS

C1. Installing the SCS

This section describes how to install the following SCS devices:

- FIO nodes (SCU, SNU, and unit for optical ESB bus repeater module)
- Terminal boards and relay boards (for FIO node)
- Node interface unit (for N-IO node)
- N-IO I/O unit (for N-IO node)
- Terminal board (for N-IO node)
- Field power supply unit

SEE ALSO

For more information about the heat-radiating space, the space for maintenance work, and the device installation environment for SCSs that support SIL 3, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

For more information about the heat-radiating space, the space for maintenance work, and the device installation environment for SCSs that support SIL 2, refer to:

ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

C1.1 Installing an FIO node

This section describes how to mount SCU, SNU, and unit for optical bus repeater module onto a rack.

Mounting/removing an FIO node on/from a rack

CAUTION

You must attach insulating bushings to isolate SCU, SNU, and unit for optical bus repeater module from the rack. When you install the devices with insulating bushings attached on a rack or instrument panel, do not keep the devices hung on loose screws in an unstable state. Too much force may apply to the insulating bushings and cause damaged or broken insulating bushings.

The following figure shows an example of installing a rack mountable device. Insulating bushings are supplied with the device.

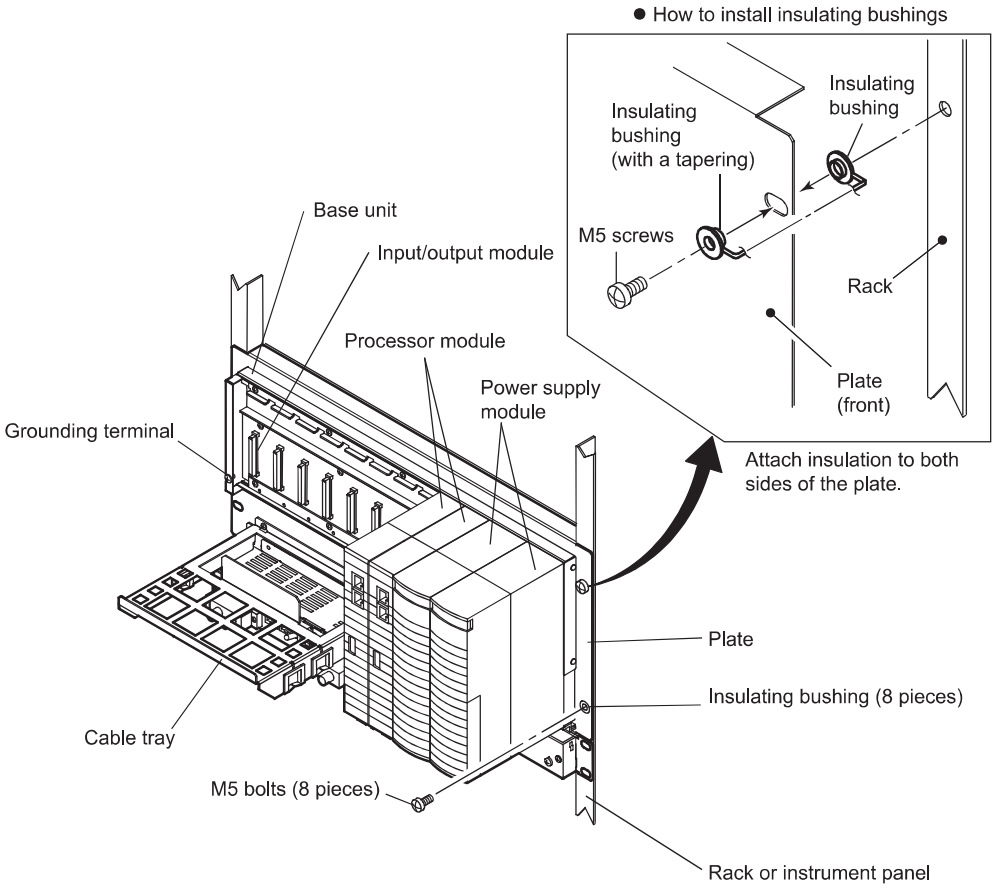


Figure C1.1-1 Example of mounting on a rack (example of standard type SCU)

Follow these steps to mount a rack mountable device on a rack:

1. Fasten a pair of insulating bushings together to each of the screw holes on the plate of the rack mountable device. Ensure that the insulating bushing that has a tapering comes on the front side of the plate.

2. Mount the device by tightening the M5 screws. The number of screws varies depending on the device you are mounting.
3. Check that the device is electrically insulated from the rack.

Follow this step when you remove a rack mountable device from a rack:

- Hold the device by hand and unscrew the M5 screws to remove the device.

Attaching the air deflector

S2SC70□-FA/L1SC70□-FA come with an air deflector. Follow these steps to attach the air deflector to the fan unit:

1. Remove the fan unit on the left side of the node fan unit.
2. On the removed fan unit, place the air deflector and insert its locking claws into the left and right mounting holes on the fan unit.

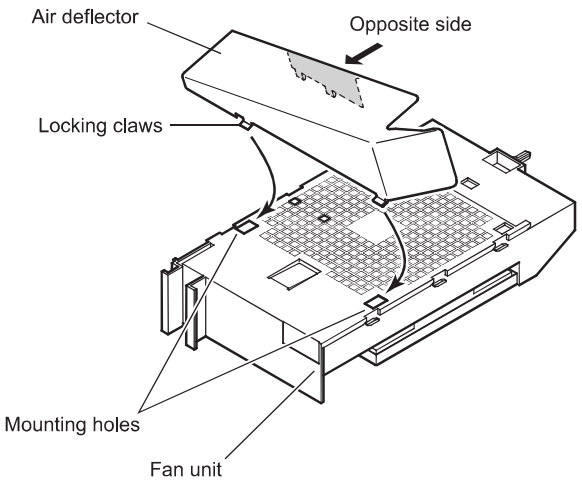


Figure C1.1-2 Attaching the air deflector

3. Insert the locking claws into the fan unit, pressing the opposite side of the air deflector with your fingers.
4. Mount the fan unit into the node fan unit.

TIP

If you can visually confirm that the locking claws of the air deflector are properly inserted into the left fan unit, you do not have to remove the fan unit from the node fan unit.

SEE ALSO

For more information about mounting or removing the fan unit, refer to:

"■ Replacing fan unit" on page E3-9

C1.2 Installing terminal boards and relay boards (for FIO node)

Rack mountable type and DIN rail mountable type terminal boards and relay boards are available.

The installation method depends on the mounting type and whether it is a terminal board or relay board:

- Rack mountable terminal board: Mounting on a rack
- Rack mountable relay board: Mounting on a rack or wall
- DIN rail mountable terminal board: Mounting on a DIN rail or wall
- DIN rail mountable relay board: Mounting on a DIN rail

SEE ALSO

For more information about types of terminal boards, refer to:

B4.7.6, “Terminal boards (for FIO node)” on page B4-33

For more information about types of relay boards, refer to:

B4.7.7, “Relay boards” on page B4-38

For more information about securing the cable area for terminal boards/relay boards, refer to:

ProSafe-RS/ProSafe-RS Lite Terminal Board/Relay Board (GS 32Q06L20-31E)

C1.2.1 Installing a rack mountable terminal/relay board

This section describes how to mount a terminal board or relay board on a rack and how to mount a relay board on a wall.

Mounting and removing a rack mountable terminal board/relay board

The following figure shows an example of how to mount a terminal/relay board on a rack.

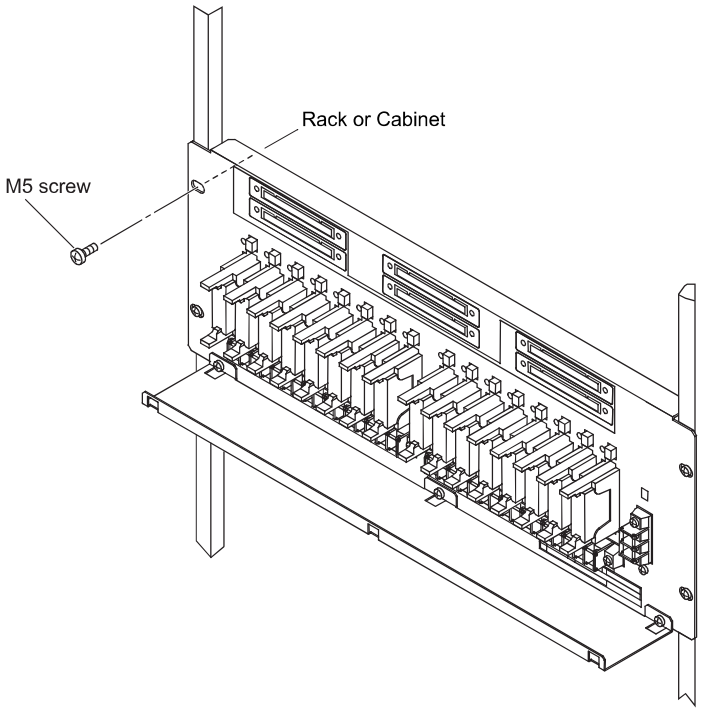


Figure C1.2.1-1 Mounting on a rack (SRM53D)

Follow this step to mount a terminal/relay board on a rack:

- Mount the device by tightening the M5 screws. The number of screws varies from device to device.

Follow this step to remove a terminal/relay board from a rack:

- Hold the device by hand and unscrew the M5 screws to remove the device.

SEE ALSO For more information about appearance of terminal boards and relay boards, refer to:

ProSafe-RS/ProSafe-RS Lite Terminal Board/Relay Board (GS 32Q06L20-31E)

Mounting/removing a rack mountable relay board on/from a wall

If the wall-mounting option is specified when a rack mountable relay board is ordered, wall-mounting fittings are supplied with the relay board.

The following figure shows how to mount a relay board on a wall.

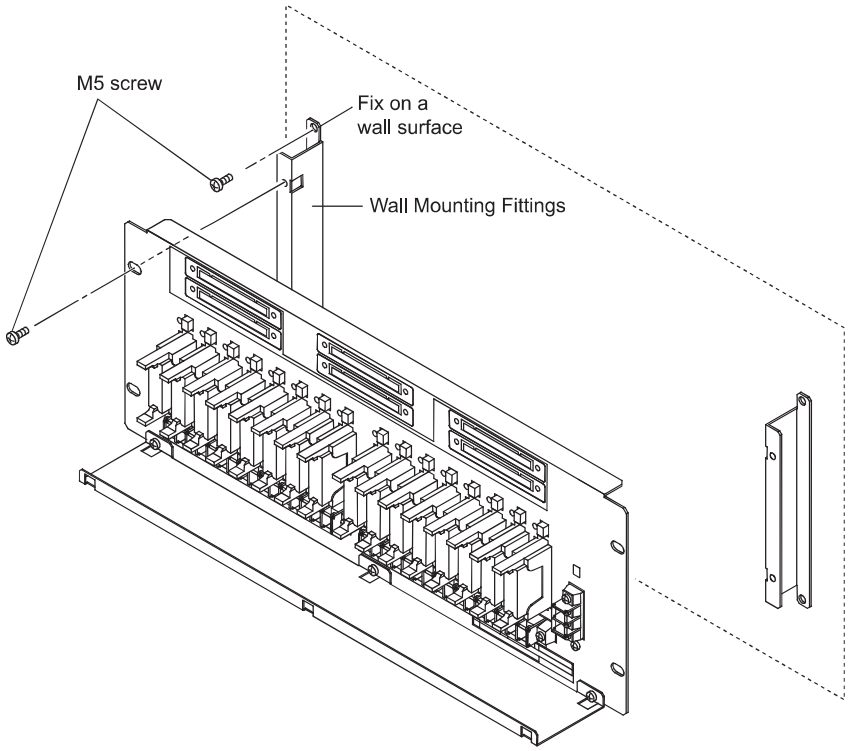


Figure C1.2.1-2 Mounting a rack mountable relay board on a wall

Follow these steps to mount a relay board on a wall:

1. Fix the wall-mounting fittings on the wall by tightening the M5 screws, two each on the left and right sides.
2. Mount the device on the wall by tightening four M5 screws.

Follow this step to remove a relay board from a wall:

- Hold the device by hand and unscrew the four M5 screws to remove the device.

SEE ALSO For more information about the mounting dimensions, screw locations, and number of screws for mounting relay boards on a wall, refer to:

ProSafe-RS/ProSafe-RS Lite Terminal Board/Relay Board (GS 32Q06L20-31E)

C1.2.2 Installing a DIN rail mountable terminal/relay board

This section describes how to mount a terminal board or relay board on a DIN rail and how to mount a terminal board on a wall.

Mounting and removing a DIN rail mountable terminal board

This section describes how to mount/remove a terminal board on/from a DIN rail.

Use a DIN rail that meets the TH35-7.5 in IEC 60715 and EN 50022.

IMPORTANT

In the back of a DIN rail mountable terminal board, there are two bumps (projections). When installing, make sure these bumps do not contact the screw tops on the DIN rail.

Mounting a terminal board on a DIN rail

1. As shown in the following figure, insert one side of the unit (the side without the latches) onto the DIN rail.

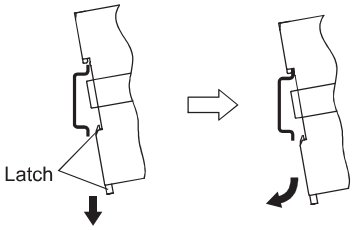


Figure C1.2.2-1 Mounting onto a DIN rail (1/2)

2. Push the unit in until you hear a clicking sound from the latches.

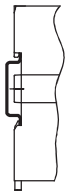


Figure C1.2.2-2 Mounting onto a DIN rail (2/2)

IMPORTANT

If the latches do not click onto the DIN rail easily, do not force them. Use a screwdriver to pull the latches from the outside while sliding the unit in.

Removing a terminal board from a DIN rail

Follow these steps to remove a terminal board from a DIN rail:

1. Use a flathead screwdriver to release the two DIN rail installation latches.

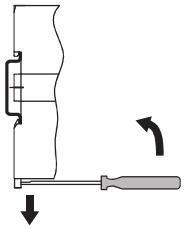


Figure C1.2.2-3 Uninstalling from a DIN rail (1/3)

2. The end with the latches becomes loose.

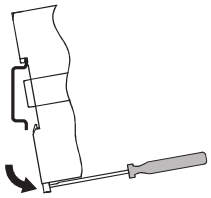


Figure C1.2.2-4 Uninstalling from a DIN rail (2/3)

3. Remove the terminal board from the end without latches.



Figure C1.2.2-5 Uninstalling from a DIN rail (3/3)

IMPORTANT

Do not forcefully rotate the terminal board when removing it.

- **Fasteners**

When installing a terminal board onto a DIN rail, you can use fasteners to hold it in place. These fasteners are not supplied and should be purchased separately. Mount the device on the DIN rail first and then secure it in place with the fasteners. To remove the device, take the fasteners off and then remove the device from the DIN rail.

Mounting and removing a DIN rail mountable relay board

This section describes how to mount/remove a relay board on/from a DIN rail.

Use a DIN rail that meets the TH35-7.5 in IEC 60715 and EN 50022.

CAUTION

The DIN rail mountable relay board (Model: SBM54D) may be hot, so you must be careful.

Mounting a relay board on a DIN rail

Follow these steps to mount a relay board on a DIN rail:

1. Tilt the relay board, lifting the bottom part of the relay board up towards you, and hook Groove a of the three attachments with the upper part of the DIN rail.

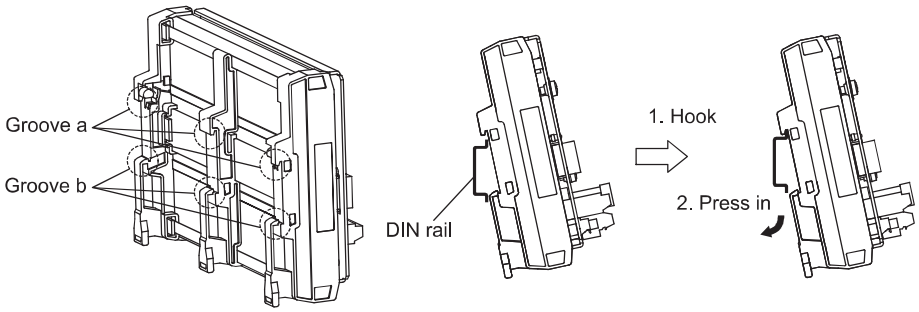


Figure C1.2.2-6 Mounting onto a DIN rail (1/2)

2. Push the tilted relay board until it becomes vertical.
   The lower part of the DIN rail fits into Groove b of the attachments. The following figure shows the relay board that is mounted on the DIN rail.

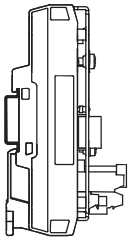


Figure C1.2.2-7 Mounting onto a DIN rail (2/2)

Removing a relay board from a DIN rail

Follow these steps to remove a relay board from a DIN rail:

1. Place your finger into the gap at the back of the relay board and push part A in the following figure in the direction shown in the figure.
   The hook on part B in the figure moves downward and a gap is created between the bottom of the DIN rail and groove b.
2. Gently pull the bottom of the relay board forward.
   The attachment separates from the DIN rail.
3. Repeat this procedure to detach the three attachments in order and remove the relay board.

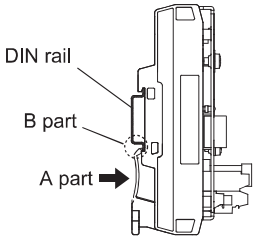


Figure C1.2.2-8 Removing from a DIN rail

Fasteners

When installing onto a DIN rail, you can use fasteners to hold it in place. These fasteners are not supplied and should be purchased separately. Mount the device on the DIN rail first and then secure it in place with the fasteners. To remove the device, take the fasteners off and then remove the device from the DIN rail.

Mounting/removing a DIN rail mountable terminal board on/from a wall

Follow this step to mount a terminal board on a wall:

- Mount the device on the wall by tightening two M4 screws.

IMPORTANT

The tightening torque of the screws should be approximately 0.8 N·m.

Follow this step to remove a terminal board from a wall:

- Hold by hand the device that you want to remove and unscrew the two M4 screws to remove the device.

SEE ALSO

For more information about the mounting dimensions, screw specifications, and space for cabling required to mount DIN rail mountable terminal boards on the wall, refer to:

ProSafe-RS/ProSafe-RS Lite Terminal Board/Relay Board (GS 32Q06L20-31E)

C1.2.3 Precautions when installing a DIN rail mountable terminal/relay board

This section describes the precautions when installing a DIN rail mountable terminal board or relay board.

Terminal/relay board installation orientations

Install a terminal board or relay board in the orientations shown in the following figure.

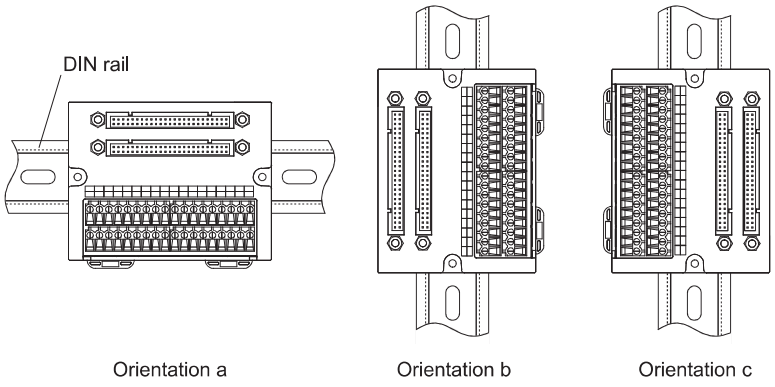


Figure C1.2.3-1 Terminal/relay board installation orientations (example of mounting SBT4D on a DIN rail)

IMPORTANT

When installing SBD2D in orientation b or c, the following conditions must be met:

- When the ambient temperature is less than 60 deg. C, the total current of the loads of all channels must be lower than the specified limit (8 A).
- When the ambient temperature is at 70 deg. C, the total current of the loads of all channels must be lower than 6 A.
- When the ambient temperature is between 60 deg. C and 70 deg. C, more precise calculation for current limit can be figured out by reducing 0.2 A from 8 A for each deg. C increase from 60 deg. C.

Precautions when installing SBT4D

SBT4D has a temperature sensor for reference junction compensation. To maintain reference junction compensation accuracy, the terminal board must not be affected by ambient heat. When installing a heat source nearby, install the heat source above the terminal board and terminal board wiring. If you must install the heat source next to or below the terminal board, install a heat shield.

IMPORTANT

The reference junction compensation is accurate when the ambient temperature is stable. If the ambient temperature changes, the measurements of the reference junction compensation accuracy will be incorrect until the temperature becomes stable again.

C1.3 Installing the node interface unit

The node interface unit that is used for N-IO nodes can be mounted either on a DIN rail or on a wall with screws. When you install the node interface unit, you must remove its cover first. Install the node interface unit, considering the space for maintenance work.

TIP

In the figures used in the installation procedures of the node interface unit, an empty node interface unit is shown.

SEE ALSO

For more information about removing the cover of the node interface unit, refer to:

"● Cover" on page B5-2

For more information about installation such as the information about space for maintenance works, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

Mounting the node interface unit on a DIN rail

The following figure shows how to mount the node interface unit on a DIN rail.

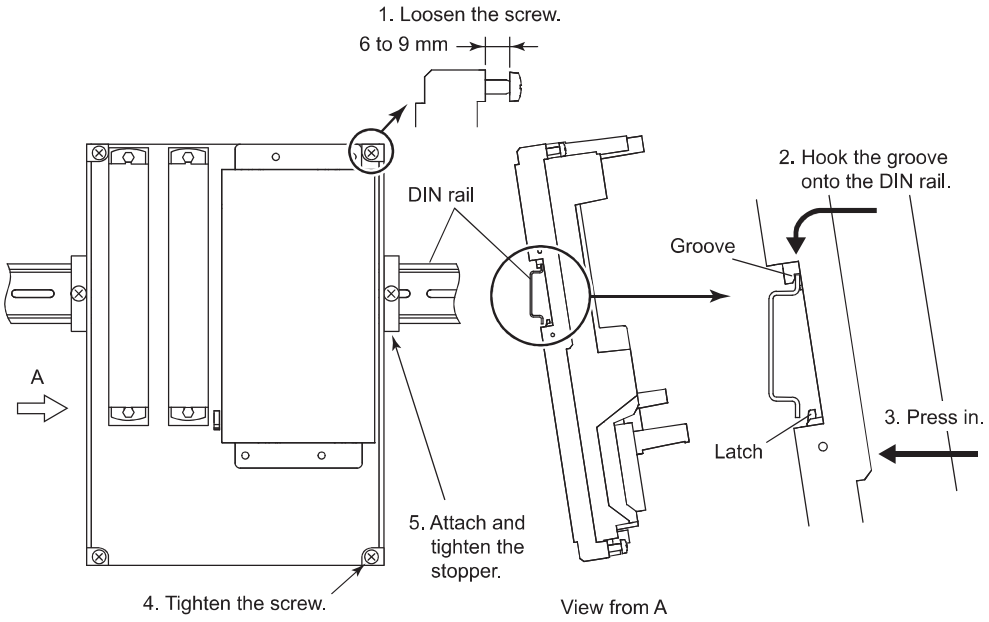


Figure C1.3-1 Mounting the node interface unit on a DIN rail

Follow these steps to mount the node interface unit on a DIN rail:

1. Loosen the four M4 screws on the node interface unit until the screw heads are 6 to 9 mm away from the bracket. Be careful not to loosen them further, or the screws may drop out of the holes.
2. Engage the upper groove in the back of the node interface unit with the top of the DIN rail.
3. Press the lower part of the node interface unit until the latch catches the DIN rail.
4. Tighten the four M4 screws on the node interface unit. Make sure that the node interface unit is fixed on the DIN rail.

IMPORTANT

The tightening torque of the screws should be 0.8 to 1.0 N·m.

5. Attach a DIN rail stopper on both sides of the node interface unit.

SEE ALSO For more information about DIN rail specifications, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

Removing the node interface unit from a DIN rail

The following figure shows how to remove the node interface unit from a DIN rail.

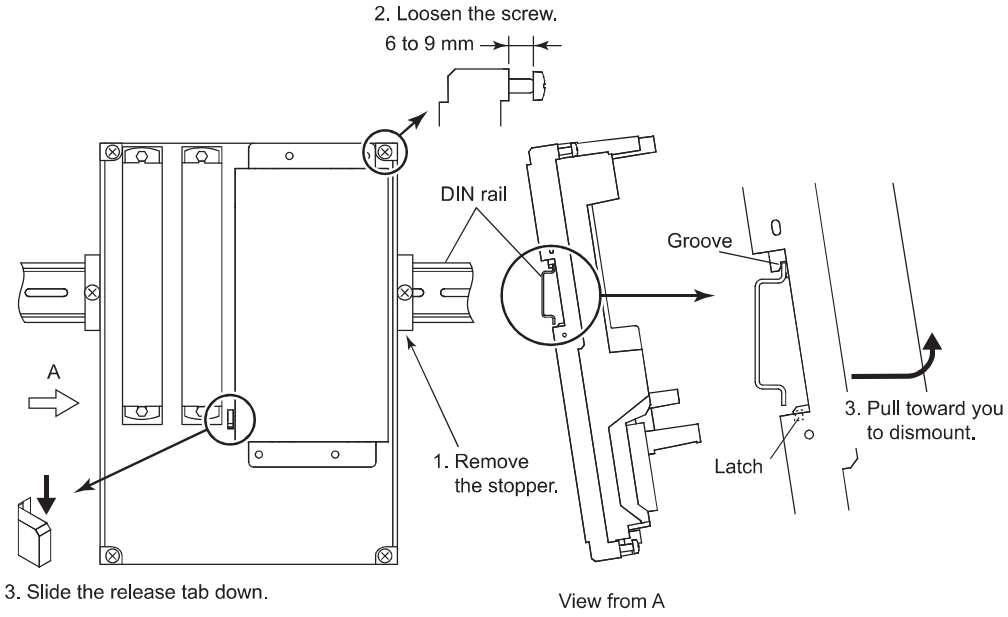


Figure C1.3-2 Removing the node interface unit from a DIN rail

Follow these steps to remove the node interface unit from a DIN rail:

1. Remove the DIN rail stoppers on both sides of the node interface unit.
2. Loosen the four M4 screws on the node interface unit until the screw heads are 6 to 9 mm away from the bracket. Be careful not to loosen them further, or the screws may drop out of the holes.
3. While pressing down the release tab by using a flat-blade screwdriver, pull the lower part of the node interface unit toward you to remove it.

Mounting/removing the node interface unit on/from a wall

Follow this step to mount the node interface unit on a wall:

- Mount the node interface unit on the wall by tightening the four M4 screws.

IMPORTANT

The tightening torque of the screws should be 0.8 to 1.0 N·m.

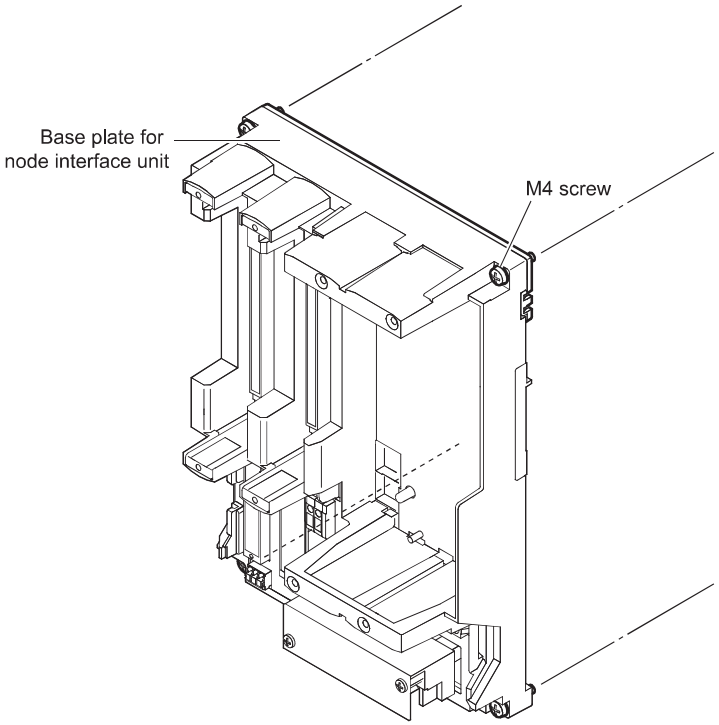


Figure C1.3-3 Mounting the node interface unit on a wall

Follow this step to remove the node interface unit from a wall:

- Holding the node interface unit by hand, unscrew the four fixing M4 screws and remove the node interface unit.

SEE ALSO For more information about the mounting dimensions, refer to:

ProSafe-RS Node Interface Units (for N-IO) (GS 32P06F20-01EN)

C1.4 Installing the N-IO I/O unit

This section describes the installation of the devices that constitute an N-IO I/O unit.

- Base plate
  - Base plate with disconnecting terminals
  - Base plate for barrier
- N-IO I/O module
- Intrinsic safety barrier
- Terminal block

When you install a base plate, you must consider the space for maintenance work.

TIP

This section describes how the base plate is installed when no modules are mounted on it.

SEE ALSO

For more information about securing space for maintenance works, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

C1.4.1 Installing the base plate with disconnecting terminals

The base plate with disconnecting terminals is available in two types: DIN rail mountable type and wall mountale type. This section describes the mounting and removing procedures for each type.

Mounting the base plate with disconnecting terminals on a DIN rail

The following figure shows how to mount the base plate with disconnecting terminals on a DIN rail.

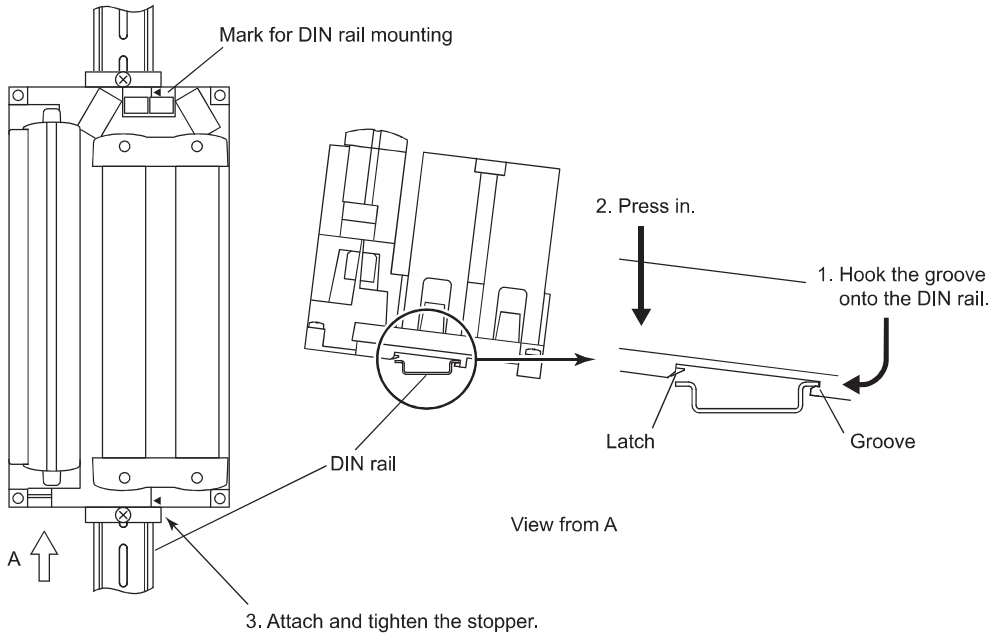


Figure C1.4.1-1 Mounting the base plate with disconnecting terminals on a DIN rail

Follow these steps to mount the base plate with disconnecting terminals on a DIN rail:

1. Engage the right-hand groove in the back of the base plate with disconnecting terminals with the DIN rail.
2. Press the left part of the base plate until the latch catches the DIN rail.
3. Attach the DIN rail stoppers on the top and bottom of the base plate with disconnecting terminals.
   However, if you mount multiple base plates, attach only one stopper between base plates.
4. Make sure that the base plate with disconnecting terminals is fixed on the DIN rail.

SEE ALSO For more information about DIN rail specifications, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

Removing the base plate with disconnecting terminals from a DIN rail

The following figure shows how to remove the base plate with disconnecting terminals from a DIN rail.

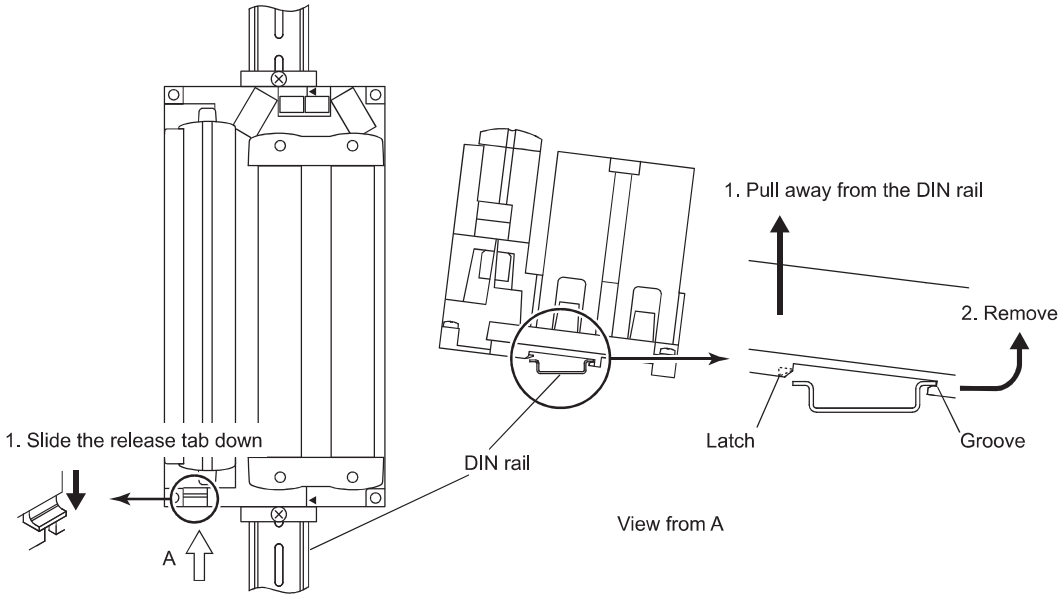


Figure C1.4.1-2 Removing the base plate with disconnecting terminals from a DIN rail

Follow these steps to remove the base plate with disconnecting terminals from a DIN rail:

1. Hold down the release tab at the bottom of the base plate with disconnecting terminals by using a Phillips screwdriver and pull the left end of the base plate away from the DIN rail.
2. Move the base plate with disconnecting terminals to the right and remove it.

Mounting/removing the base plate with disconnecting terminals on/from a wall

Follow this step to mount the base plate with disconnecting terminals on a wall:

- Mount the base plate with disconnecting terminals on the wall by tightening the four M4 screws.

IMPORTANT

The tightening torque of the screws should be 0.8 to 1.0 N·m.

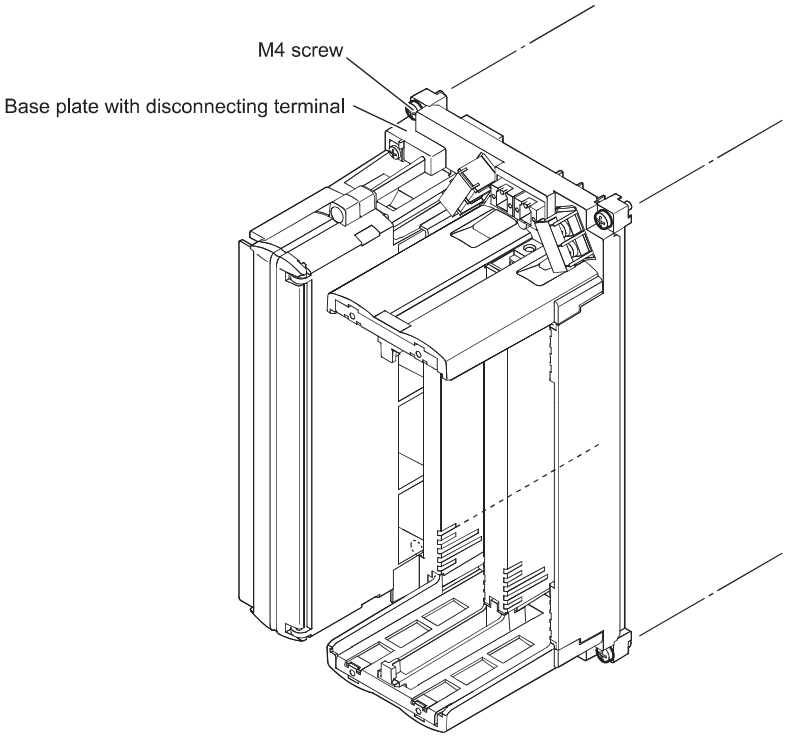


Figure C1.4.1-3 Mounting the base plate with disconnecting terminals on a wall

Follow this step to remove the base plate with disconnecting terminals from a wall:

- Hold the base plate with disconnecting terminals by hand and unscrew the four M4 screws to remove the base plate.

C1.4.2 Installing the base plate for barrier

This section describes the installation of the base plate for barrier.

Mounting and removing the base plate for barrier (Model: S2BN4D)

The base plate for barrier S2BN4D is mounted on a wall when it is used. To ensure single point grounding of the base plate, use insulated supporters when mounting it.

The following figure shows how to mount the base plate for barrier S2BN4D on a wall.

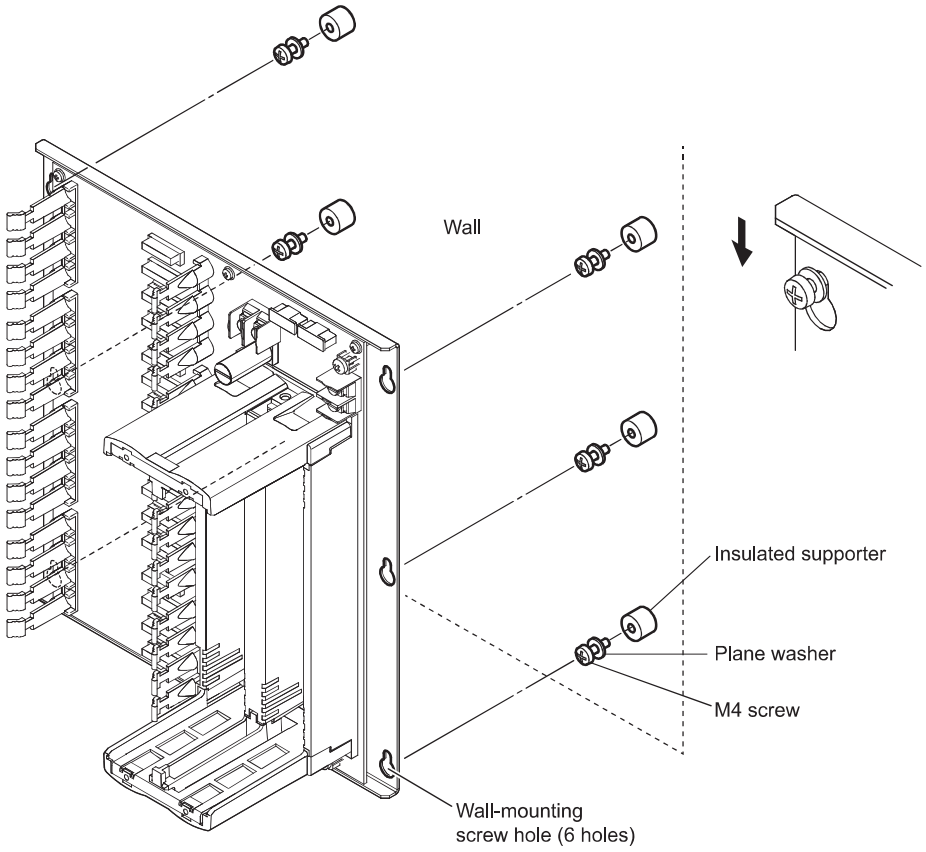


Figure C1.4.2-1 Mounting S2BN4D on a wall

IMPORTANT

When you mount S2BN4D, use M4 screws with the length suited for the insulated supporter and flat washers with a 9 mm or less external diameter. The thickness of the S2BN4D around the mounting screw holes is 1.6 mm.

Follow these steps to mount the base plate for barrier S2BN4D on a wall:

1. Fit the six M4 screws for mounting into the hole of the insulated supporters that are fixed on the wall.
2. Pass the screws that you have placed on the wall through the six wall-mounting screw holes of the base plate, and slightly shift the base plate downward so that the screws fit into the narrow part of the holes.
3. Mount the base plate for barrier on the insulated supporters by tightening the six M4 screws.

Follow these steps to remove the base plate for barrier from a wall:

1. Loosen the six M4 screws. You must only loosen the screws without removing them from the insulated supporters.
2. In reverse of the mounting procedure, slightly shift the base plate upward and remove the base plate by releasing it from the screws.

SEE ALSO For more information about the screw mounting dimensions for S2BN4D, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

Mounting and removing the base plate for barrier (Model: S2BN5D)

Follow this step to mount S2BN5D on a wall:

- Mount the base plate for barrier on the wall by tightening the four M4 screws.

IMPORTANT

Prepare M4 screws that meet the following conditions:

- When washers are used
  - Screw with a length of 18 mm or more
  - Plane washer with a diameter of 8 mm or less
- When washers are not used
  - Screw with a length of 16 mm or more

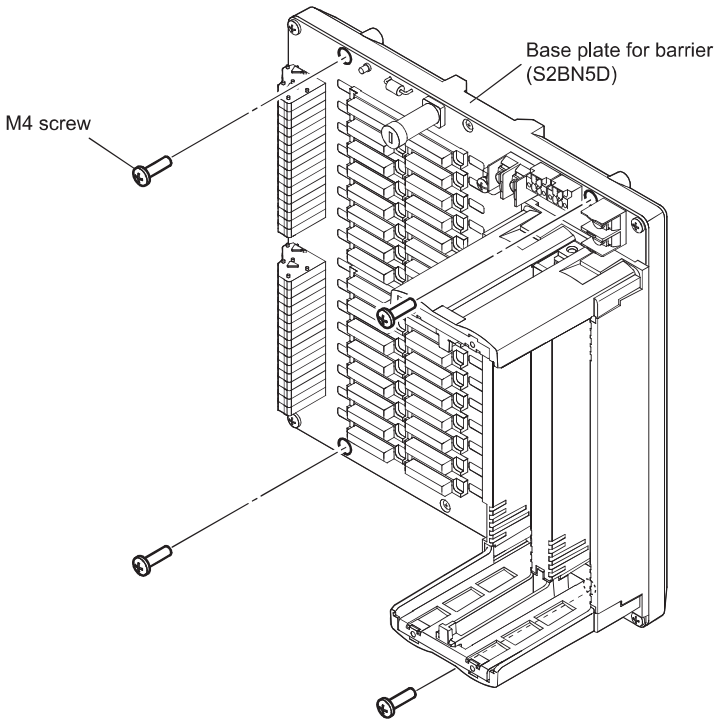


Figure C1.4.2-2 Mounting S2BN5D on a wall (without washers)

Follow this step to remove S2BN5D from a wall:

- Hold the base plate for barrier by hand and unscrew the four M4 screws.

SEE ALSO For more information about the screw mounting dimensions for S2BN5D, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

C1.4.3 Mounting N-IO I/O module

This section describes how to mount/remove the N-IO I/O module onto/from a base plate.

Mounting and removing the N-IO I/O module

Follow this step to mount an N-IO I/O module onto a base plate:

- Mount the N-IO I/O module on the base plate by tightening the two M3 screws.

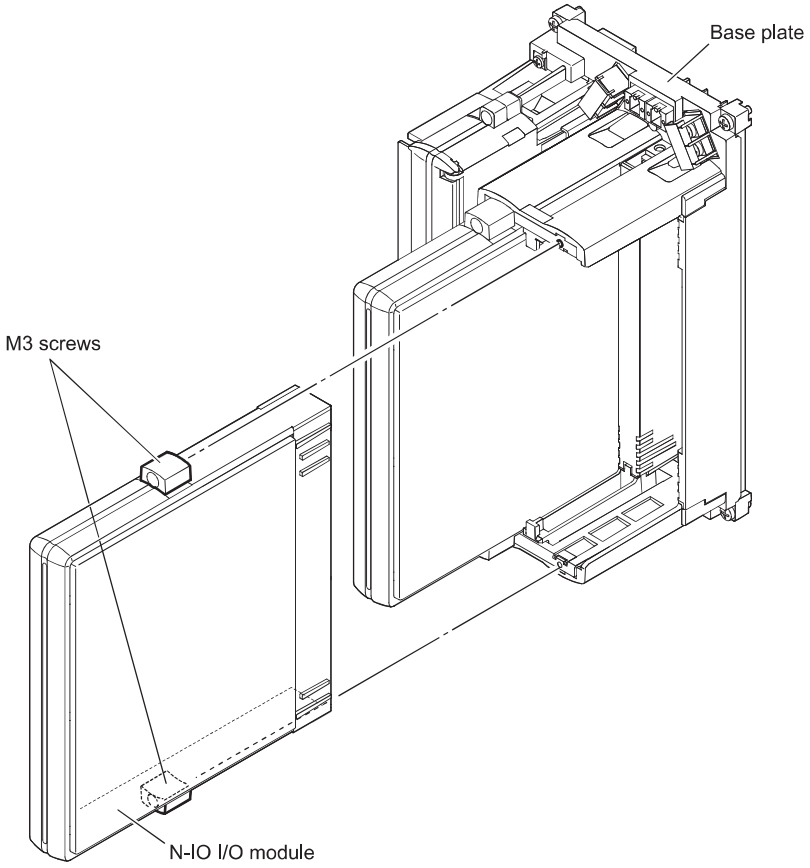


Figure C1.4.3-1 Example of mounting N-IO I/O module

Follow this step to remove an N-IO I/O module from a base plate:

- Loosen the two M3 screws and remove the N-IO I/O module.

CAUTION

Be aware that the modules may be hot.

Mounting and removing a dummy cover for I/O module

You must attach a dummy cover (Model: S2DCV02) to unused N-IO I/O module slots.

Follow these steps to mount a dummy cover on the N-IO I/O module slot:

1. Engage the dummy cover with the bottom edge of the N-IO I/O module slot.
2. Press the top of the dummy cover in the direction shown in the figure.

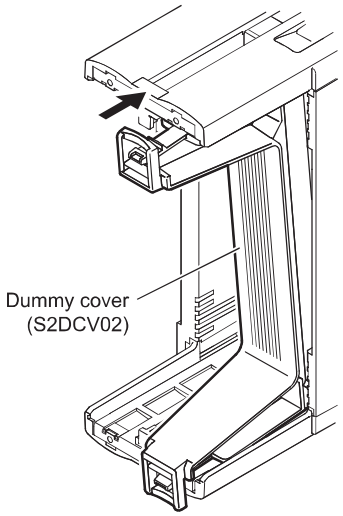


Figure C1.4.3-2 Mounting a dummy cover

Follow these steps to remove a dummy cover from the N-IO I/O module slot:

1. Press down the claw at the top of the dummy cover.
2. Remove the dummy cover from the slot.

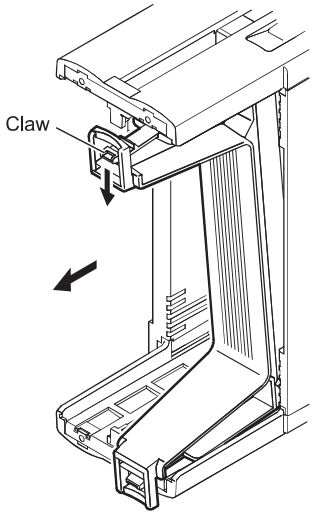


Figure C1.4.3-3 Removing a dummy cover

C1.4.4 Mounting intrinsic safety barriers

This section describes how to mount/remove intrinsic safety barriers.

Mounting intrinsic safety barriers: S2BN4D

This section describes how to mount/remove intrinsic safety barriers onto/from the base plate for barrier S2BN4D.

Mounting an intrinsic safety barrier onto S2BN4D

The following figure shows how to mount an intrinsic safety barrier onto the base plate for barrier S2BN4D.

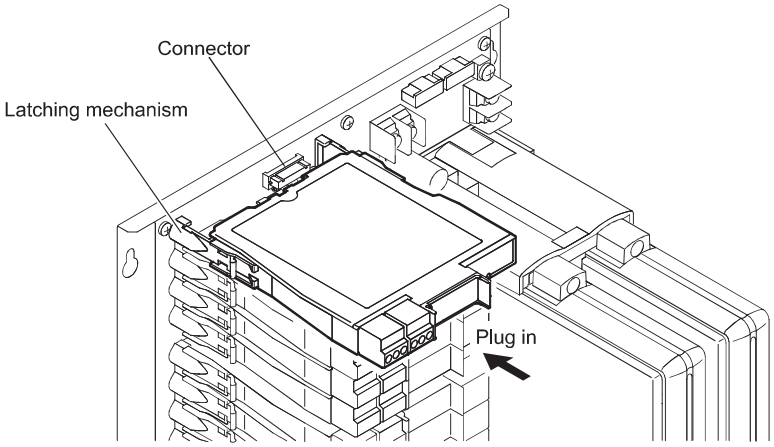


Figure C1.4.4-1 Mounting an intrinsic safety barrier onto S2BN4D

Follow these steps to mount an intrinsic safety barrier onto the base plate for barrier S2BN4D:

1. Confirm the channel on which you mount an intrinsic safety barrier.
2. Insert the barrier into the latching mechanism of the base plate.
3. Connect the connector of the barrier to the connector of the base plate.

Removing an intrinsic safety barrier from S2BN4D

The following figure shows how to remove an intrinsic safety barrier from the base plate for barrier S2BN4D.

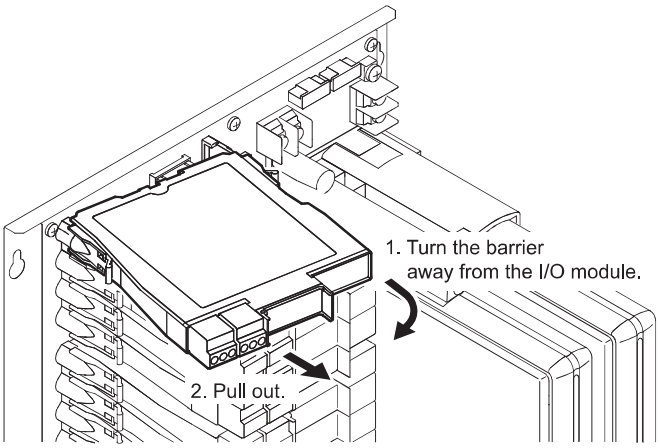


Figure C1.4.4-2 Removing an intrinsic safety barrier from S2BN4D

Follow these steps to remove an intrinsic safety barrier from the base plate for barrier S2BN4D:

1. To release the barrier from the latching mechanism, turn the barrier as shown in the figure so that the part closer to the N-IO I/O module comes toward you. If it is difficult to turn the barrier, turn the barrier while expanding the latching mechanism on the N-IO I/O module side.
   The barrier is disconnected from the connector.
2. Pull out the barrier to remove it from the base plate.

Mounting intrinsic safety barriers: S2BN5D

This section describes how to mount/remove intrinsic safety barriers onto/from the base plate for barrier S2BN5D.

Mounting an intrinsic safety barrier onto S2BN5D

The following figure shows how to mount an intrinsic safety barrier onto the base plate for barrier S2BN5D.

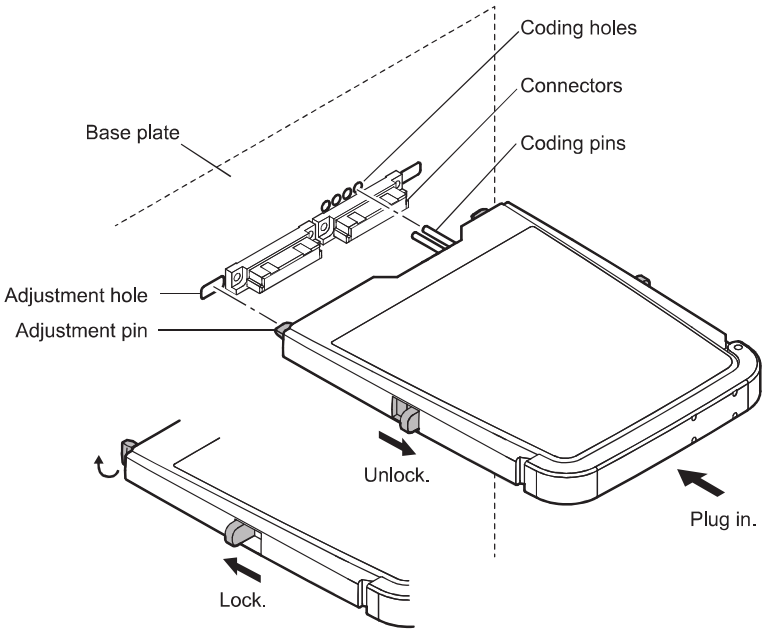


Figure C1.4.4-3 Mounting an intrinsic safety barrier onto S2BN5D

Follow these steps to mount an intrinsic safety barrier onto the base plate for barrier S2BN5D:

1. Confirm the module number on the base plate where you mount an intrinsic safety barrier.
2. Slide the tabs on both sides of the barrier toward you to set them in the UNLOCK position.
3. Carefully press the barrier perpendicularly to the base plate so that the barrier is plugged into the connector of the base plate.
   When you plug the barrier, fit the adjustment pins of the barrier to the adjustment holes that are located on both sides of the connectors on the base plate.
4. Slide the tabs on both sides of the barrier toward the base plate to set them in the LOCK position.
   The adjustment pins of the barrier rotate, fixing the barrier on the base plate.

Removing an intrinsic safety barrier from S2BN5D

The following figure shows how to remove an intrinsic safety barrier from the base plate for barrier S2BN5D.

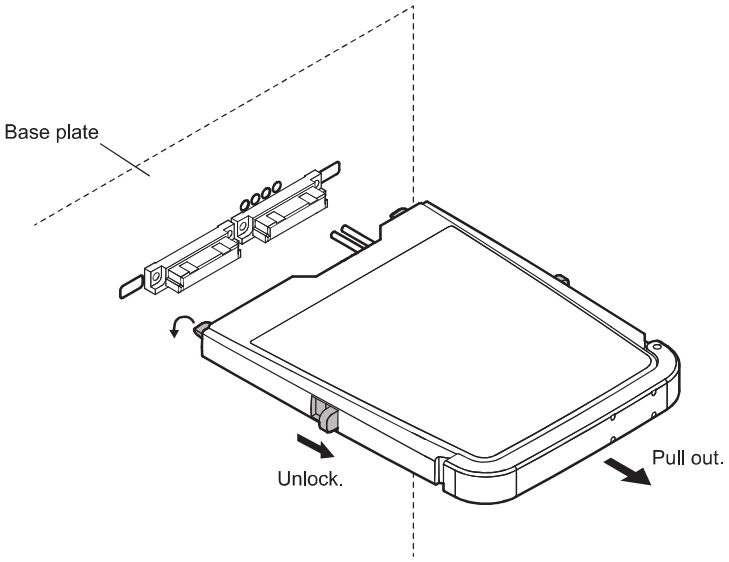


Figure C1.4.4-4 Removing an intrinsic safety barrier from S2BN5D

Follow these steps to remove an intrinsic safety barrier from the base plate for barrier S2BN5D:

1. Slide the red tabs on both sides of the barrier toward you to set them in the UNLOCK position.
2. Pull out the barrier horizontally from the connector of the base plate.

C1.4.5 Mounting the terminal block

Follow this step to mount the terminal block onto a base plate:

- Mount the terminal block onto the base plate by tightening the two M3 screws.

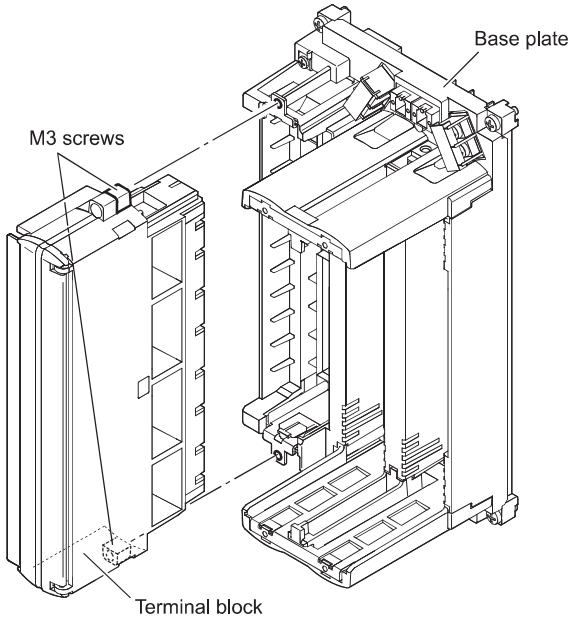


Figure C1.4.5-1 Mounting the terminal block

Follow this step to remove the terminal block from a base plate:

- Loosen the two M3 screws and remove the terminal block.

C1.5 Installing the terminal board (for N-IO node)

You can mount a terminal board on a DIN rail or on a wall. The terminal board must be oriented as instructed here when you mount it on either a DIN rail and a wall.

The following figures show an example of orientation when a terminal board is mounted on a DIN rail.

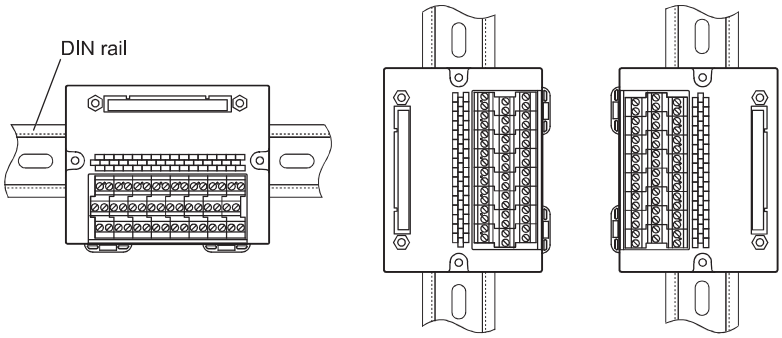


Figure C1.5-1 Orientation of terminal board to mount

When you mount a terminal board, you must consider sufficient clearance around it for maintenance works.

SEE ALSO For more information about securing space for maintenance works, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

■ Mounting/removing a terminal board on/from a DIN rail

You can mount a terminal board on a DIN rail or remove it from a DIN rail with the same procedures as the procedures for a DIN rail mountable terminal board for FIO node.

SEE ALSO For more information about mounting/removing a terminal board on/from a DIN rail, refer to:

"■ Mounting and removing a DIN rail mountable terminal board" on page C1-7

For more information about the specifications and installation of DIN rails, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

■ Mounting/removing a terminal board on/from a wall

You can mount a terminal board on a wall or remove it from a wall with the same procedures as the procedures for a DIN rail mountable terminal board for FIO node.

SEE ALSO For more information about mounting/removing a terminal board on/from a wall, refer to:

"■ Mounting/removing a DIN rail mountable terminal board on/from a wall" on page C1-10

For more information about the mounting dimensions, refer to:

ProSafe-RS Terminal Boards (for N-IO) (GS 32P06L20-01EN)

For more information about the specifications for wall mount screw, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

C1.6 Installing the field power supply unit

The power supply unit for CENTUM VP (Model: A2PW50□/DN) can be used as a field power supply that is connected to the base plate of ProSafe-RS.

The following figure shows how to mount A2PW50□/DN on a DIN rail.

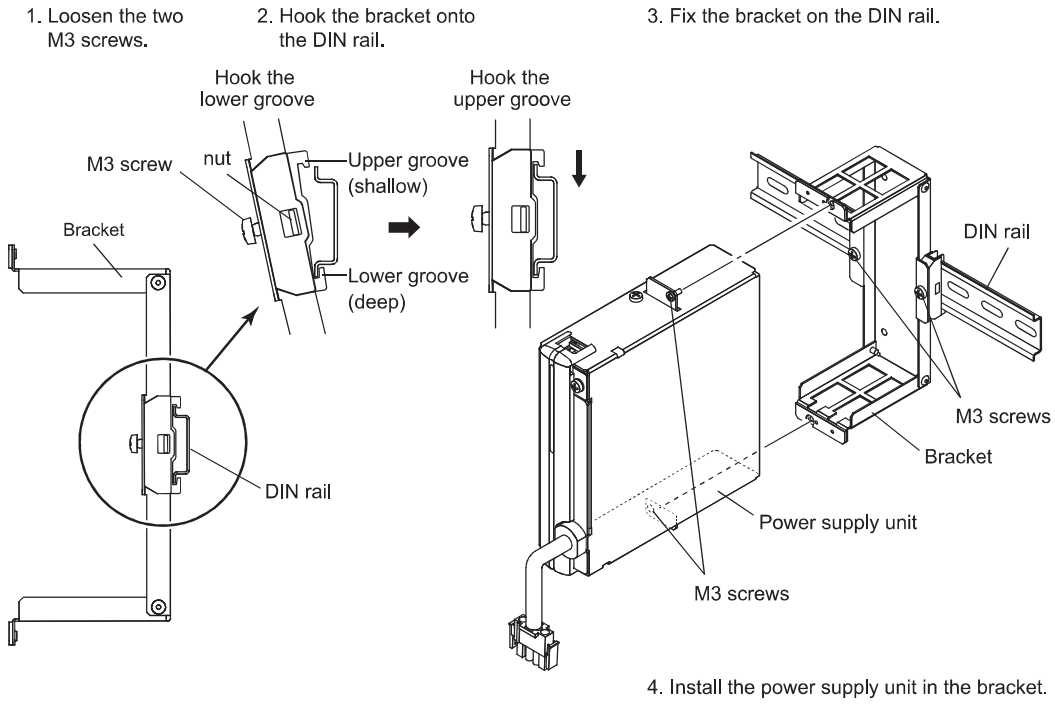


Figure C1.6-1 Mounting A2PW50□/DN on a DIN rail

Follow these steps to mount the power supply unit on a DIN rail:

1. Loosen the two M3 screws of the bracket.
   You must only loosen the screws without removing them from the nut.
2. Hook the bracket onto the DIN rail as shown in the figure.
3. Tighten the two M3 screws of the bracket to fix the bracket on the DIN rail.
4. Install the power supply unit in the bracket by tightening the two M3 screws on the power supply unit.

C2. Ground wiring and power supply wiring for SCS

This section describes the ground wiring and power supply wiring of the following SCS devices:

- Power supply module
- power supply unit for fan unit
- FIO node, terminal board/relay board
- Node interface unit
- N-IO I/O unit

WARNING

- Turn off the power supply source, and be sure that no electricity is flowing into the power cable to be connected before starting the work.
- Provide a separate switch or breaker for turning on/off the power.

CAUTION

The power cable must be wired through a conduit at the entrance of the instrument panel for the following reasons:

- To prevent the power cable from being damaged through direct contact with the metal plate.
- To prevent an excessive load being applied to the power supply connection terminals due to the weight of the cable itself.

IMPORTANT

Wire the power cable by keeping a minimum distance of 1 cm from other signal wiring.

C2.1 Ground wiring and power supply wiring of the power supply module

The following figure shows the power supply terminals and grounding terminal of the power supply module that is installed in the SCU, SNU, or unit for optical bus repeater module.

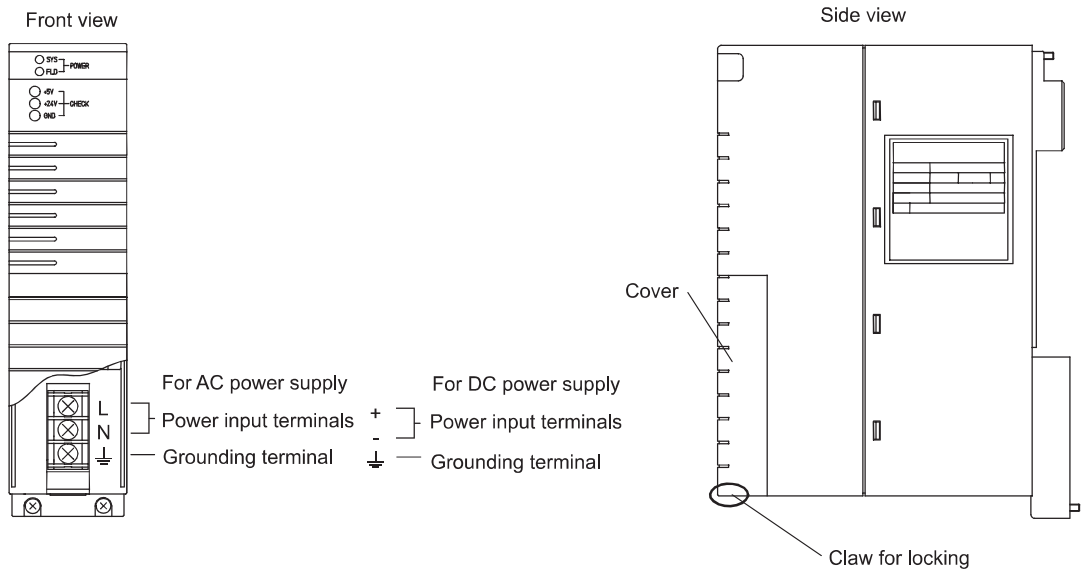


Figure C2.1-1 Power supply terminals and grounding terminal of the power supply module

Follow these steps to connect the power supply cable to the power supply module. The power supply cable should be purchased separately.

1. Find a claw at the lower side of the protective cover (marked with a circle in the figure). Push the claw upward to unlock it and gently pull the protective cover toward you. The protective cover is removed.
2. Connect the power cable to the power input terminals. Connect the grounding cable to the grounding terminal. The screw of the terminal is an M4 screw.
3. Put back the protective cover after the wiring is completed.

SEE ALSO For more information about power supply wiring and ground wiring cables and cable termination, refer to:

- ProSafe-RS Installation Guidance (TI 32P01J10-01EN)
- ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

C2.2 Connecting the power cable to the power supply unit for fan unit

Power supply units for fan unit are provided in the left and right of the node fan unit. Connect a power cable to each of the power supply units. The following figure shows the power input terminals and grounding terminal of the power supply unit for fan unit.

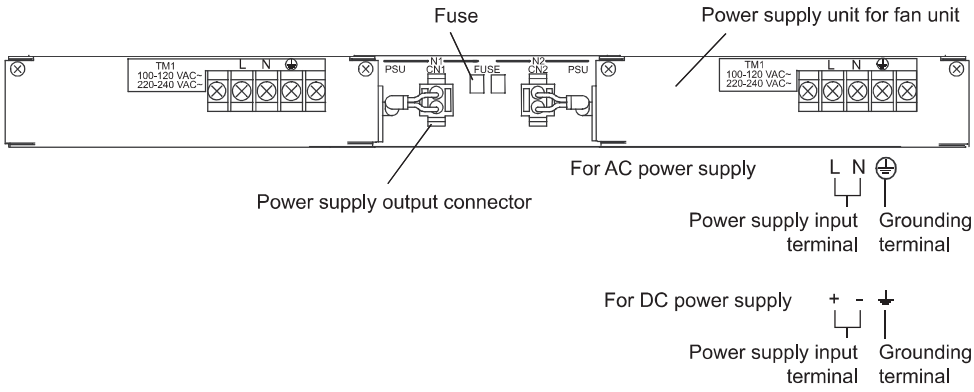


Figure C2.2-1 Power input terminals and grounding terminal of the power supply unit for fan unit

Follow these steps to connect the power cable to the power supply unit for fan unit:

1. Remove the protective cover of the power supply module.
2. Connect the power cable to the power input terminals and the grounding cable to the grounding terminal. The screw of the terminal is an M4 screw.
3. After the connection is completed, put back the protective cover.

SEE ALSO For more information about power supply wiring and ground wiring cables and cable termination, refer to:

- ProSafe-RS Installation Guidance (TI 32P01J10-01EN)
- ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

C2.3 Connecting the field power supply cable to a DIN rail mountable terminal board/relay board (for FIO node)

CAUTION

You can use dual field power supply. Before connecting the power supply, check the positive and negative polarity.

Follow this step to connect the field power supply cable to a DIN rail mountable terminal board or relay board:

- Confirming the cable polarity, insert the cable to the pressure clamp terminal and tighten the screw.

IMPORTANT

The tightening torque of the screws should be 0.5 to 0.6 N·m.

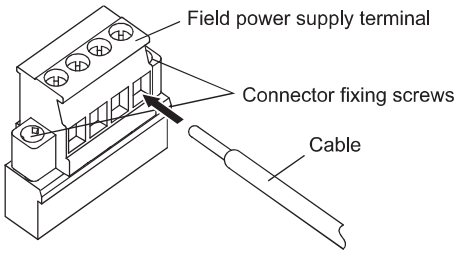


Figure C2.3-1 Connecting the field power supply cable

TIP

By loosening the connector fixing screws, you can detach the field power input terminals from the body and connect the power cable.

SEE ALSO

For more information about Cable termination, refer to:

"■ Signal connections to a DIN rail mountable terminal board/relay board" on page D1-9

C2.4 Ground wiring of the FIO node devices

To prevent effects of external noise, grounding terminals must be grounded to the protective grounding system: The following devices have a grounding terminal:

- SCU
- SNU
- Unit for optical bus repeater module
- Rack mountable terminal board
- Rack mountable relay board
- DIN rail mountable relay board

Ground wiring

Use the grounding terminals to ground the devices. The screw of the grounding terminal is an M4 screw.
Pull down the grounding wire through the tray and from the right side of the rack.

- Ground the grounding terminal to the protective grounding system.
- Use cables with a nominal conductor cross-sectional area of 2.0 mm^2 or more.

IMPORTANT

You must ground the devices individually without connecting their grounding terminals to each other.

The following figure shows an example of the ground wiring of SCU.

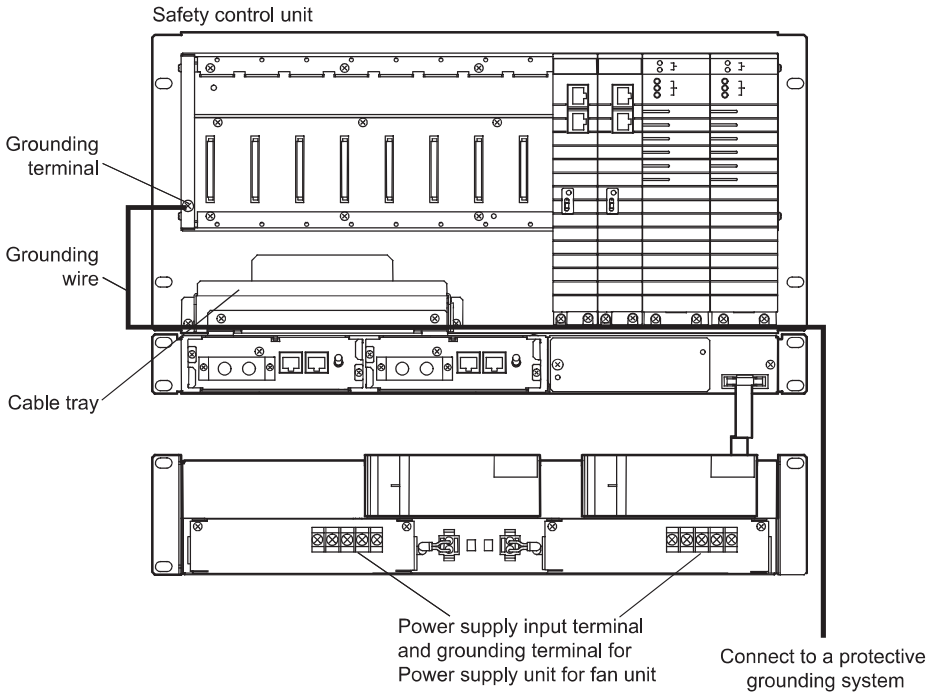


Figure C2.4-1 Ground wiring of SCU

The following figure shows an example of the ground wiring of SNU.

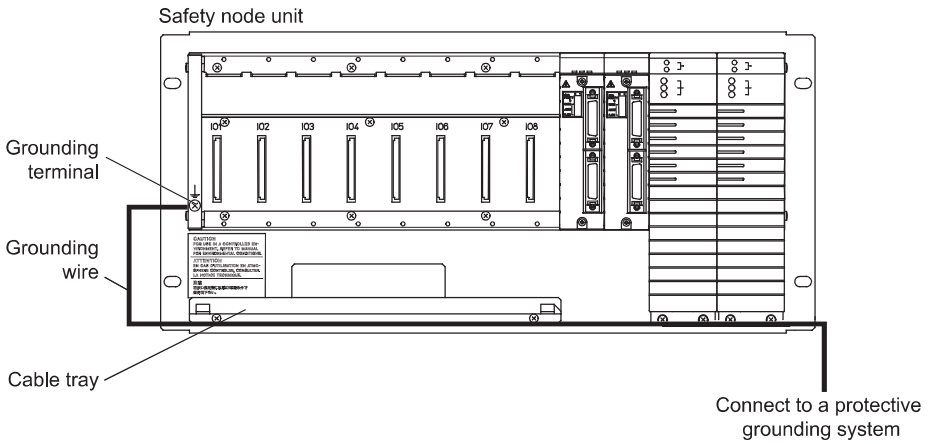


Figure C2.4-2 Ground wiring of SNU

The following figure shows an example of ground wiring of the unit for optical bus repeater module.

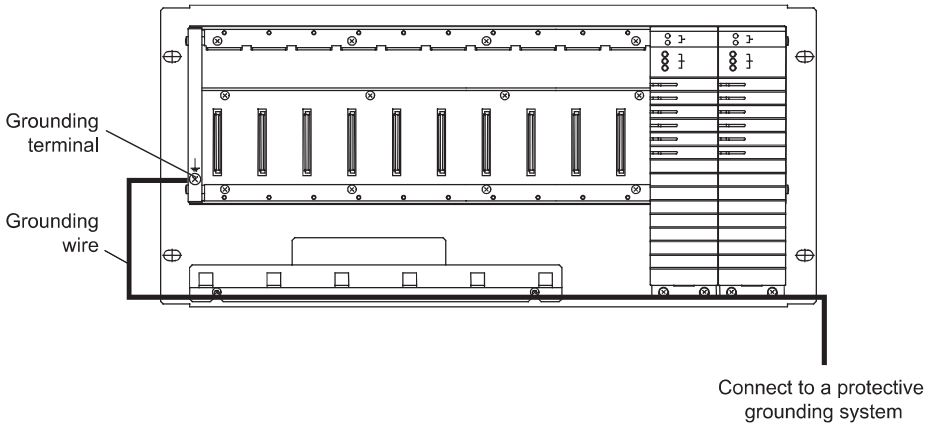


Figure C2.4-3 Ground wiring of the unit for optical bus repeater module

The following figure shows an example of the ground wiring of a rack mountable terminal board.

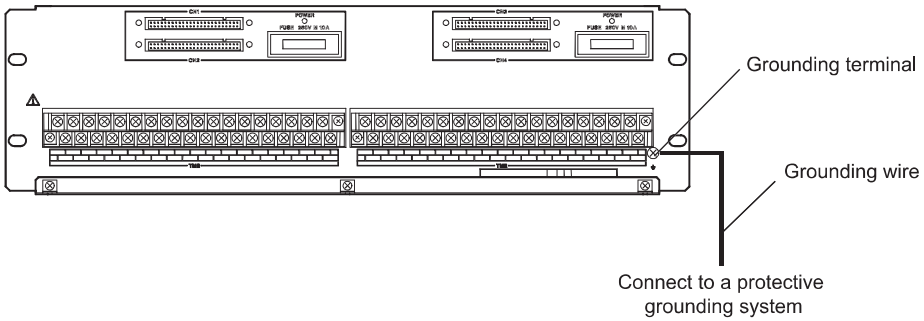


Figure C2.4-4 Ground wiring of a rack mountable terminal board

The following figure shows an example of the ground wiring of a rack mountable relay board.

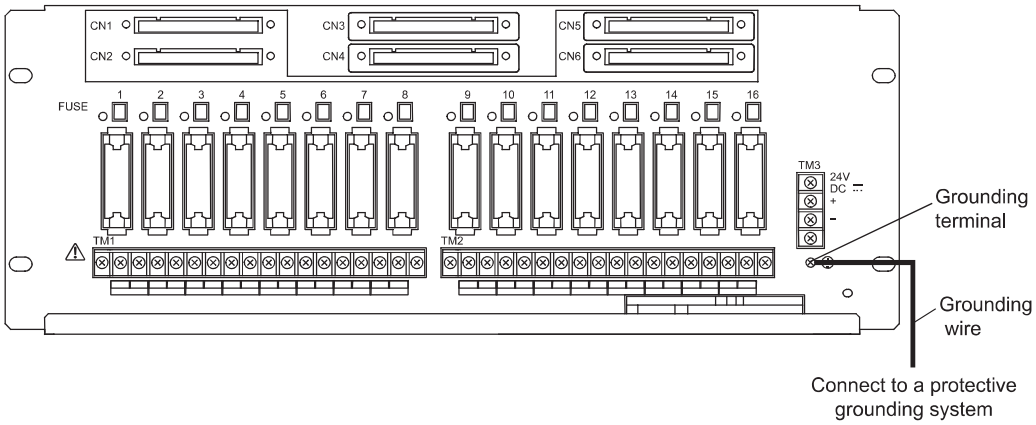


Figure C2.4-5 Ground wiring of a rack mountable relay board

The following figure shows an example of the ground wiring of a DIN rail mountable relay board.

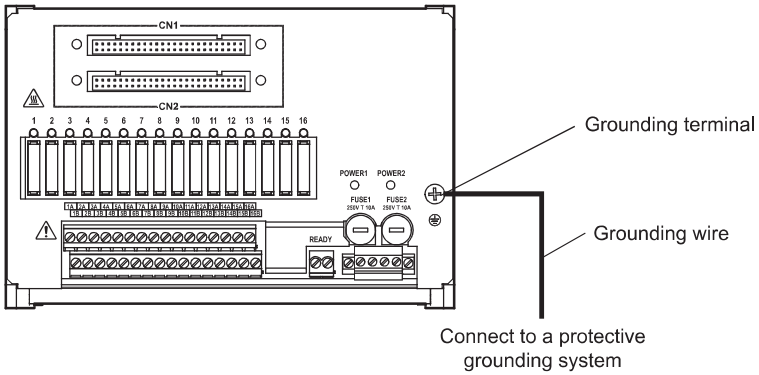


Figure C2.4-6 Ground wiring of a DIN rail mountable relay board

SEE ALSO

For more information about ground wiring cables and cable termination, refer to:

- ProSafe-RS Installation Guidance (TI 32P01J10-01EN)
- ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

C2.5 Ground and power supply wiring of the node interface unit

This section describes the ground wiring and power supply wiring of the components of the node interface unit.

- Ground wiring of the base plate for node interface unit
- Ground wiring and power supply wiring of the power supply unit

C2.5.1 Ground wiring of the base plate for node interface unit

Connect the grounding terminal of the base plate for node interface unit to the protective grounding system. The screw of the grounding terminal is an M4 screw.

Remove the cover of the node interface unit before you connect the cable, and put it back after you finished the connection.

Use cables with a nominal conductor cross-sectional area of 2.0 mm^2 or more.

SEE ALSO

For more information about the grounding terminal of the base plate for node interface unit, refer to:

"■ Elements on the base plate for node interface unit" on page B5-4

For more information about removing and attaching the cover of the node interface unit, refer to:

"● Cover" on page B5-2

For more information about ground wiring cables and cable termination, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

C2.5.2 Ground and power supply wiring of the power supply unit

This section describes the ground and power supply wiring of the power supply unit.

The cables should be purchased separately. For ground wiring and power supply wiring, use cables with the following nominal conductor cross-sectional areas:

- Grounding cable: 1.25 to 2.0 mm^2
- Power supply cable: 1.25 mm^2

SEE ALSO For more information about examples of conforming power supply wiring and ground wiring cables and cable termination, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

Ground wiring of the power supply unit

Prepare an appropriate cable and ground the grounding terminal of the power supply unit to the protective grounding system. The screw of the grounding terminal is an M4 screw. Use the screw that came with the product.

Power supply wiring of the power supply unit

IMPORTANT

When you connect cables to pressure clamp terminals, use a flat-blade screwdriver that conforms to the DIN 5264B standard having a thickness at the tip of 0.6 mm and a body shaft diameter of 3.5 mm.

Follow these steps to install the wiring by using the cables that you prepare:

1. Release the lower claw of the cover.
2. Lift the cover up to release the upper claw of the cover.
   The cover leaves the power supply unit.
   The following figure shows how to remove the cover.

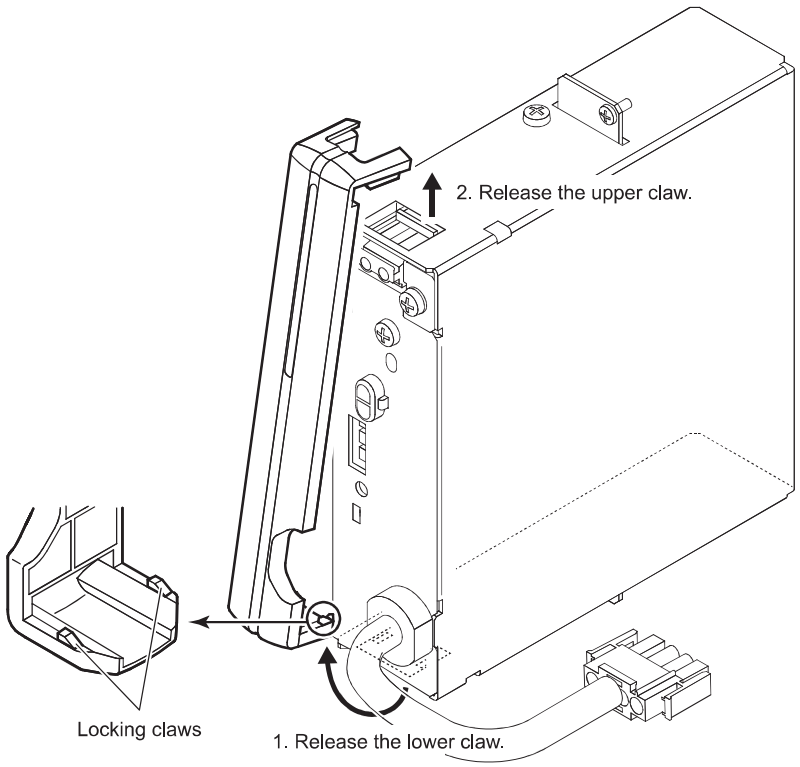


Figure C2.5.2-1 Removing the cover

3. Insert the power supply cables to the pressure clamp terminals and tighten the screws.

IMPORTANT

The tightening torque of the screws should be 0.5 N·m.

The following figure shows how to install the power cable.

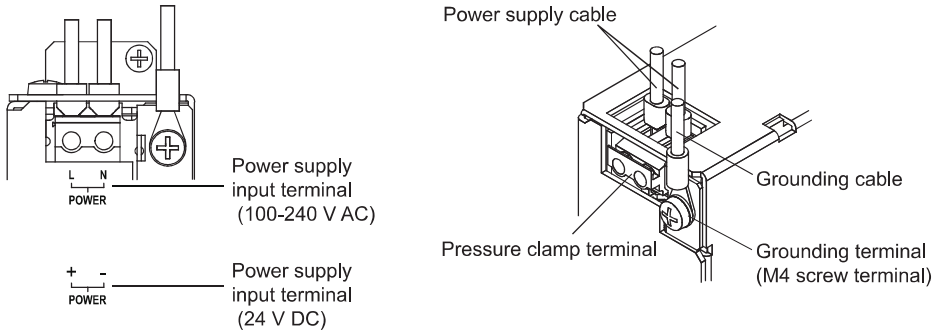


Figure C2.5.2-2 Connecting the power cables

4. Hook the upper claw of the cover over the groove at the top of the power supply unit.
5. Press the lower end of the cover until the claw fits into the groove in the bottom of the power supply unit.
6. Connect the cables to the power supply source.

Ensure that the power cables do not touch the case.

Output wiring of the power supply unit

The following figure shows the output cable wiring of the power supply unit.

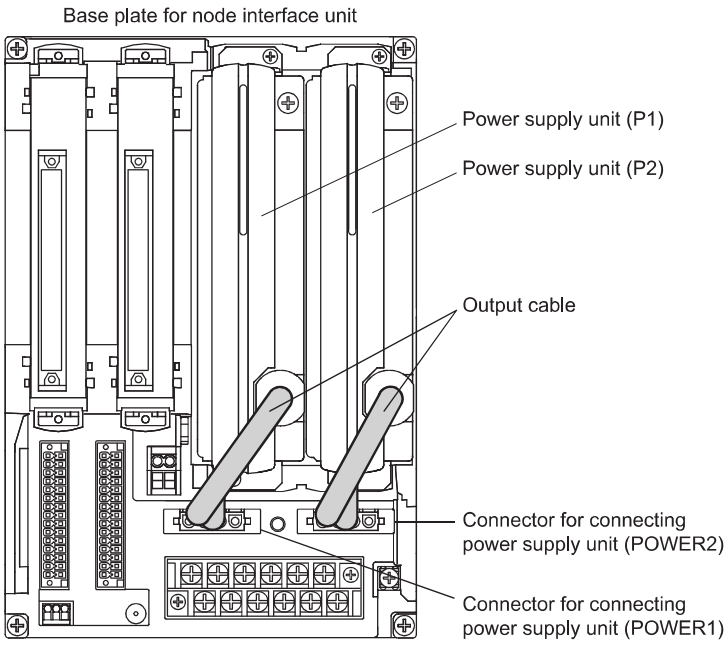


Figure C2.5.2-3 Output wiring of the power supply unit

Follow these steps to connect the output cable of the power supply unit:

1. Remove the cover of the node interface unit.
2. Connect the output cable of the power supply unit to the connector for connecting power supply unit on the base plate for node interface unit.
3. Attach the cover of the node interface unit.

SEE ALSO For more information about removing and attaching the cover of the node interface unit, refer to:

"● Cover" on page B5-2

C2.6 Ground and power supply wiring of the N-IO I/O unit

This section describes the ground wiring and power supply wiring of the base plate for N-IO I/O unit.

- Ground wiring
- System power supply wiring
- Field power supply or barrier power supply wiring

Ground wiring of base plates

The following figure shows an example of ground wiring of base plates.

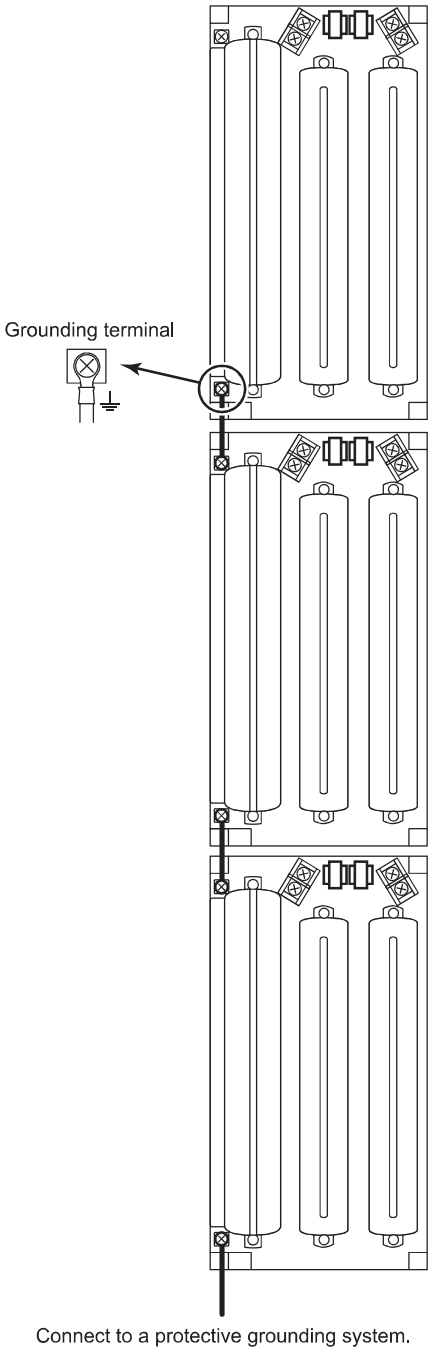


Figure C2.6-1 Ground wiring of base plates

Ground any one of the grounding terminals that are provided at the top and bottom of each base plate to the protective grounding system. The screw of the grounding terminal of the base plate with disconnecting terminals is an M3 screw. The screw of the grounding terminal of the base plates for barrier S2BN4D and S2BN5D is an M4 screw.

IMPORTANT

For S2BN4D, the tightening torque of the screws should be 0.81 to 0.99 N·m.

If the base plates are installed adjacently, connect the grounding terminals of the neighboring base plates by using the provided grounding cable and ground the top or bottom base plate to the protective grounding system.

SEE ALSO For more information about ground wiring cables and cable termination, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

System power supply wiring

For system power supply wiring, use the power cable for base plates (Model: S2KPB10).

The following figure shows the system power supply wiring.

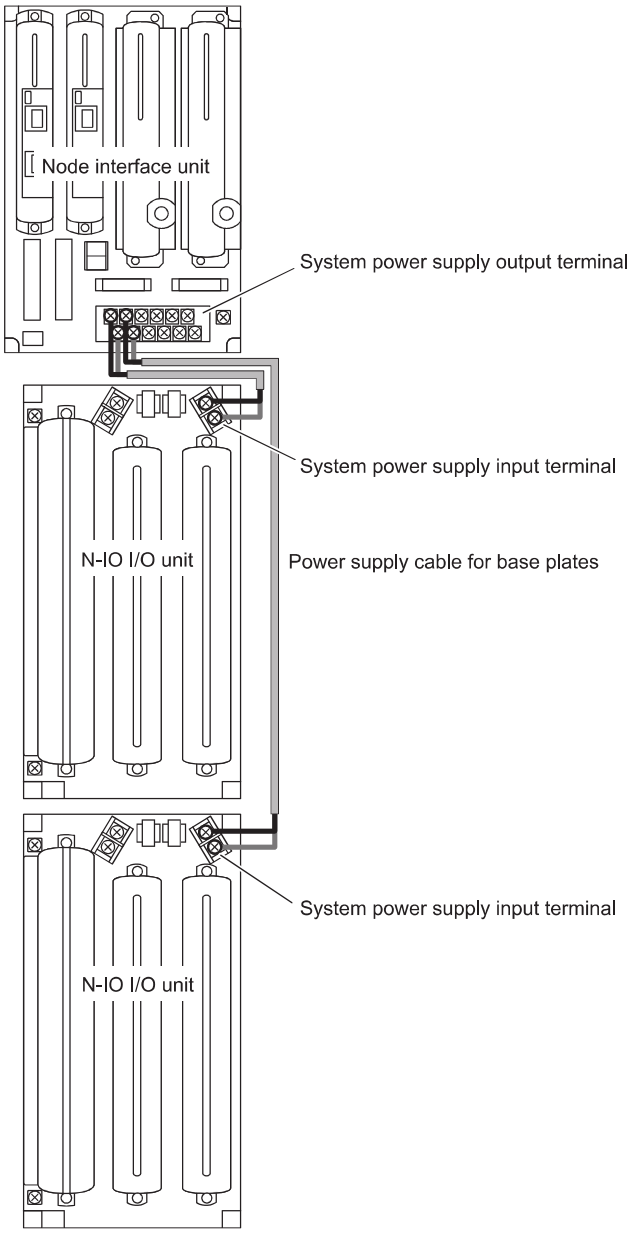


Figure C2.6-2 Example of system power supply wiring

Follow these steps to install system power supply wiring:

1. Remove the cover of the node interface unit.
2. Confirming the cable polarity, connect the node interface unit and the N-IO I/O units by using the power cables for base plates. The screws of the connecting terminals are M4 screws.
3. Attach the cover of the node interface unit.

SEE ALSO For more information about removing and attaching the cover of the node interface unit, refer to:

"● Cover" on page B5-2

Field power supply or barrier power supply wiring

CAUTION

When you connect a field power supply or a barrier power supply, provide a fuse or a circuit breaker in an appropriate location.

You can use the same procedure to install wiring for field power supply and barrier power supply.

The following figure shows an example of the field power supply wiring.

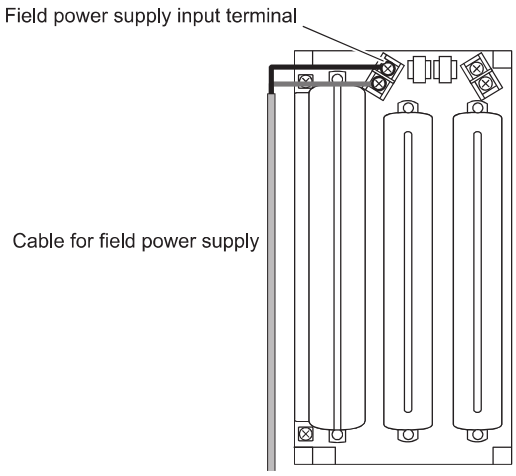


Figure C2.6-3 Example of field power supply wiring

Confirming the cable polarity, connect the power cable to the field power input terminals or barrier power input terminals that are provided on the base plate. The cable polarity is indicated on the base plate. The screw of the terminal is an M4 screw.

SEE ALSO For more information about Cable termination, refer to:

"● Cable termination for signal wiring" on page D1-9

For more information about the specifications of field power supply or barrier power supply cables, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

C3. Bus cable wiring of SCS

This section describes how to wire the following bus cables:

- Cables for Vnet/IP
- ESB bus cables
- Cables for optical ESB bus
- Cables for N-ESB bus
- F-SB bus cables

IMPORTANT

To reduce the mechanical stress on the cables and connectors, fix the cables to the rack in the cabinet or other suitable places.

C3.1 Connecting cables for Vnet/IP

The section explains how to connect the cables for Vnet/IP.

IMPORTANT

When you connect the cables for Vnet/IP to the processor modules of the SCU, note the following:

- For each SCU, connect "Layer 2 switch for Bus 1 to the BUS1 connector of the processor module" and connect "Layer 2 switch for Bus 2 to the BUS2 connector of the processor module."
- Before connecting the cable, remove the processor module from the SCU.

The following figure shows an example where a safety engineering PC (SENG) and an SCU are connected on Vnet/IP.

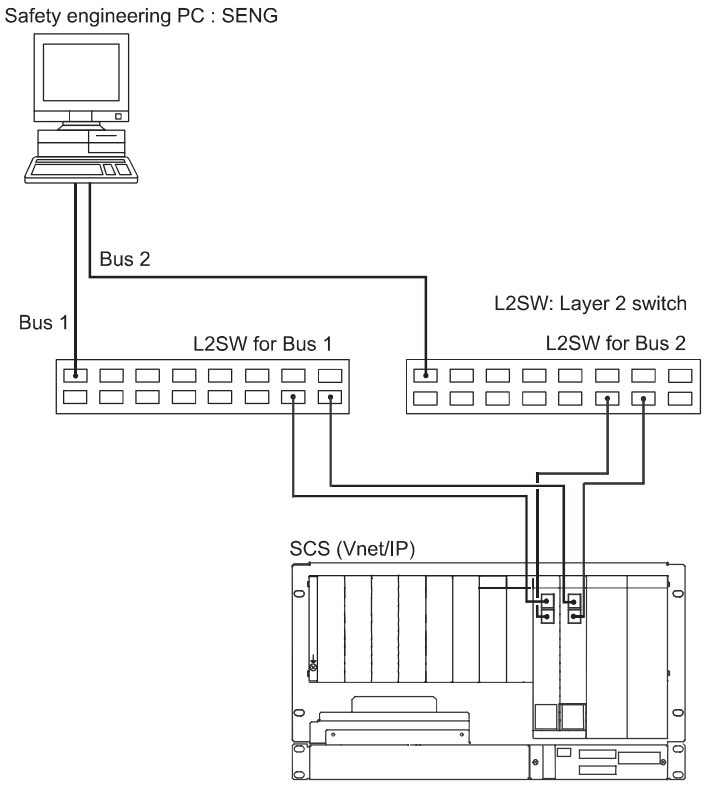


Figure C3.1-1 Example of Vnet/IP cable connection

Follow one of these steps to connect cables for Vnet/IP:

- When turning the power on:
  Connect the cables to the processor module, and then turn on the power.
- When removing the processor module while the system is running:
  Remove the processor module with the cables connected to it.
- When mounting the processor module while the system is running:
  Connect the cables to the processor module, and then mount the module.

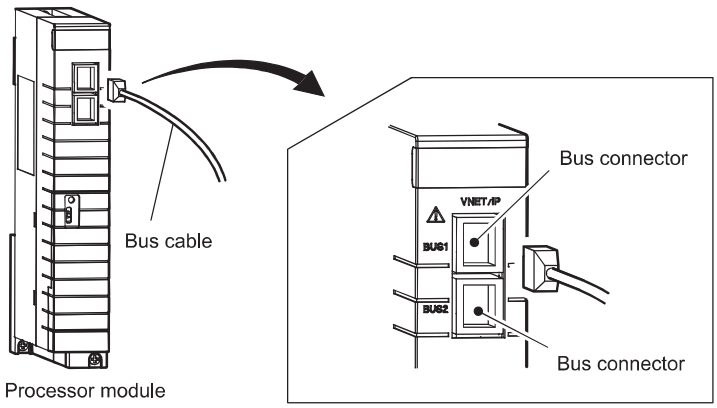
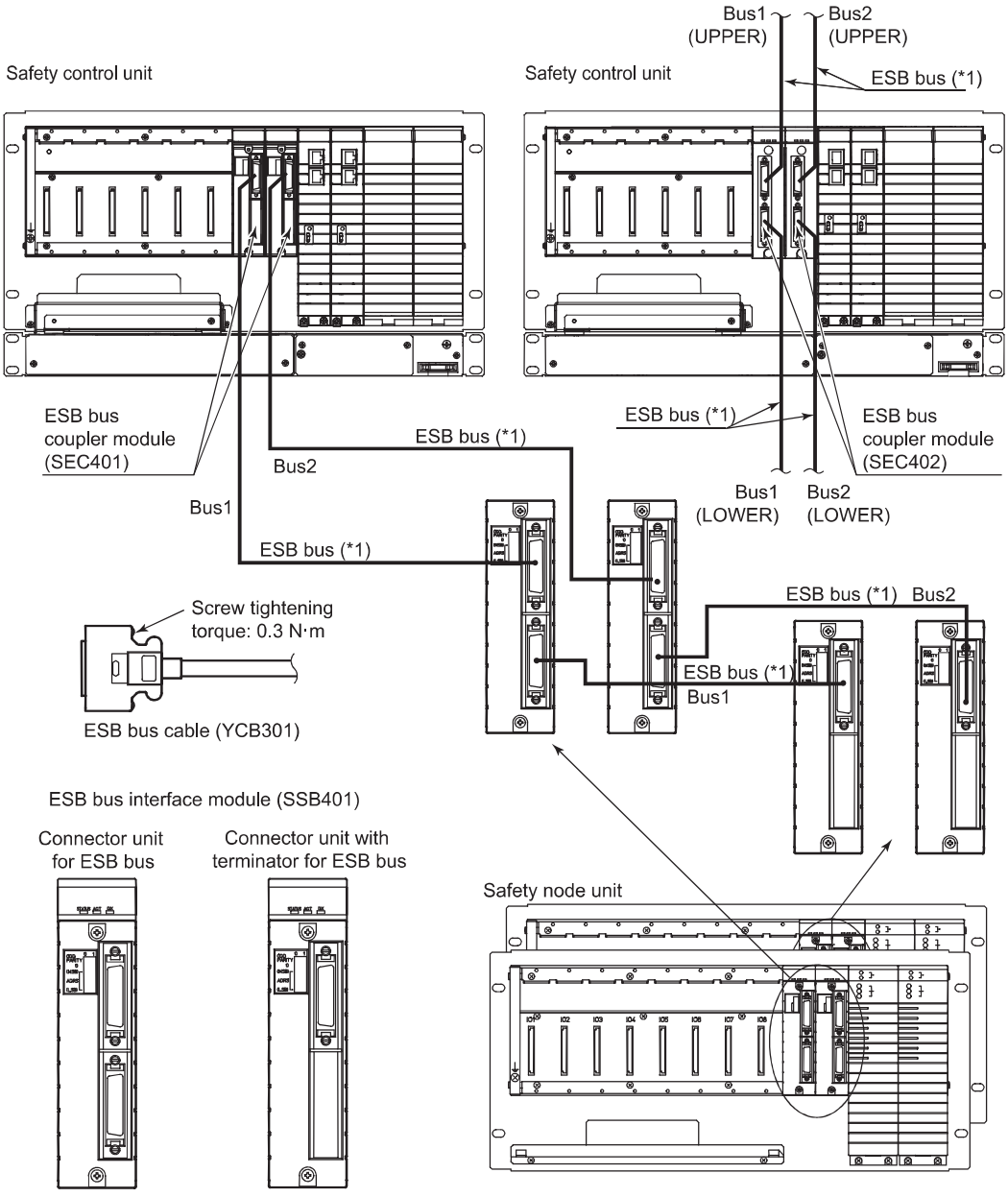


Figure C3.1-2 Connecting cables for Vnet/IP

C3.2 Connecting ESB bus cables

The communication bus that is used to connect the SCU and SNUs is called ESB bus.

ESB bus must be terminated at the module that is connected to each end of the ESB bus. The ESB bus coupler module in the SCU is always at one end of the ESB bus and has a connector unit with terminator for ESB bus. In the SNU at the other end of the ESB bus, install an ESB bus interface module that has a connector unit with terminator for ESB bus. In the SNUs that are not at the end of the ESB bus, install an ESB bus interface module that has a connector unit for ESB bus without a terminator. The following figure shows an example of an ESB bus connection in an SCS that supports SIL 3.



*1: Total transmission distance of ESB bus1 and ESB bus2 is less than 10 m each.

Figure C3.2-1 ESB bus connection in an SCS that supports SIL 3

C3.3 Connecting optical ESB bus cables (FIO node)

The transmission distance can be extended by connecting the SCU, SNUs, and the unit for optical bus repeater module with the optical ESB bus repeater module mounted onto each using optical ESB bus.

Star type and chain type connections are available for optical ESB bus connection.

CAUTION

The optical ESB bus repeater modules are class 1 laser products which comply with the requirements of IEC 60825-1. These modules comply with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007.



Figure C3.3-1 Label of class 1 laser product

SEE ALSO

For more information about the fiber-optic cable transmission distance of the optical ESB bus repeater modules for SCSs that support SIL 3, refer to:

ProSafe-RS Optical ESB Bus Repeater Module (GS 32Q06L15-31E and GS 32Q06L16-31E)

For more information about the fiber-optic cable transmission distance of the optical ESB bus repeater modules for SCSs that support SIL 2, refer to:

ProSafe-RS Lite Optical ESB Bus Repeater Module (GS 32P56L15-01EN and GS 32P56L16-01EN)

Termination of ESB bus on the master and slave sides

On the master side and slave side of the optical ESB bus of the FIO node, ESB bus is connected. ESB bus must be terminated at the module that is connected to each end of the ESB bus. The following modules are used at the ends of ESB bus for termination:

- ESB bus coupler module
  ESB bus coupler modules have built-in terminators. They can be used directly.
- ESB bus interface module
  Available in two types: module with ESB bus terminator and module with ESB bus branch connector. For termination, use the module with ESB bus terminator.
- Optical ESB bus repeater master module
  Available in two types: module with ESB bus terminator and module with ESB bus branch connector. For termination, use the module with ESB bus terminator.
- Optical ESB bus repeater slave module
  This module has a terminator for ESB bus, so you can use it as is.

Star type connection

In star type connection, SNUs and the unit for optical bus repeater module are connected using fiber-optic cables. Both ends of the ESB bus must be terminated. The following figure shows an example of a star type connection in an SCS that supports SIL 3.

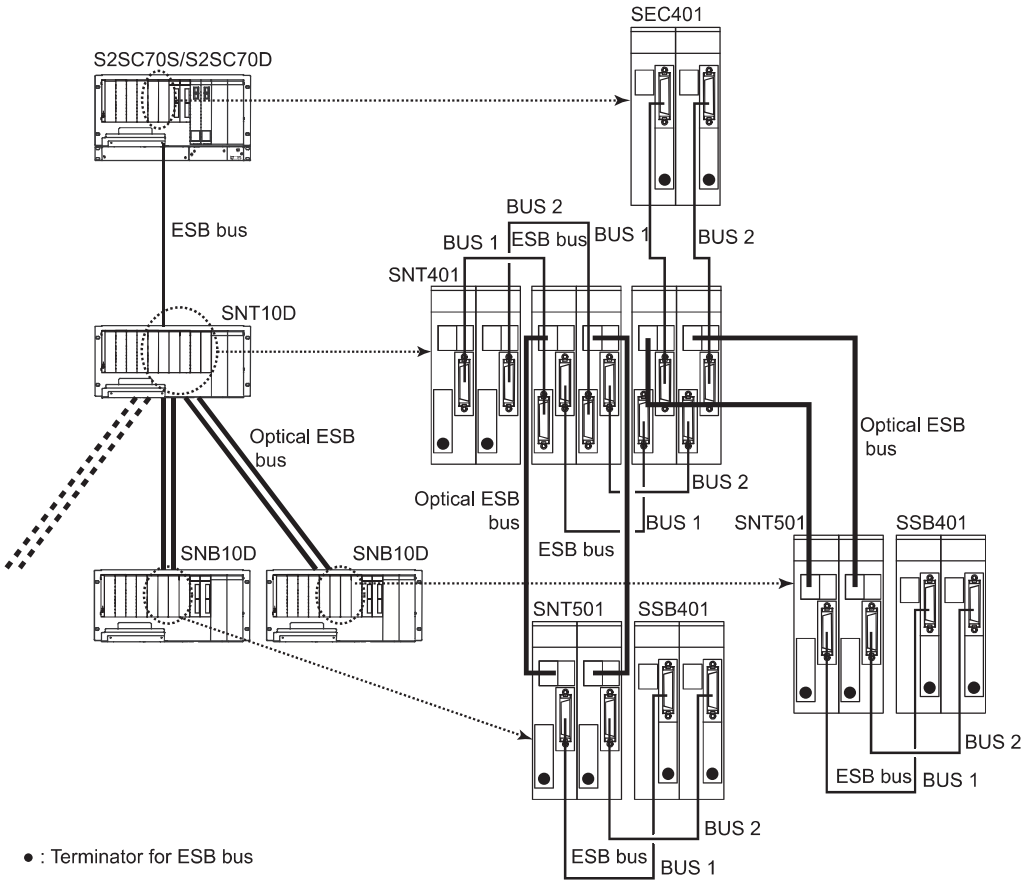


Figure C3.3-2 Star type connection in an SCS that supports SIL 3

At the top level, mount the ESB bus coupler module (SEC401) in the SCU, mount the optical ESB bus repeater master module (SNT401) in the unit for optical bus repeater module (SNT10D), and connect them with the ESB bus. Mount the ESB bus interface module (SSB401) and the optical ESB bus repeater slave module (SNT501) onto the lowest-level safety node unit (SNB10D) and connect with the ESB bus.

For the modules at the end of ESB bus, use a module with ESB bus terminator.

Connect the optical ESB bus repeater modules (SNT401 and SNT501) with fiber-optic cables.

Chain type connection

For the chain type connection, two methods are available: using SCU and SNU and using SCU and unit for optical bus repeater module.

Using SCU and SNU

In this method, the SCU and SNUs mounted with optical ESB bus repeater modules are connected using fiber-optic cables. Both ends of the ESB bus must be terminated at each level. The following figure shows an example of a chain type connection in an SCS that supports SIL 3.

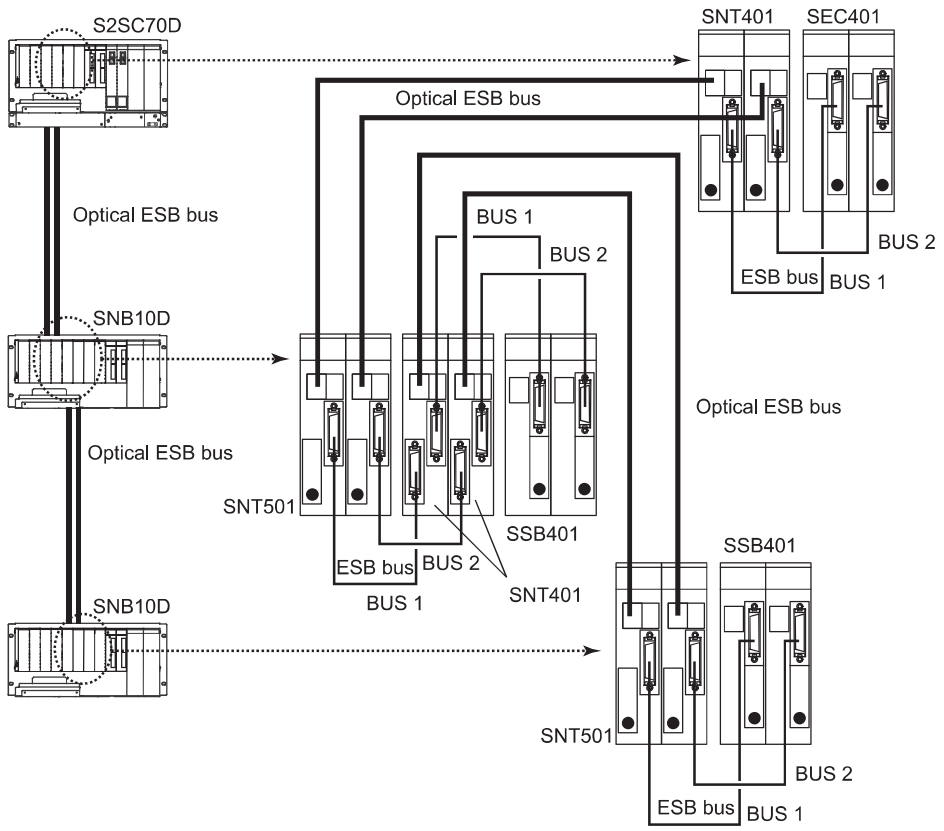


Figure C3.3-3 Chain type connection in an SCS that supports SIL 3: Using SCU and SNU

At the top level, mount the ESB bus coupler module (SEC401) and the optical ESB bus repeater master module (SNT401) in the SCU, and connect them with the ESB bus. At the next level, mount the ESB bus interface module (SSB401), optical ESB bus repeater master module (SNT401), and optical ESB bus repeater slave module (SNT501) in the SNU (SNB10D), and connect the modules with the ESB bus. At the lowest level, mount the ESB bus interface module (SSB401) and optical ESB bus repeater slave module (SNT501) in the SNU (SNB10D), and connect the modules with the ESB bus.

For the modules at the end of ESB bus, use a module with ESB bus terminator.

Connect the optical ESB bus repeater modules (SNT401 and SNT501) with fiber-optic cables.

● Using unit for optical bus repeater module

In this method, the unit for optical bus repeater module loaded with optical ESB bus repeater modules is connected to the SCU and SNU. Both ends of the ESB bus must be terminated at each level. The following figure shows an example of a chain type connection where the units for optical bus repeater module are used in an SCS that supports SIL 3.

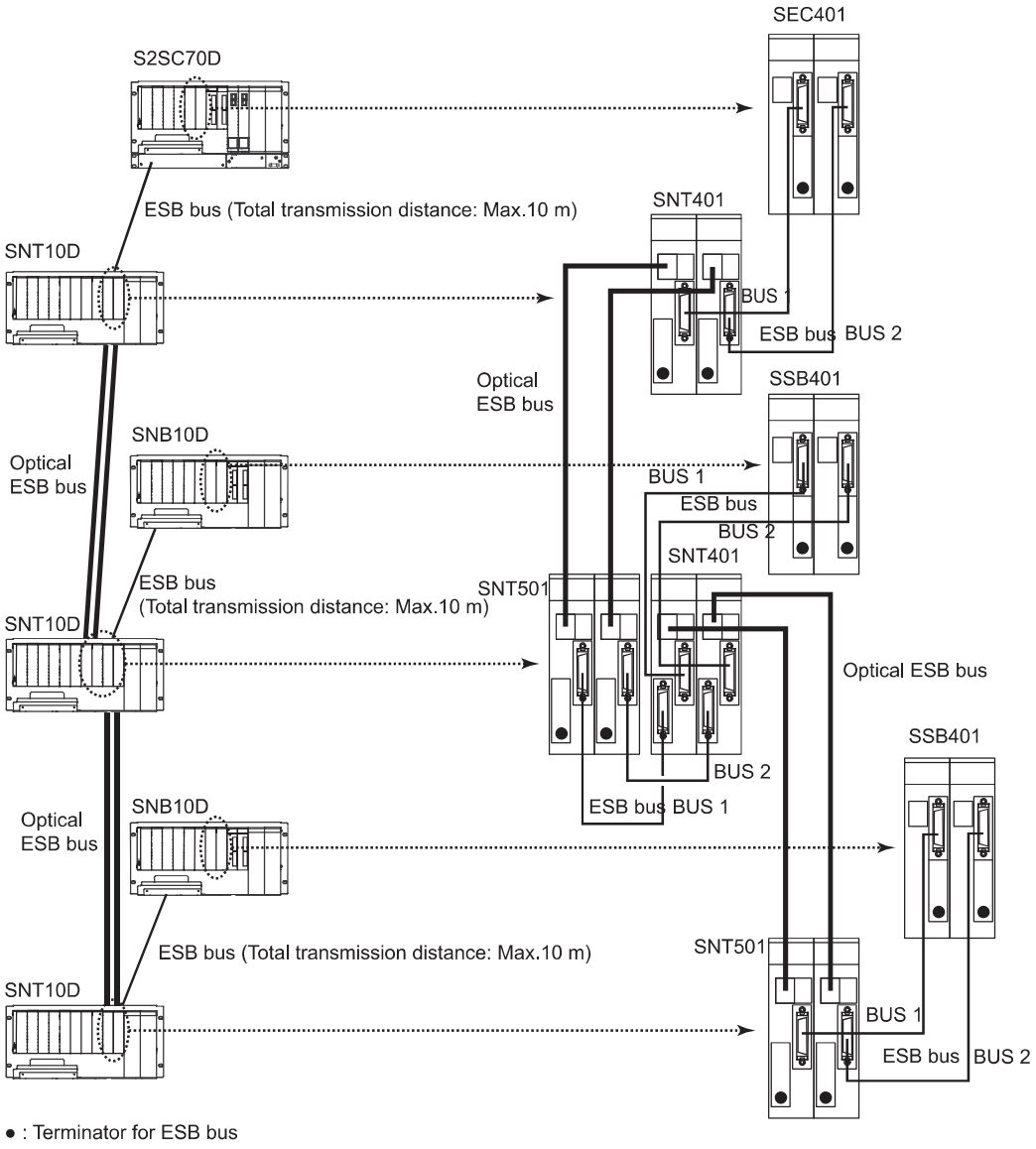


Figure C3.3-4 Chain type connection in an SCS that supports SIL 3: Using unit for optical bus repeater module

At the top level, mount the ESB bus coupler module (SEC401) in the SCU, mount the optical ESB bus repeater master module (SNT401) in the unit for optical bus repeater module (SNT10D), and connect them with the ESB bus. At the next level, mount the ESB bus interface module (SSB401) in the SNU (SNB10D), mount the optical ESB bus repeater master module (SNT401) and the optical ESB bus repeater slave module (SNT501) in the unit for optical bus repeater module (SNT10D), and connect them with the ESB bus. At the lowest level, mount the ESB bus interface module (SSB401) in the SNU (SNB10D), mount the optical ESB bus repeater slave module (SNT501) in the unit for optical bus repeater module (SNT10D), and connect them with the ESB bus.

For the modules at the end of ESB bus, use a module with ESB bus terminator.

Connect the optical ESB bus repeater modules with fiber-optic cables.

The number and location of optical ESB bus repeater modules that can be mounted in each unit

The connectable number of optical ESB bus repeater modules and their location are determined by each unit.

IMPORTANT

Note the following points when using optical ESB bus repeater modules.

- The optical ESB bus repeater master module and the optical ESB bus repeater slave module both connected to ESB bus1 must be mounted on the odd-numbered slots. The Optical ESB bus repeater master module and the optical ESB bus repeater slave module both connected to ESB bus2 must be mounted on the even-numbered slots.
- Be sure to put a dummy cover (SDCV01) on each slot with no module.

SEE ALSO

For more information about restrictions on installation of optical ESB bus repeater modules to SCSs that support SIL 3, refer to:

ProSafe-RS Optical ESB Bus Repeater Module (GS 32Q06L15-31E and GS 32Q06L16-31E)

For more information about restrictions on installation of optical ESB bus repeater modules to SCSs that support SIL 2, refer to:

ProSafe-RS Lite Optical ESB Bus Repeater Module (GS 32P56L15-01EN and GS 32P56L16-01EN)

SCU

The following figure shows the slots of SCU to which optical ESB bus repeater modules can be mounted.

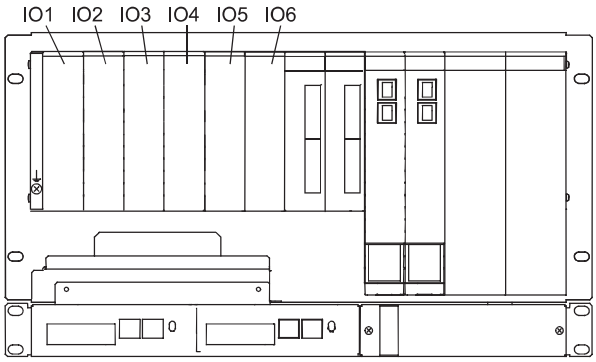


Figure C3.3-5 Slots of SCU to which optical ESB bus repeater modules can be mounted

You can mount the modules to slots IO1 to IO6. Use an odd-number slot and the next even-number slot together.

SNU

The following figure shows the slots of SNU to which optical ESB bus repeater modules can be mounted.

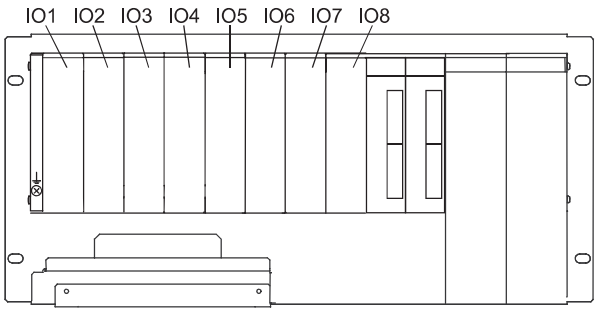


Figure C3.3-6 Slots of SNU to which optical ESB bus repeater modules can be mounted

You can mount the modules to slots IO1 to IO8. Use an odd-number slot and the next even-number slot together.

Unit for optical bus repeater module

The following figure shows the slots of the unit for optical bus repeater module to which optical ESB bus repeater modules can be mounted.

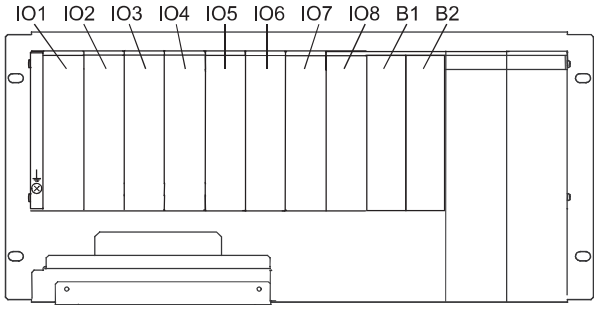


Figure C3.3-7 Slots of the unit for optical bus repeater module to which optical ESB bus repeater modules can be mounted

You can mount the modules to slots IO1 to IO8, B1, and B2. Use an odd-number slot and the next even-number slot together.

C3.4 Connecting N-ESB bus cables

This section describes the N-ESB bus cable connection between the SCU and an N-IO node and between N-IO nodes.

IMPORTANT

You must set the node number of the N-IO node first before you connect the bus cables.

SEE ALSO

For more information about the models of N-ESB bus module that can be connected to N-ESB bus, refer to:

"■ Elements on the N-ESB bus module" on page B5-6

For more information about setting the node number of an N-IO node, refer to:

F2.1.1, "Using the Node Number Setting Tool" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Connecting N-ESB bus cables between SCU and N-IO node

The following figure shows an example of N-ESB bus cable connection between the SCU and an N-IO node.

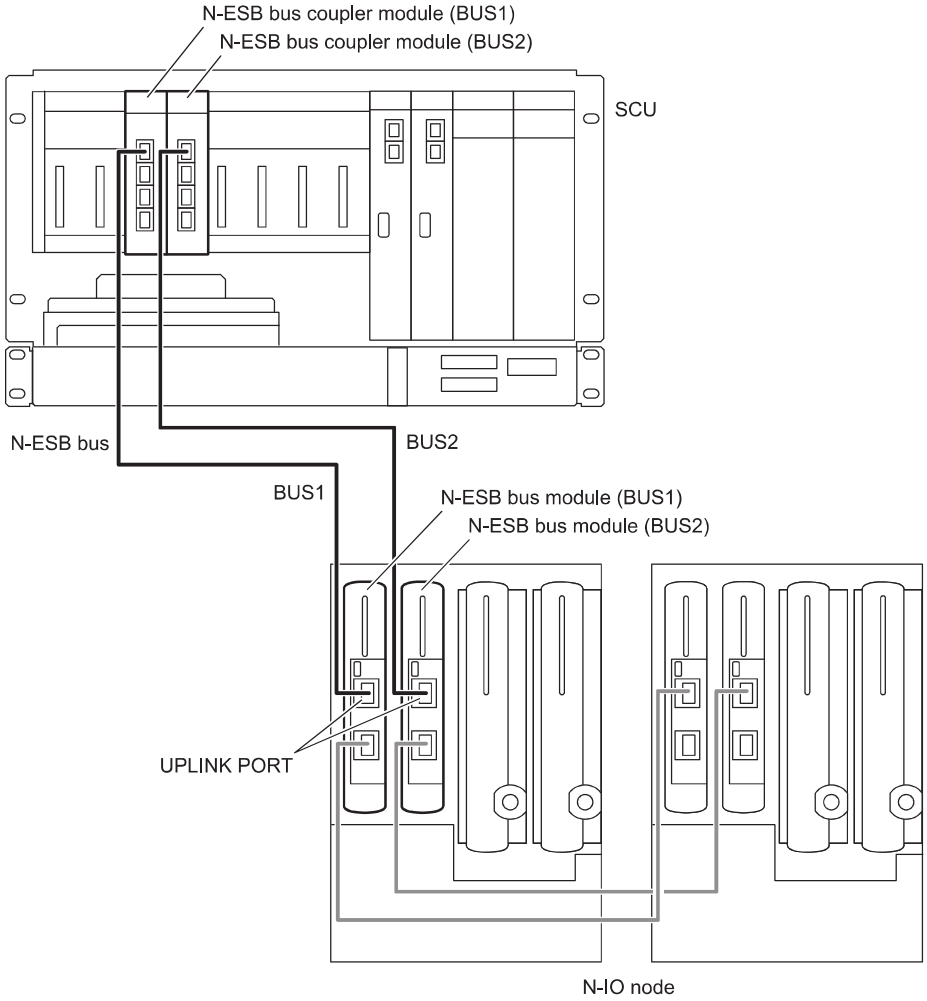


Figure C3.4-1 Example of N-ESB bus cable connection between SCU and N-IO node

Using N-ESB bus cables, connect the N-ESB bus coupler module (BUS1) and the N-ESB bus module (BUS1) and connect the N-ESB bus coupler module (BUS2) and the N-ESB bus module (BUS2).

The N-ESB bus cables must be installed so that they run over the base plate for node interface unit. Ensure that stress is not applied to the N-ESB bus cables and connectors.

SEE ALSO For more information about the specifications of N-ESB bus cables, refer to:

ProSafe-RS Safety Instrumented System Overview (for Vnet/IP) (GS 32P01B10-01EN)

Connecting N-ESB bus cables between N-IO nodes

The following figure shows an example of N-ESB bus cable connection between N-IO nodes.

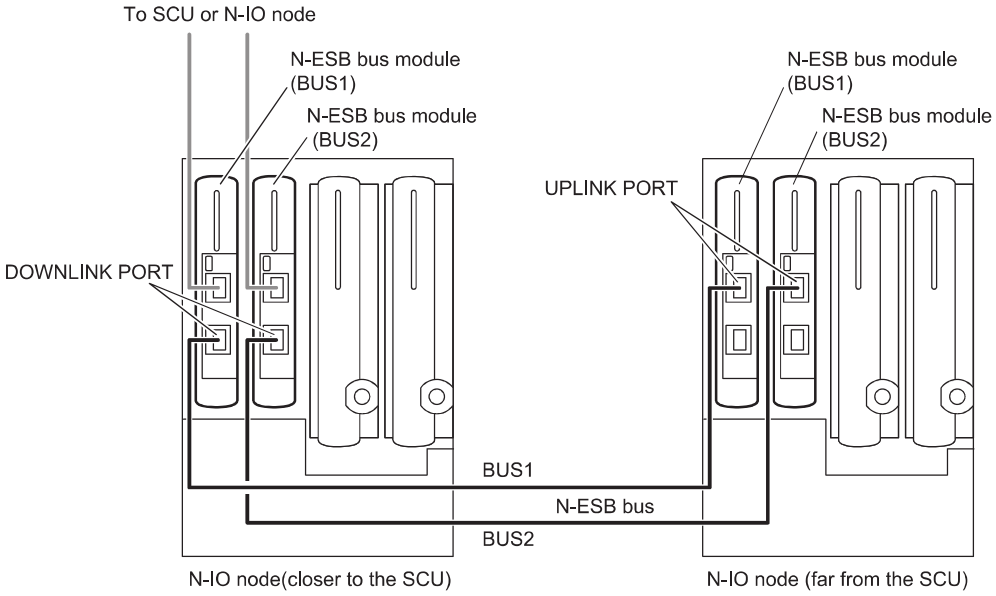


Figure C3.4-2 Example of N-ESB bus cable connection between N-IO nodes

Using N-ESB bus cables, connect between N-ESB bus modules (BUS1) and between N-ESB bus modules (BUS2) of neighboring N-IO nodes. Connect the DOWNLINK PORT of the N-IO node that is closer to the SCU to the UPLINK PORT of the N-IO node that is far from the SCU.

The N-ESB bus cables must be installed so that they run over the base plate for node interface unit. Ensure that stress is not applied to the N-ESB bus cables and connectors.

SEE ALSO For more information about the specifications of N-ESB bus cables, refer to:

ProSafe-RS Safety Instrumented System Overview (for Vnet/IP) (GS 32P01B10-01EN)

C3.5 Connecting optical ESB bus cables (N-IO node)

This section describes the following optical ESB bus cable connections:

- Connection between an N-IO node and an FIO node (including SCU) that is connected on the UPLINK port (SCU side)
- Connection between an N-IO node and an FIO node that is connected on the DOWN-LINK port (the side opposite SCU)
- Connection between N-IO nodes

CAUTION

The optical ESB bus repeater modules and N-ESB bus modules are class 1 laser products which comply with the requirements of IEC 60825-1. These modules comply with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007.



Figure C3.5-1 Label of class 1 laser product

IMPORTANT

You must set the node number of the N-IO node first before you connect the bus cables.

SEE ALSO For more information about the models of N-ESB bus module that can be connected to N-ESB bus, refer to:

"■ Elements on the N-ESB bus module" on page B5-6

For more information about setting the node number of an N-IO node, refer to:

F2.1.1, "Using the Node Number Setting Tool" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Connecting optical ESB bus cables between an N-IO node and an FIO node that is connected on the UPLINK port

When connecting an N-IO node and an FIO node (including the SCU) that is connected on the UPLINK port (SCU side), connect the optical ESB bus repeater master module in the FIO node to the N-ESB bus module in the N-IO node. The following figure shows an example when connecting the SCU.

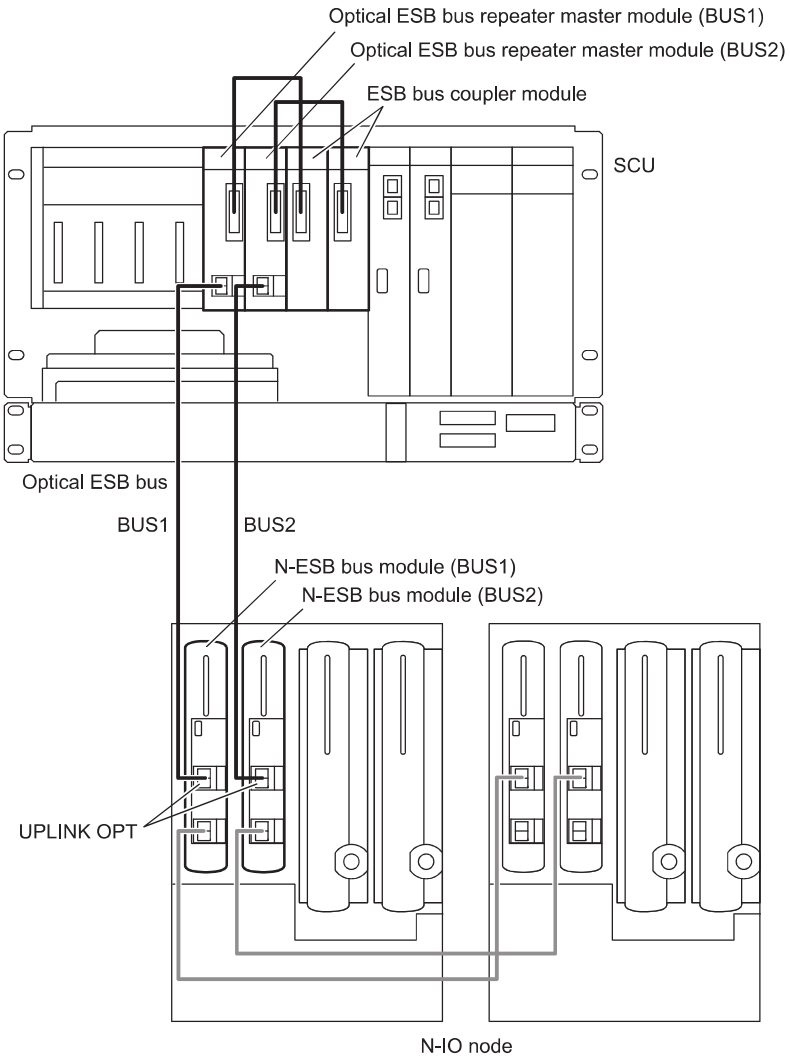


Figure C3.5-2 Example of optical ESB bus cable connection between SCU and N-IO node

Using fiber-optic cables, connect the optical ESB bus repeater master module (BUS1) and the N-ESB bus module (BUS1), and connect the optical ESB bus repeater master module (BUS2) and the N-ESB bus module (BUS2).

The fiber-optic cables must be installed so that they run over the base plate for node interface unit. Ensure that stress is not applied to the fiber-optic cables and connectors.

SEE ALSO For more information about the specifications of fiber-optic cables, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

For more information about the connectable combinations of the N-ESB bus module and optical ESB bus repeater modules, refer to:

ProSafe-RS Optical ESB Bus Repeater Module (GS 32Q06L15-31E and GS 32Q06L16-31E)

Connecting optical ESB bus cables between an N-IO node and an FIO node that is connected on the DOWNLINK port

When connecting an N-IO node and an FIO node that is connected on the DOWNLINK port (the side opposite SCU), connect the N-ESB bus module in the N-IO node to the optical ESB

bus repeater slave module in the FIO node. The following figure shows an example of connection between an N-IO node and SNU.

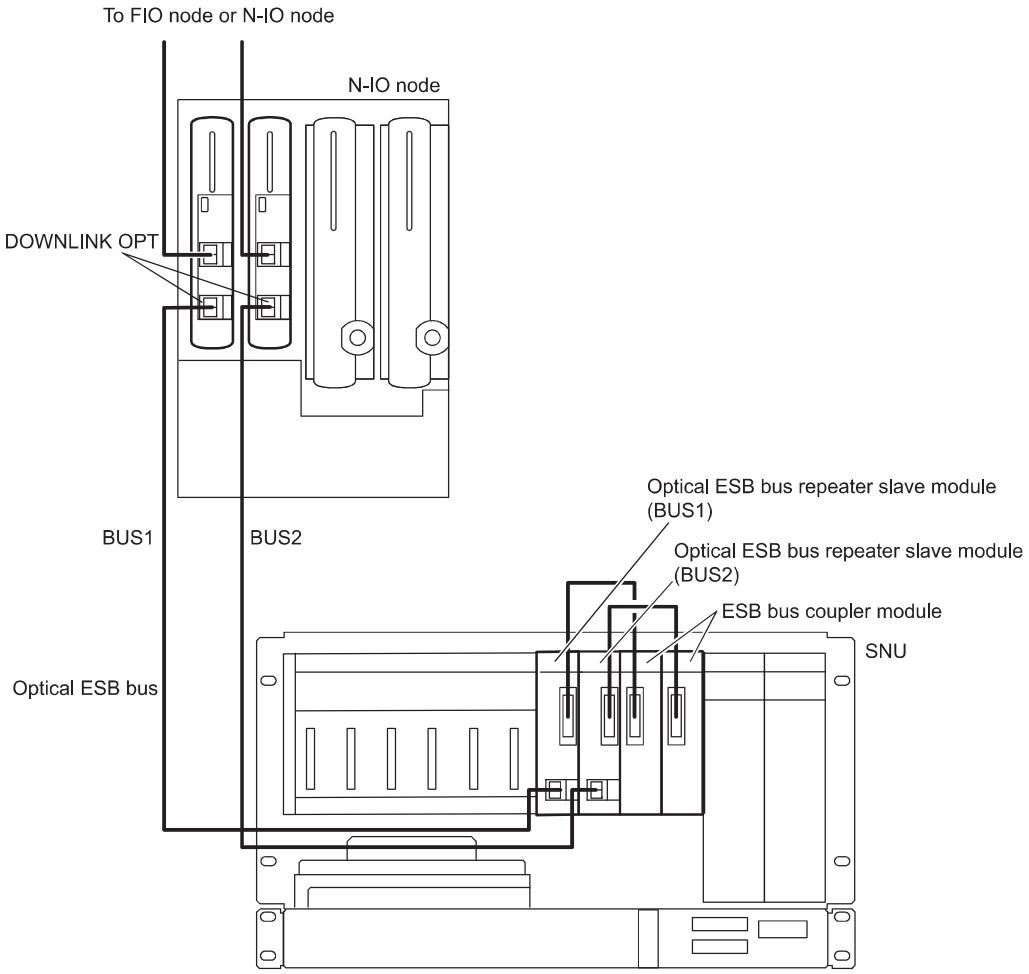


Figure C3.5-3 Example of optical ESB bus cable connection between N-IO node and SNU

Using fiber-optic cables, connect the N-ESB bus module (BUS1) and the optical ESB bus repeater slave module (BUS1), and connect the N-ESB bus module (BUS2) and the optical ESB bus repeater slave module (BUS2).

The fiber-optic cables must be installed so that they run over the base plate for node interface unit. Ensure that stress is not applied to the fiber-optic cables and connectors.

SEE ALSO For more information about the specifications of fiber-optic cables, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

For more information about the connectable combinations of the N-ESB bus module and optical ESB bus repeater modules, refer to:

ProSafe-RS Optical ESB Bus Repeater Module (GS 32Q06L15-31E and GS 32Q06L16-31E)

Connecting optical ESB bus cables between N-IO nodes

The following figure shows an example of optical ESB bus cable connection between N-IO nodes.

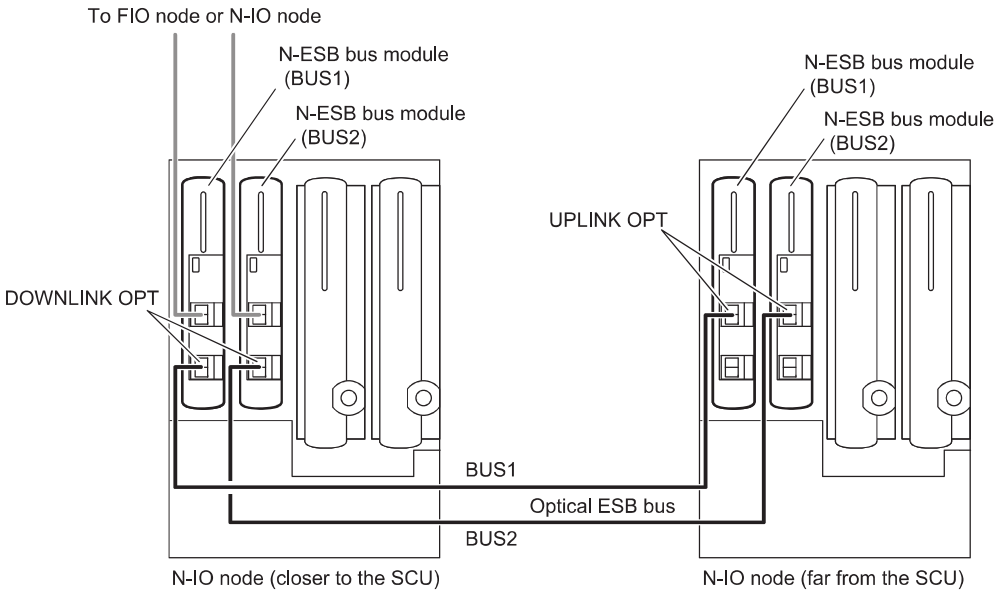


Figure C3.5-4 Example of optical ESB bus cable connection between N-IO nodes

Using fiber-optic cables, connect between N-ESB bus modules (BUS1) and between N-ESB bus modules (BUS2) of neighboring N-IO nodes. Connect the DOWNLINK OPT of the N-IO node that is closer to the SCU to the UPLINK OPT of the N-IO node that is farther from the SCU.

The fiber-optic cables must be installed so that they run over the base plate for node interface unit. Ensure that stress is not applied to the fiber-optic cables and connectors.

SEE ALSO For more information about the specifications of fiber-optic cables, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

C3.6 Connecting F-SB bus cables

IMPORTANT

- When you connect the F-SB bus cable to N-IO I/O units, match the unit number of the N-IO I/O unit and the unit number that is indicated on the cable.
- When you tighten the connector fixing screws of the F-SB bus cable, use a flat-blade screwdriver that conforms to the DIN 5264B standard having a thickness at the tip of 0.4 mm and a body shaft diameter of 2.5 mm.

The following figure shows an example of connection between the node interface unit and N-IO I/O units.

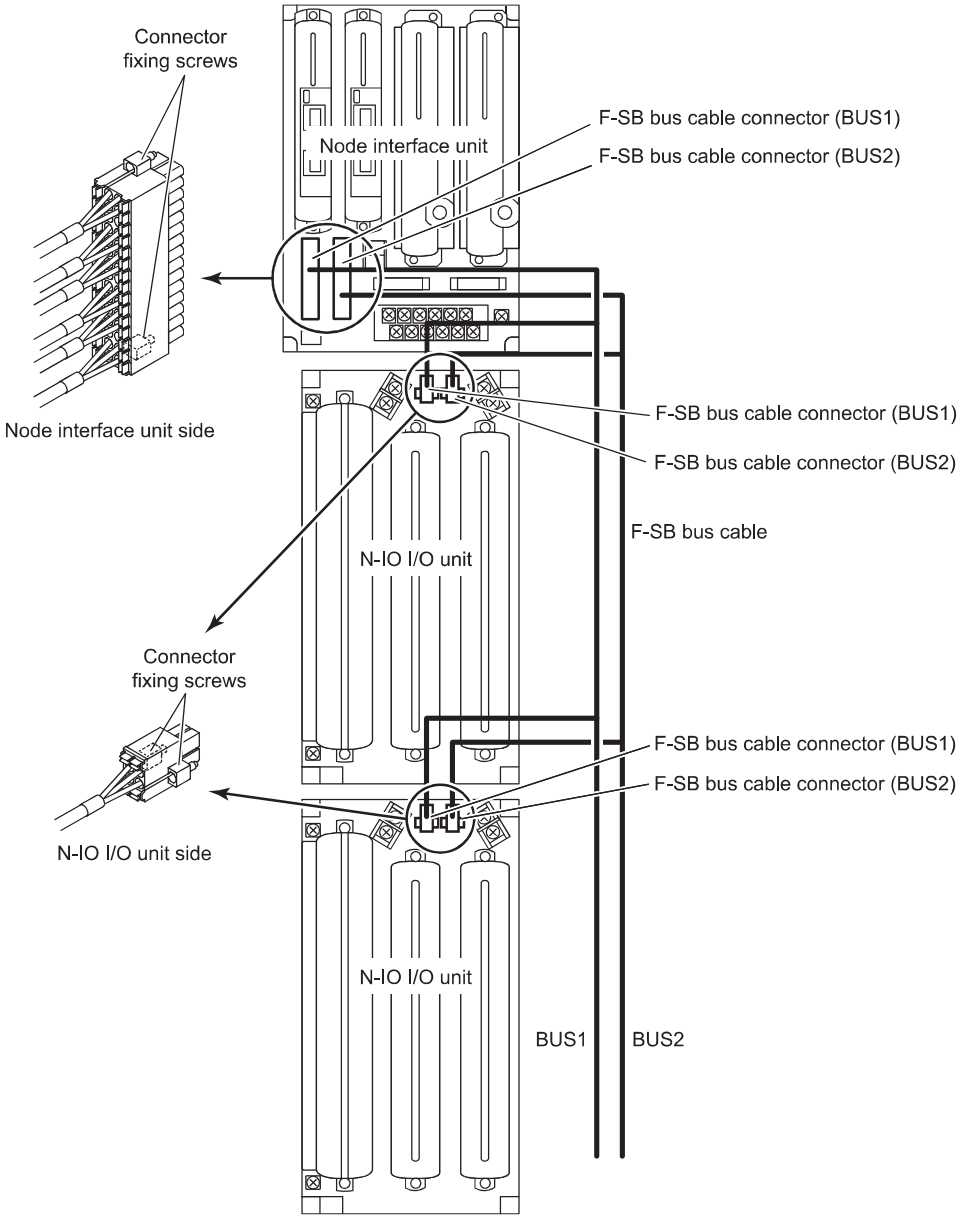


Figure C3.6-1 Example of connection between the node interface unit and N-IO I/O units

Follow these steps to connect the node interface unit and N-IO I/O units by using F-SB bus cables (Model: S2KLF10):

1. Remove the cover of the node interface unit.
2. Using F-SB bus cables, connect the F-SB bus connector (BUS1) of the base plate for node interface unit and the F-SB bus connector (BUS1) of each base plate for N-IO I/O, and do the same for BUS2.
3. Tighten the fixing screws of the connectors.

IMPORTANT

The tightening torque of the screws should be 0.2 to 0.3 N·m.

4. Attach the cover of the node interface unit.

SEE ALSO

For more information about removing and attaching the cover of the node interface unit, refer to:

"● Cover" on page B5-2

For more information about the F-SB bus cable and N-IO I/O unit numbers, refer to:

"■ F-SB bus cable" on page B5-21

D. Signal wiring between SCS and field devices

This section describes the signal wiring between I/O modules and the field devices. I/O modules include FIO I/O modules and N-IO I/O modules.

IMPORTANT

To reduce the mechanical stress on the cables and connectors, fix the cables to the rack in the cabinet or other suitable places.

D1. Signal wiring between FIO I/O modules and field devices

This section describes the signal wiring between FIO I/O modules and the field devices. The following types of FIO I/O modules are available:

- Analog I/O module
- Digital I/O module
- Communication module

D1.1 Types of FIO I/O module signal connection

Signal cables of field devices can be connected to FIO I/O modules in the following ways, depending on whether the wiring space needs to be reduced, whether the instrumentation style needs to be unified, or other circumstances:

- Connection by using pressure clamp terminals
  Signal cables of the field device are directly connected to the pressure clamp terminal block of the I/O module.
- Connection by using MIL connectors
  The connector of field device signal cable is directly connected to the MIL connector of the I/O module.
- Connection through a terminal board
  Signal cables of the field devices are connected to a terminal board, and the terminal board is connected to the I/O module with signal cable interface adapter by using a dedicated signal cable.
- Connection through a relay board
  The output signals from a digital output module are received by a relay board and transmitted to the field devices as contact output signals.

The following figure shows the signal cable connection by pressure clamp terminal block, MIL connector, and terminal board.

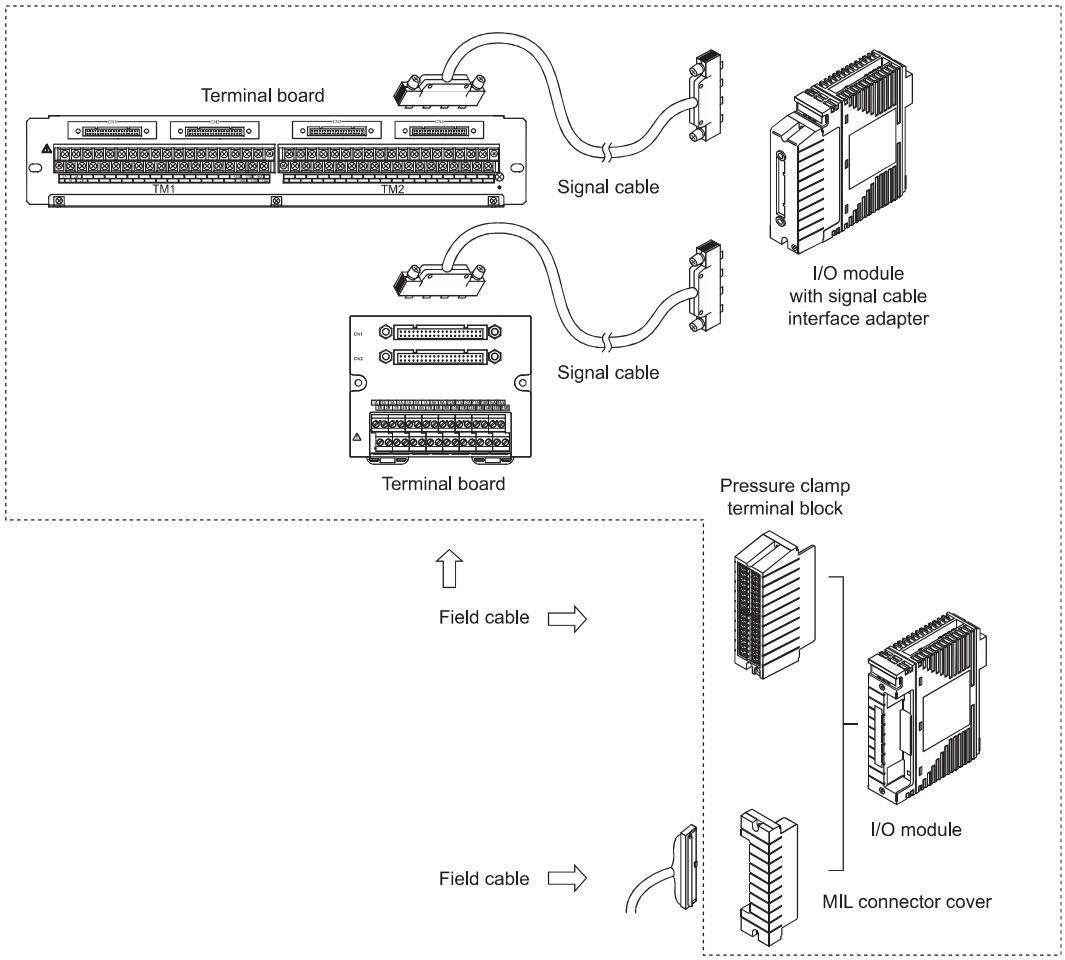


Figure D1.1-1 Examples of connection through a terminal board, pressure clamp terminal block, and MIL connector

The following figure shows the signal cable connection through a relay board.

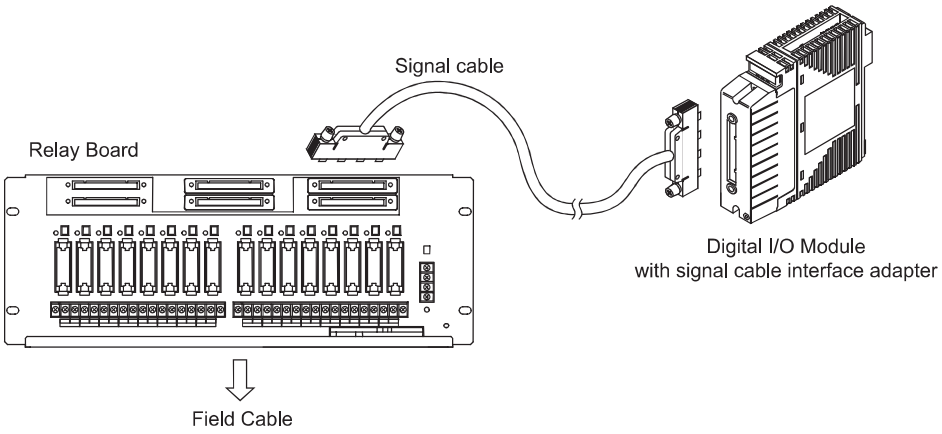


Figure D1.1-2 Example of connection through a relay board

SEE ALSO

For more information about the combinations of I/O modules for SCSs that support SIL 3 and terminal blocks, etc., refer to:

ProSafe-RS Outline of I/O Modules (for FIO) (GS 32P06K60-01EN)

For more information about the combinations of I/O modules for SCSs that support SIL 2 and terminal blocks, etc., refer to:

ProSafe-RS Lite Outline of I/O Modules (GS 32P56K60-01EN)

D1.1.1 Signal connections to the pressure clamp terminal block

This section describes the signal connections to the pressure clamp terminal block.

Cables for signal wiring

For signal wiring to pressure clamp terminal blocks, you can use the following nominal cross sectional area cables.

- With sleeve: 0.5 to 1.5 mm^2 (AWG20-16)
- Without sleeve: 0.5 to 2 mm^2 (AWG20-14)

SEE ALSO For more information about examples of compatible cable lines for signal wiring, refer to:

- ProSafe-RS Installation Guidance (TI 32P01J10-01EN)
- ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

Cable termination

IMPORTANT

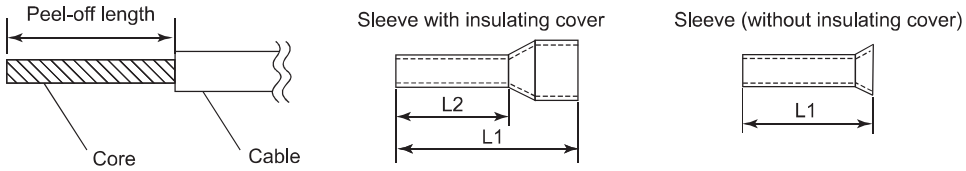
- Use sleeves that conform to the following DIN standards.
  - Sleeves without insulating cover: DIN 46 228/1
  - Sleeves with insulating cover: DIN 46 228/4
- Use sleeves and a tool that are of the same make and match the thickness of the wire.
- Insert the cables deep into the terminals and make sure they are securely installed.

On the cables for pressure clamp terminals, you must perform the following terminations:

- When using a sleeve
  At the cable end, peel off the coating and attach a sleeve. The following table shows the sleeve dimensions.

Table D1.1.1-1 Sleeve dimension

Cable thickness (mm^2)	When using a sleeve with insulating cover			When using a sleeve (without insulating cover)	
	Peel-off length (mm)	Sleeve dimension (mm)		Peel-off length (mm)	Sleeve dimension (mm)
		L1	L2		L1
0.5	12	16	10	10	10
0.75	12	16	10	10	10
1.0	12	16	10	10	10
1.25 to 1.5	12	16	10	10	10



- When not using a sleeve
  The peel-off length should be 11 mm.

Signal connections to the pressure clamp terminal block

Insert the cables deep into the pressure clamp terminals and tighten the screws.

IMPORTANT

- When you connect cables to pressure clamp terminals, use a flat-blade screwdriver that conforms to the DIN 5264B standard having a thickness at the tip of 0.6 mm and a body shaft diameter of 3.5 mm.
- The tightening torque of the screws should be approximately 0.5 N·m.
- Fasten the cables securely to cable clamps, etc., so that the cables do not weigh on the terminals.

D1.1.2 Signal connections to the MIL connectors

For MIL connectors, connect the MIL cables directly to the I/O modules.

To prevent the MIL cable from being disconnected, a cable connector cover is required separately.

The types of connector covers for MIL cables are as follows:

- SCCC01/L1CCC01: For flat ribbon cables
- SCCC02/L1CCC02: For discrete wire cables (DI, DO cables)

The following figure shows how to install the connector cover.

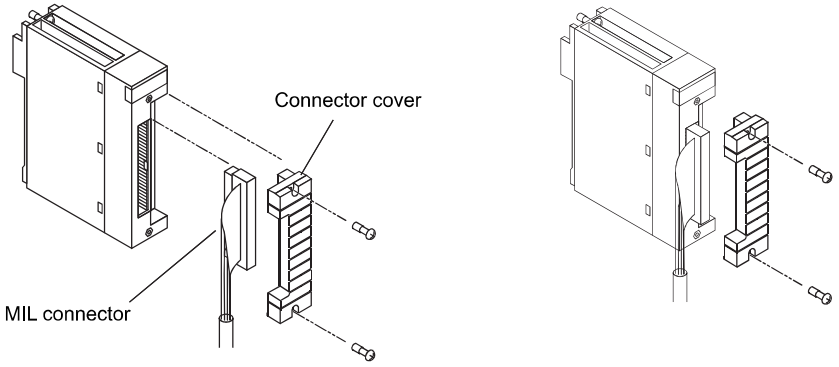


Figure D1.1.2-1 MIL cable connection

When the MIL cable has a shield lead wire, this wire needs to be fastened to the screw at the lower part of the MIL cable connector cover.

The following figure shows how to connect the shield wire.

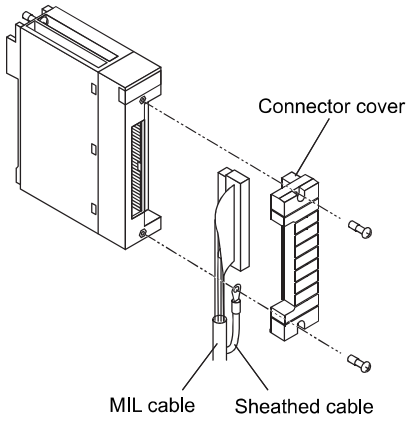


Figure D1.1.2-2 Connecting the shield lead wires of the MIL cable

D1.1.3 Signal connections to the terminal board/relay board

This section describes the signal connections through a terminal board or relay board. The signal cables of the field devices are connected to the terminal board or relay board. The terminal board or relay board and an I/O module with a signal cable interface adapter are connected by using a dedicated signal cable.

Connecting an I/O module with a terminal board/relay board

The following figure shows the components of the I/O modules with a signal cable interface adapter. In the signal cable that is dedicated to connecting the I/O modules with the terminal board/relay board, there is a pin (as a option) to prevent incorrect insertion. You can connect the signal cable shield wire to the ground terminal on the front part of the I/O module. Then you can connect the connector on the opposite side of the signal cable to the terminal board/relay board.

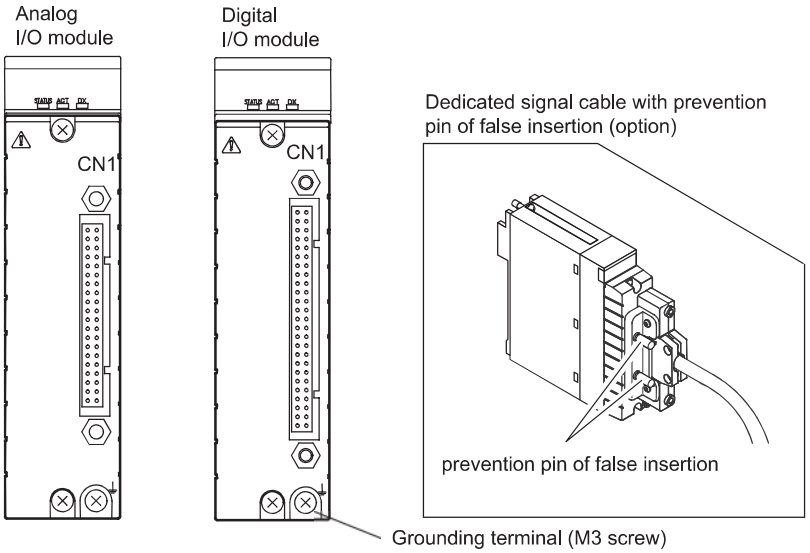


Figure D1.1.3-1 Input/Output modules connected via signal cable interface adapters

Types of signal cables for I/O modules

The following figure shows the shapes of the signal cables that are dedicated for connecting I/O modules to the terminal board or relay board.

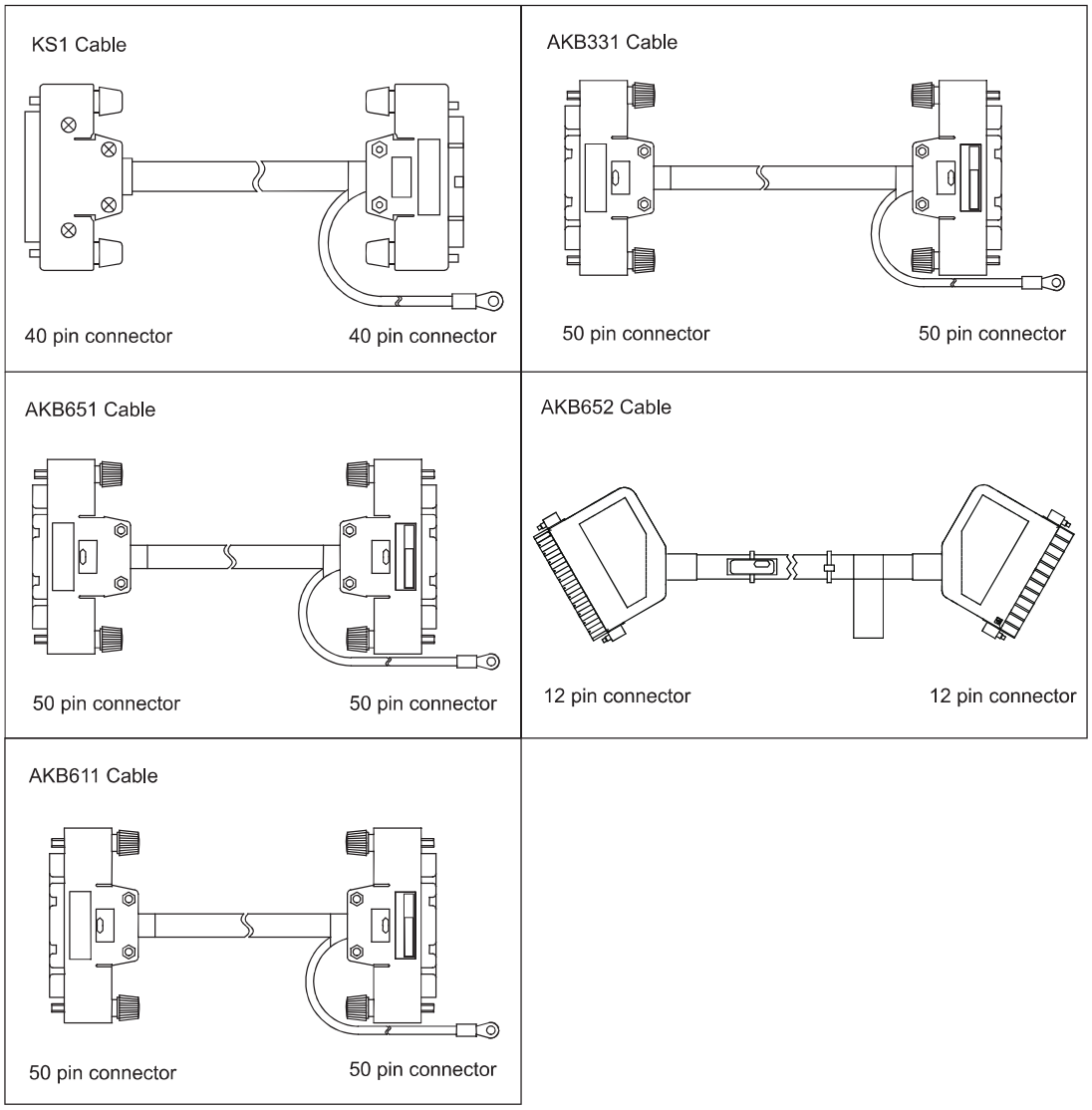


Figure D1.1.3-2 Type of signal cable

Signal connections to a rack mountable terminal board/relay board

You can connect the signal cable of the field devices to the field wiring terminals of the terminal board/relay board by fastening it with an M4 screw.

IMPORTANT

- On unused connectors, put the provided connector caps for dust prevention and connector pin protection.
- Connect the signal wires ensuring that the insulation covers of adjacent ring terminals do not overlap.

SEE ALSO For more information about examples of compatible cable lines for signal wiring, refer to:

- ProSafe-RS Installation Guidance (TI 32P01J10-01EN)
- ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

Cable termination for signal wiring

Use ring terminals with insulating sleeve at the ends of the wires. The ring terminals and crimping tool should be from the same vendor.

The following figure shows the dimensions of the ring terminal.

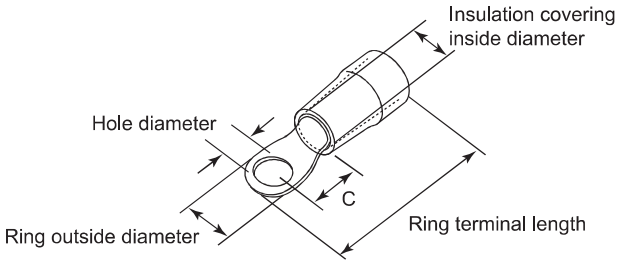


Figure D1.1.3-3 Ring terminal

Table D1.1.3-1 Ring terminal dimensions

Nominal cross sectional area (mm^2)	Screw (mm)	Hole diameter (mm)	Ring outside diameter (mm)	Ring terminal length (mm)	Insulation covering inside diameter (mm)	Dimension "C" (mm)	Remarks
1.25(*1)	4	4.3 or more	8.2 or less	About 21	3.6 or more	7.0 or more	
2.0(*2)	4	4.3 or more	8.7 or less	About 21	4.3 or more	7.1 or more	
5.5(*3)	4	4.3 or more	8.7 or less	About 25	5.8 or more	5.9 or more	Only SED2D

*1: This type of ring terminals are mainly applied for the cables in the range of 0.25 to 1.65 mm^2. It is necessary to check the specifications from the vender to select the appropriate terminals.

*2: This type of ring terminals are mainly applied for the cables in the range of 1.0 to 2.6 mm^2. It is necessary to check the specifications from the vender to select the appropriate terminals.

*3: This type of ring terminals are mainly applied for the cables in the range of 2.6 to 6.6 mm^2. It is necessary to check the specifications from the vender to select the appropriate terminals.

Signal connections to a DIN rail mountable terminal board/relay board

Connect the signal cables from the field devices to the pressure clamp terminals for field wiring on the terminal/relay board.

IMPORTANT

On unused connectors, put the provided connector caps for dust prevention and connector pin protection.

Cables for signal wiring

For signal wiring to the pressure clamp terminal, you can use the following nominal cross sectional area cables:

- 0.5 to 2.5 mm^2 (AWG 20 to 14)

SEE ALSO For more information about examples of compatible cable lines for signal wiring, refer to:

- ProSafe-RS Installation Guidance (TI 32P01J10-01EN)
- ProSafe-RS Lite Installation Guidance (TI 32P51J10-01EN)

For more information about the signal wiring cables for SBT4D, refer to:

"■ Cables for signal wiring" on page D1-4

Cable termination for signal wiring

IMPORTANT

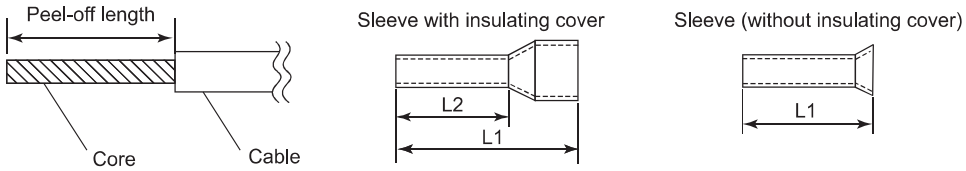
- Use sleeves that conform to the following DIN standards.
  - Sleeves without insulating cover: DIN 46 228/1
  - Sleeves with insulating cover: DIN 46 228/4
- Use sleeves and a tool that are of the same make and match the thickness of the wire.
- Insert the cables deep into the terminals and make sure they are securely installed.

On the cables for pressure clamp terminals, you must perform the following terminations:

- When using a sleeve
  At the cable end, peel off the coating and attach a sleeve. The following table shows the sleeve dimensions.

Table D1.1.3-2 Sleeve dimensions

Cable thickness (mm^2)	When using a sleeve with insulating cover			When using a sleeve (without insulating cover)	
	Peel-off length (mm)	Sleeve dimension (mm)		Peel-off length (mm)	Sleeve dimension (mm)
		L1	L2		L1
0.5	10	14	8	6	6
0.75	10	14	8	6	6
1.0	10	14	8	6	6
1.5	10	14	8	7	7
2.5	10	14	8	7	7



- When not using a sleeve
  The peel-off length should be 7 mm.

SEE ALSO For more information about Cable termination for the SBT4D signal wiring, refer to:

"■ Cable termination" on page D1-4

Connecting cables for signal wiring

Insert the cables deep into the pressure clamp terminals and tighten the screws.

IMPORTANT

- The tightening torque of the screws should be 0.5 to 0.6 N·m.
- When you connect cables to pressure clamp terminals, use a flat-blade screwdriver that conforms to the DIN 5264B standard having a thickness at the tip of 0.6 mm and a body shaft diameter of 3.5 mm.
- Fasten the cables securely to cable clamps, etc., so that the cables do not weigh on the terminals.

D1.2 Signal cable connection to analog Input/ Output modules

This section describes the signal connections of analog I/O modules.

The following table shows how to connect an analog I/O module to a field device.

Table D1.2-1 Connecting an analog I/O module with a field device

Analog input/output module (type)	Method of connection with field devices (*1)		
	Pressure clamp terminal	Terminal board	MIL cable
SAI143/L1AI143	Yes	Yes	Yes
SAV144/L1AV144	Yes	Yes	Yes
SAT145/L1AT145	-	Yes	-
SAR145/L1AR145	-	Yes	-
SAI533/L1AI533	Yes	Yes	Yes

*1: Yes: Connection possible

SEE ALSO

For more information about the field connection diagram for SCSs that support SIL 3, refer to:

ProSafe-RS Field Device Connection (for FIO) (GS 32Q06J10-31E)

For more information about the field connection diagram for SCSs that support SIL 2, refer to:

ProSafe-RS Lite Field Device Connection (GS 32P56J10-01EN)

D1.2.1 Terminal numbers and signal names of pressure clamp terminal blocks and the MIL connector of analog I/O modules

This section describes terminal numbers and signal names of pressure clamp terminal blocks and the MIL connector of analog I/O modules.

The following figure shows the terminal number layout of a pressure clamp terminal block.

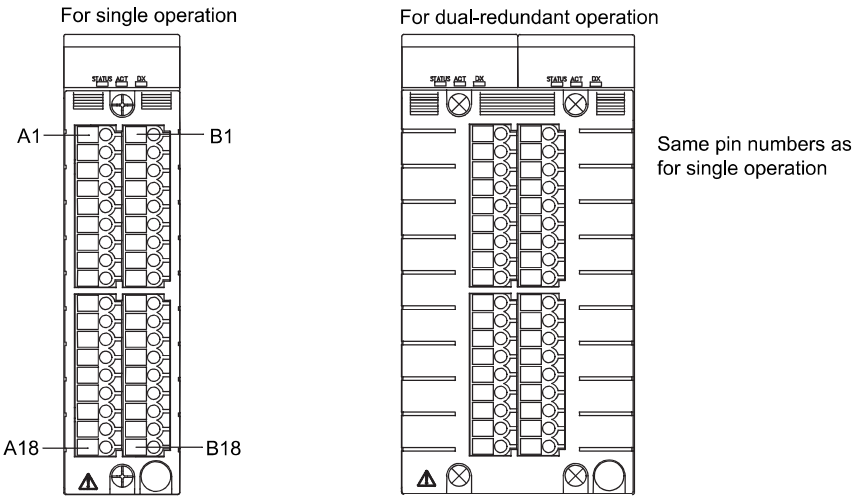


Figure D1.2.1-1 Terminal number layout of a pressure clamp terminal block

The terminal numbers of a pressure clamp terminal block are arranged in the order from A1, A2 and so on until A18 starting from the top of the left column and from B1, B2 and so on until B18 from the top of the right column with the terminal block on the front. The terminal number layout of a dual-redundant type pressure clamp terminal is the same.

The following figure shows the layout of the terminal numbers of the MIL connector.

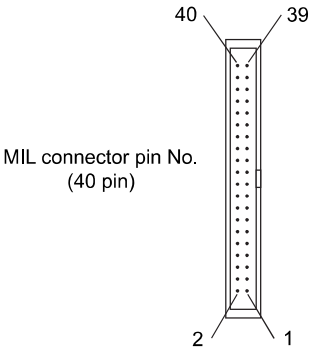


Figure D1.2.1-2 Terminal number layout of the MIL connector

Input terminal numbers and signal names of SAI143/L1AI143

The following figure shows the terminal numbers of the pressure clamp terminal block of SAI143/L1AI143, and the pin numbers and signal names of the MIL connector.

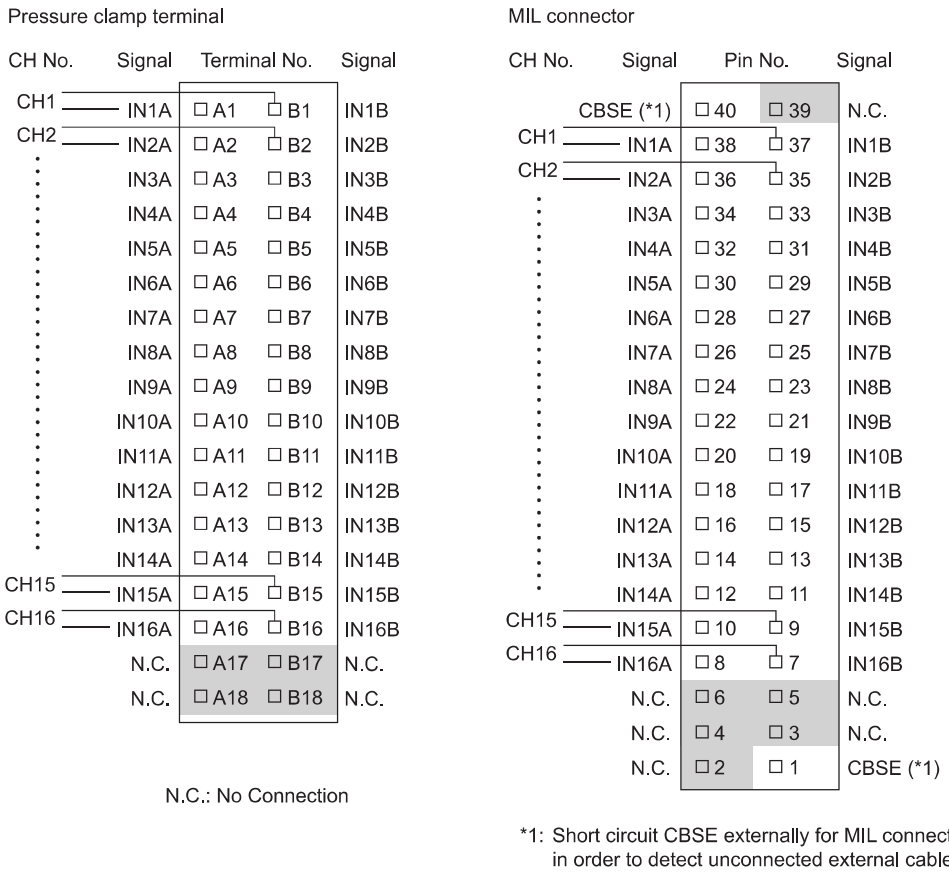


Figure D1.2.1-3 SAI143/L1AI143 signal connection

The following table shows the type of signals that are connected to SAI143/L1AI143 and their corresponding setting pins.

Table D1.2.1-1 Type of signals that are connected to SAI143/L1AI143 and their corresponding setting pins

Type of field devices	Signal name (*1)	Signal types	SAI143/L1AI143 setting pins
2-wire type	IN□A	2-wire transmitter input +	2-wire type
	IN□B	2-wire transmitter input –	
4-wire type	IN□A	4-wire current input –	4-wire type
	IN□B	4-wire current input +	
3-wire type	IN□A	3-wire current input – / external power supply –	
	IN□B	3-wire current input +	

*1: □: 1 to 16

Signal cable connections of SAI143/L1AI143

The following figure shows the signal cable connections of SAI143/L1AI143.

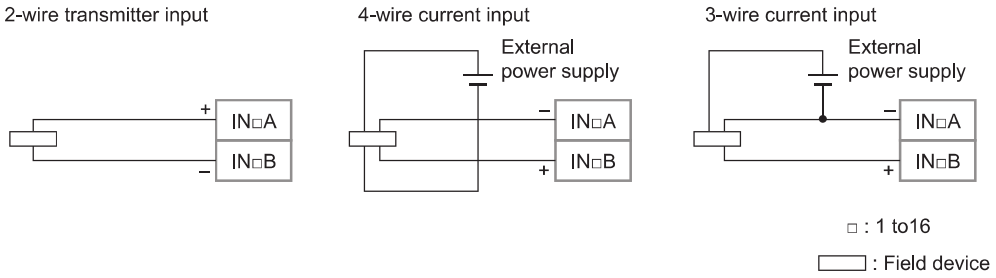


Figure D1.2.1-4 SAI143/L1AI143 signal connection

You must purchase the external power supply separately.

If the power is turned off or an error occurs in SAI143/L1AI143, the current input loop becomes open. Do not share the current signal with any other signal-receiving instrument.

SEE ALSO For more information about the setting pins of SAI143/L1AI143, refer to:

"■ Setting pins of the current input module" on page B4-23

■ Input terminal numbers and signal names of SAV144/L1AV144

The following figure shows the terminal numbers of the pressure clamp terminal block of SAV144/L1AV144, and the pin numbers and signal names of the MIL connector.

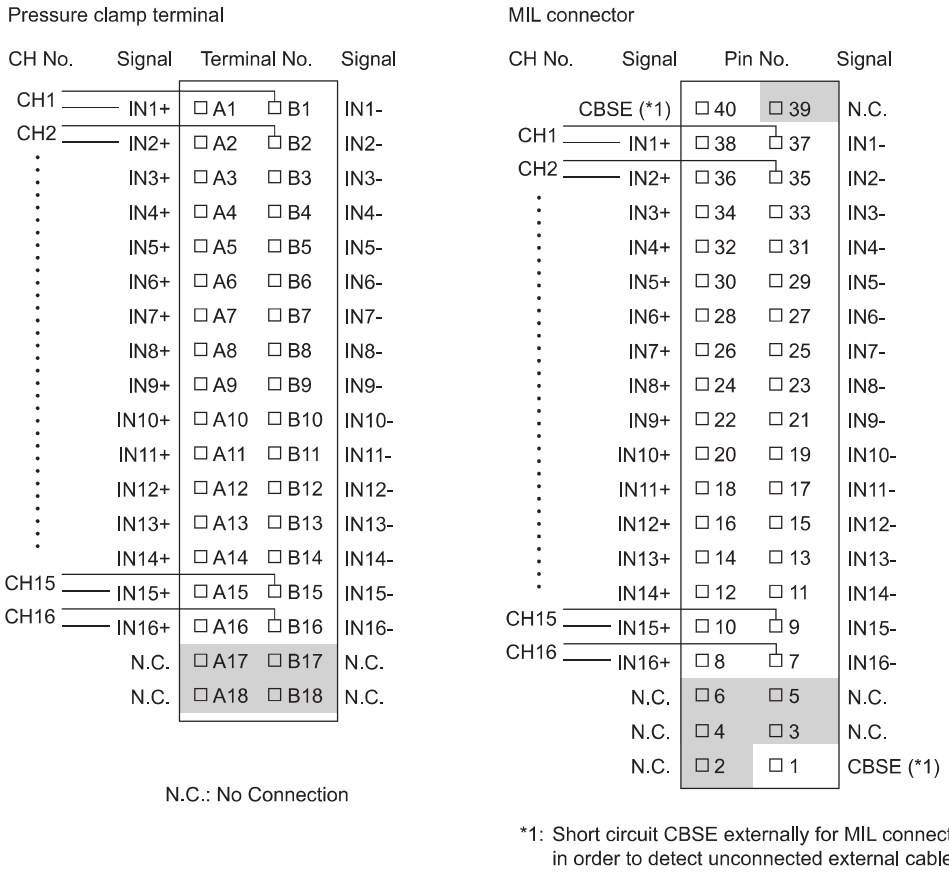


Figure D1.2.1-5 SAV144/L1AV144 signal connection

Output terminal numbers and signal names of SAI533/L1AI533

The following figure shows the terminal numbers of the pressure clamp terminal block of SAI533/L1AI533, and the pin numbers and signal names of the MIL connector.

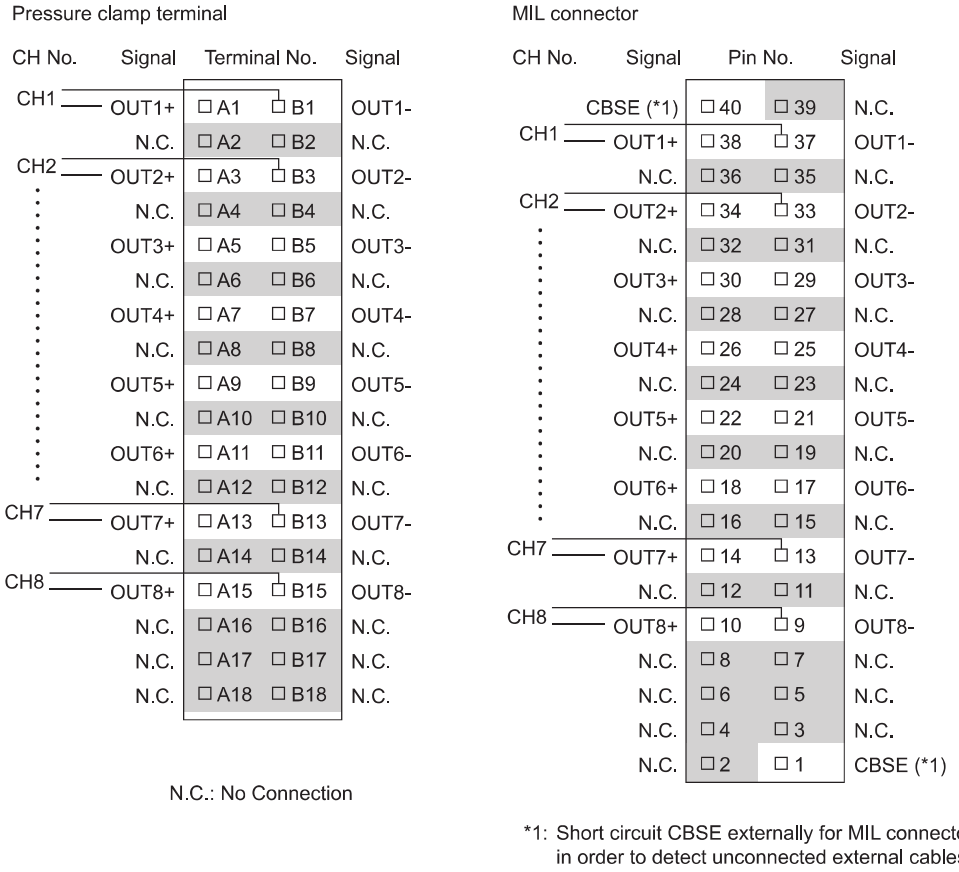


Figure D1.2.1-6 SAI533/L1AI533 signal connection

D1.2.2 Terminal numbers and signal names of the terminal board for analog I/O modules

This section describes the terminal numbers and signal names of terminal boards for analog I/O modules. The following table shows the modules that you can connect to the terminal board.

Table D1.2.2-1 Relationship between terminal boards and analog I/O modules

Terminal board	Connectable analog I/O module	
	For SCSs that support SIL 3	For SCSs that support SIL 2
SEA4D	SAI143, SAV144, SAI533	L1AI143, L1AV144, L1AI533
SBA4D	SAI143, SAV144, SAI533	L1AI143, L1AV144, L1AI533
SBT4D	SAT145	L1AT145
SBR4D	SAR145	L1AR145
S1BB4D	SAI143	L1AI143

Signal cable connections of the SEA4D

SEA4D has two sets of 16 channels of field wiring terminals. I/O modules in non-redundant or dual-redundant configuration can be connected. For a non-redundant configuration, you can connect CN1 or CN3 to a module through a signal cable. For a dual-redundant configuration, you can connect CN1 and CN2 or CN3 and CN4 to a module through a signal cable.

The following figure shows the connectors for signal cables and field wiring terminals of SEA4D.

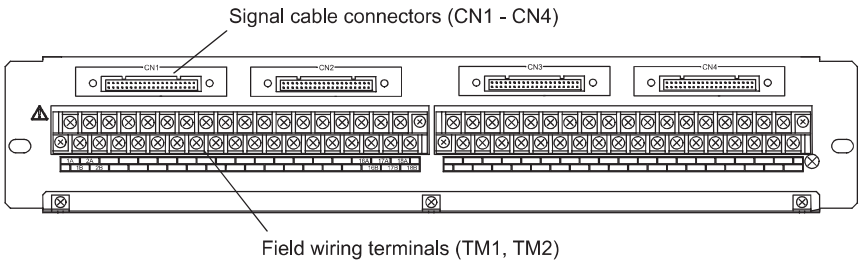


Figure D1.2.2-1 SEA4D terminal board

Terminal numbers and signal names when connecting SAI143/L1AI143

The following figure shows the terminal numbers and signal names of the terminal board when connecting SAI143/L1AI143.

Signal Name	IN1A	IN2A	IN3A	IN4A	IN5A	IN6A	IN7A	IN8A	IN9A	IN10A	IN11A	IN12A	IN13A	IN14A	IN15A	IN16A	N.C.	N.C.
TM1, TM2 Terminal No.	1A	2A	3A	4A	5A	6A	7A	8A	9A	10A	11A	12A	13A	14A	15A	16A	17A	18A
	1B	2B	3B	4B	5B	6B	7B	8B	9B	10B	11B	12B	13B	14B	15B	16B	17B	18B
Signal Name	IN1B	IN2B	IN3B	IN4B	IN5B	IN6B	IN7B	IN8B	IN9B	IN10B	IN11B	IN12B	IN13B	IN14B	IN15B	IN16B	N.C.	N.C.

N.C. : No Connection

Figure D1.2.2-2 Terminal numbers and signal names when connecting SAI143/L1AI143

Terminal numbers and signal names when connecting SAV144/L1AV144

The following figure shows the terminal numbers and signal names of the terminal board when connecting SAV144/L1AV144.

Signal Name	IN1+	IN2+	IN3+	IN4+	IN5+	IN6+	IN7+	IN8+	IN9+	IN10+	IN11+	IN12+	IN13+	IN14+	IN15+	IN16+	N.C.	N.C.
TM1, TM2	1A	2A	3A	4A	5A	6A	7A	8A	9A	10A	11A	12A	13A	14A	15A	16A	17A	18A
Terminal No.	1B	2B	3B	4B	5B	6B	7B	8B	9B	10B	11B	12B	13B	14B	15B	16B	17B	18B
Signal Name	IN1-	IN2-	IN3-	IN4-	IN5-	IN6-	IN7-	IN8-	IN9-	IN10-	IN11-	IN12-	IN13-	IN14-	IN15-	IN16-	N.C.	N.C.

N.C. : No Connection

Figure D1.2.2-3 Terminal numbers and signal names when connecting SAV144/L1AV144

Terminal numbers and signal names when connecting SAI533/L1AI533

The following figure shows the terminal numbers and signal names of the terminal board when connecting SAI533/L1AI533.

Signal Name	OUT1+	N.C.	OUT2+	N.C.	OUT3+	N.C.	OUT4+	N.C.	OUT5+	N.C.	OUT6+	N.C.	OUT7+	N.C.	OUT8+	N.C.	N.C.	N.C.
TM1, TM2	1A	2A	3A	4A	5A	6A	7A	8A	9A	10A	11A	12A	13A	14A	15A	16A	17A	18A
Terminal No.	1B	2B	3B	4B	5B	6B	7B	8B	9B	10B	11B	12B	13B	14B	15B	16B	17B	18B
Signal Name	OUT1-	N.C.	OUT2-	N.C.	OUT3-	N.C.	OUT4-	N.C.	OUT5-	N.C.	OUT6-	N.C.	OUT7-	N.C.	OUT8-	N.C.	N.C.	N.C.

N.C. : No Connection

Figure D1.2.2-4 Terminal numbers and signal names when connecting SAI533/L1AI533

Signal cable connection of the SBA4D

SBA4D has two sets of 16 channels of field wiring terminals. I/O modules in non-redundant or dual-redundant configuration can be connected. For a non-redundant configuration, you can connect CN1 to a module through a signal cable. For a dual-redundant configuration, you can connect CN1 and CN2 to a module through a signal cable.

The following figure shows the connectors for signal cables and field wiring terminals of SBA4D.

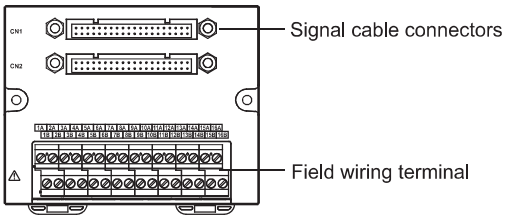


Figure D1.2.2-5 SBA4D terminal board

Terminal numbers and signal names when connecting SAI143/L1AI143

The following figure shows the terminal numbers and signal names of the terminal board when connecting SAI143/L1AI143.

Signal Name	IN1A	IN2A	IN3A	IN4A	IN5A	IN6A	IN7A	IN8A	IN9A	IN10A	IN11A	IN12A	IN13A	IN14A	IN15A	IN16A
Terminal No.	1A	2A	3A	4A	5A	6A	7A	8A	9A	10A	11A	12A	13A	14A	15A	16A
	1B	2B	3B	4B	5B	6B	7B	8B	9B	10B	11B	12B	13B	14B	15B	16B
Signal Name	IN1B	IN2B	IN3B	IN4B	IN5B	IN6B	IN7B	IN8B	IN9B	IN10B	IN11B	IN12B	IN13B	IN14B	IN15B	IN16B

Figure D1.2.2-6 Terminal numbers and signal names when connecting SAI143/L1AI143

Terminal numbers and signal names when connecting SAV144/L1AV144

The following figure shows the terminal numbers and signal names of the terminal board when connecting SAV144/L1AV144.

Signal Name	IN1+	IN2+	IN3+	IN4+	IN5+	IN6+	IN7+	IN8+	IN9+	IN10+	IN11+	IN12+	IN13+	IN14+	IN15+	IN16+
Terminal No.	1A	2A	3A	4A	5A	6A	7A	8A	9A	10A	11A	12A	13A	14A	15A	16A
	1B	2B	3B	4B	5B	6B	7B	8B	9B	10B	11B	12B	13B	14B	15B	16B
Signal Name	IN1-	IN2-	IN3-	IN4-	IN5-	IN6-	IN7-	IN8-	IN9-	IN10-	IN11-	IN12-	IN13-	IN14-	IN15-	IN16-

Figure D1.2.2-7 Terminal numbers and signal names when connecting SAV144/L1AV144

● Terminal numbers and signal names when connecting SAI533/L1AI533

The following figure shows the terminal numbers and signal names of the terminal board when connecting SAI533/L1AI533.

Signal Name	OUT1+	N.C.	OUT2+	N.C.	OUT3+	N.C.	OUT4+	N.C.	OUT5+	N.C.	OUT6+	N.C.	OUT7+	N.C.	OUT8+	N.C.
Terminal No.	1A	2A	3A	4A	5A	6A	7A	8A	9A	10A	11A	12A	13A	14A	15A	16A
	1B	2B	3B	4B	5B	6B	7B	8B	9B	10B	11B	12B	13B	14B	15B	16B
Signal Name	OUT1-	N.C.	OUT2-	N.C.	OUT3-	N.C.	OUT4-	N.C.	OUT5-	N.C.	OUT6-	N.C.	OUT7-	N.C.	OUT8-	N.C.

N.C. : No Connection

Figure D1.2.2-8 Terminal numbers and signal names when connecting SAI533/L1AI533

■ Signal cable connection of the SBT4D

SBT4D has 16 channels of field wiring terminals. I/O modules in non-redundant or dual-redundant configuration can be connected. For a non-redundant configuration, you can connect CN1 to a module through a signal cable. For a dual-redundant configuration, you can connect CN1 and CN2 to a module through a signal cable.

The following figure shows the connectors for signal cables and field wiring terminals of SBT4D.

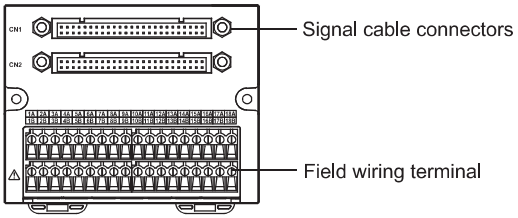


Figure D1.2.2-9 SBT4D terminal board

● Terminal numbers and signal names when connecting SAT145/L1AT145

The following figure shows the terminal numbers and signal names of the terminal board when connecting SAT145/L1AT145.

Signal Name	IN1+	IN2+	IN3+	IN4+	IN5+	IN6+	IN7+	IN8+	IN9+	IN10+	IN11+	IN12+	IN13+	IN14+	IN15+	IN16+	N.C.	N.C.
Terminal No.	1A	2A	3A	4A	5A	6A	7A	8A	9A	10A	11A	12A	13A	14A	15A	16A	17A	18A
	1B	2B	3B	4B	5B	6B	7B	8B	9B	10B	11B	12B	13B	14B	15B	16B	17B	18B
Signal Name	IN1-	IN2-	IN3-	IN4-	IN5-	IN6-	IN7-	IN8-	IN9-	IN10-	IN11-	IN12-	IN13-	IN14-	IN15-	IN16-	N.C.	N.C.

N.C. : No Connection

Figure D1.2.2-10 Terminal numbers and signal names when connecting SAT145/L1AT145

■ Signal cable connection of the SBR4D

SBR4D has 16 channels of field wiring terminals. I/O modules in non-redundant or dual-redundant configuration can be connected. For a non-redundant configuration, you can connect CN1 to a module through a signal cable. For a dual-redundant configuration, you can connect CN1 and CN2 to a module through a signal cable.

The following figure shows the connectors for signal cables and field wiring terminals of SBR4D.

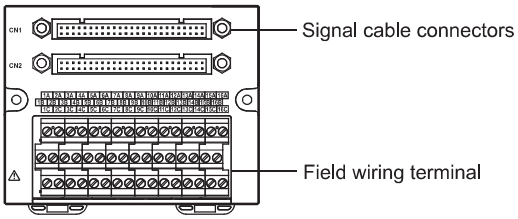


Figure D1.2.2-11 SBR4D terminal board

● Terminal numbers and signal names when connecting SAR145/L1AR145

The following figure shows the terminal numbers and signal names of the terminal board when connecting SAR145/L1AR145.

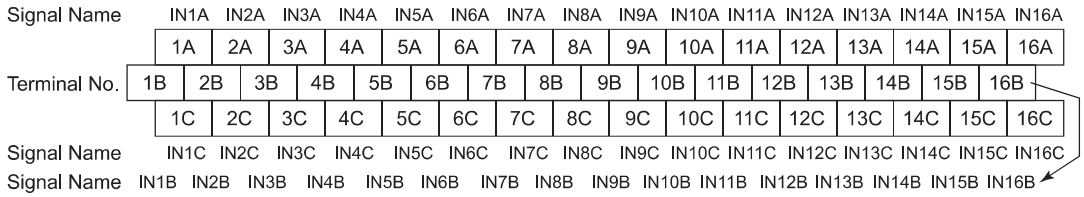


Figure D1.2.2-12 Terminal numbers and signal names when connecting SAR145/L1AR145

■ Signal cable connection of the S1BB4D

S1BB4D has 16 channels of field wiring terminals. I/O modules in non-redundant or dual-redundant configuration can be connected. For a non-redundant configuration, you can connect CN1 to a module through a signal cable. For a dual-redundant configuration, you can connect CN1 and CN2 to a module through a signal cable.

The following figure shows the connectors for signal cables and field wiring terminals of S1BB4D.

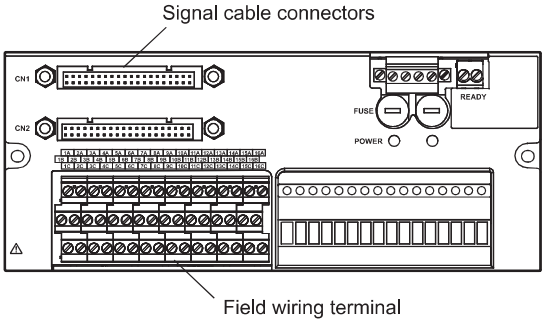


Figure D1.2.2-13 S1BB4D terminal board

● Terminal numbers and signal names when connecting SAI143/L1AI143

The following figure shows the terminal numbers and signal names of S1BB4D when connecting SAI143/L1AI143.

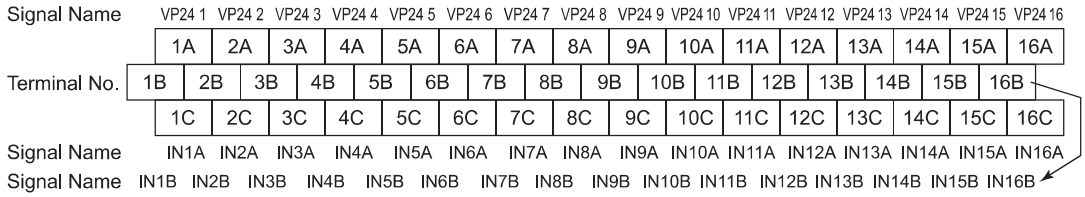


Figure D1.2.2-14 Terminal numbers and signal names of S1BB4D

Connect a 24 V DC power supply to the field power supply terminals of S1BB4D.

Configure the setting pins of SAI143/L1AI143 to four-wire type input.

The following table shows the signal names and their descriptions of S1BB4D.

Table D1.2.2-2 Signal names and descriptions of S1BB4D

Terminal number (*1)	Signal name (*1)	Description
□A	VP24□	Power supply output +
□B	IN□B (*2)	Current input +
□C	IN□A (*2)	Current input - Power supply output -

*1: □: 1 to 16
*2: This signal name is shared with SAI143/L1AI143.

SEE ALSO For more information about the setting pins of SAI143/L1AI143, refer to:

"● Signal cable connections of SAI143/L1AI143" on page D1-14

D1.3 Signal cable connection to digital I/O modules

This section describes the signal connections of digital I/O modules.

The following table shows the available methods of connecting digital I/O modules and field devices.

Table D1.3-1 Methods of connecting digital I/O modules and field devices

Digital I/O module	Method of connection with field devices (*1)		
	Pressure clamp terminal	Terminal board	MIL cable
SDV144/L1DV144	Yes	Yes	Yes
SDV521/L1DV521	-	Yes	-
SDV526/L1DV526	-	Yes	-
SDV531/L1DV531	Yes	Yes	Yes
SDV53A/L1DV53A	-	Yes	-
SDV541/L1DV541	Yes	Yes	Yes

*1: Yes: connection possible

SEE ALSO

For more information about the field connection diagram for SCSs that support SIL 3, refer to:

ProSafe-RS Field Device Connection (for FIO) (GS 32Q06J10-31E)

For more information about the field connection diagram for SCSs that support SIL 2, refer to:

ProSafe-RS Lite Field Device Connection (GS 32P56J10-01EN)

D1.3.1 Terminal numbers and signal names of pressure clamp terminal blocks and the MIL connector of digital I/O modules

This section describes the terminal numbers and signal names of pressure clamp terminal blocks and the MIL connector of digital I/O modules.

The following figure shows the terminal number layout of a pressure clamp terminal.

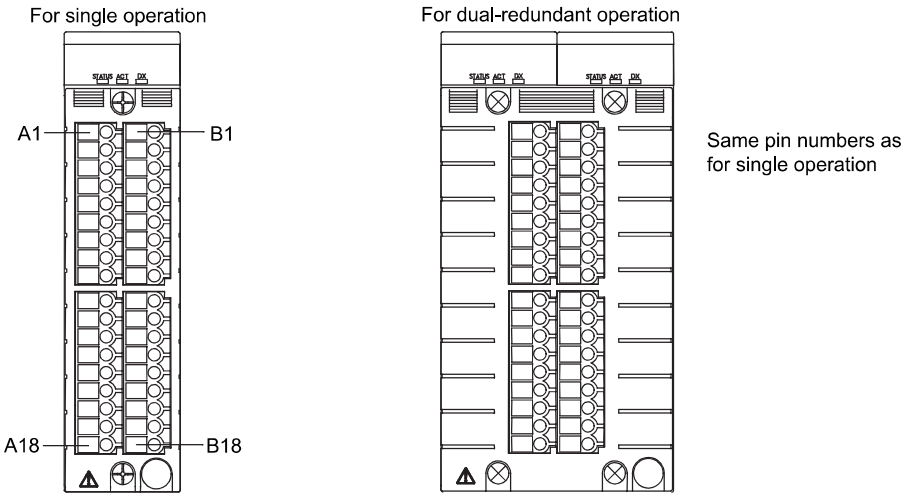


Figure D1.3.1-1 Terminal number layout of a pressure clamp terminal

The terminal numbers of a pressure clamp terminal block are arranged in the order from A1, A2 and so on until A18 starting from the top of the left column and from B1, B2 and so on until B18 from the top of the right column with the terminal block on the front. The terminal number layout of a dual-redundant type pressure clamp terminal is the same.

The following figure shows the layout of the terminal numbers of the MIL connector.

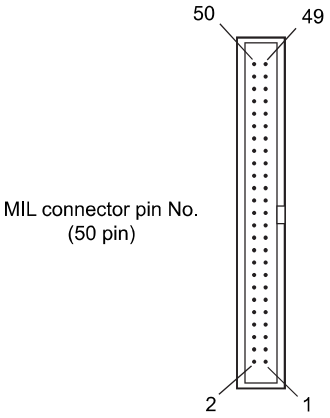


Figure D1.3.1-2 Terminal number layout of the MIL connector

Input terminal numbers and signal names of SDV144/L1DV144

The following figure shows the pressure clamp terminal numbers, MIL connector pin numbers, and signal names of SDV144/L1DV144.

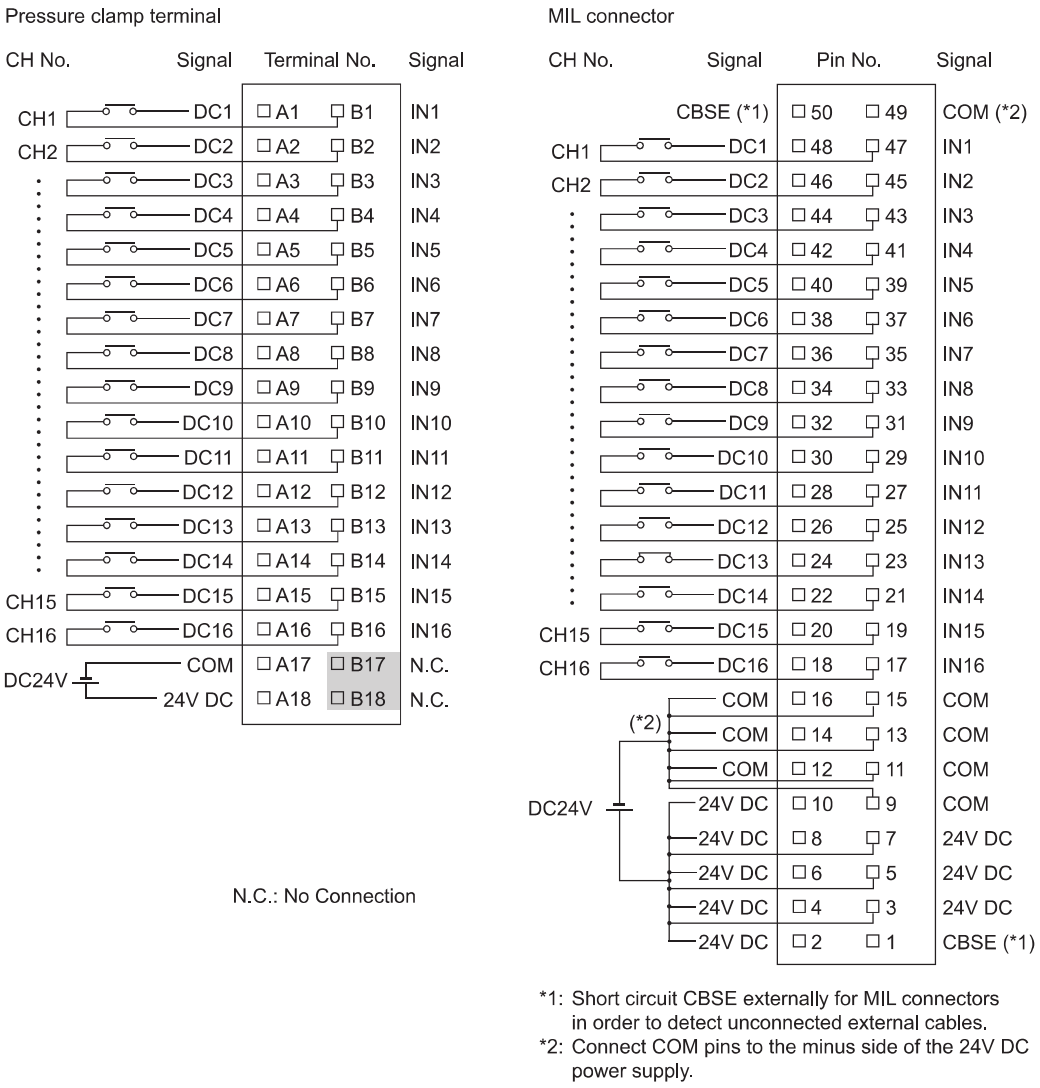


Figure D1.3.1-3 SDV144/L1DV144 signal connection

Output terminal numbers and signal names of SDV531/L1DV531

The following figure shows the pressure clamp terminal numbers, MIL connector pin numbers, and signal names of SDV531/L1DV531.

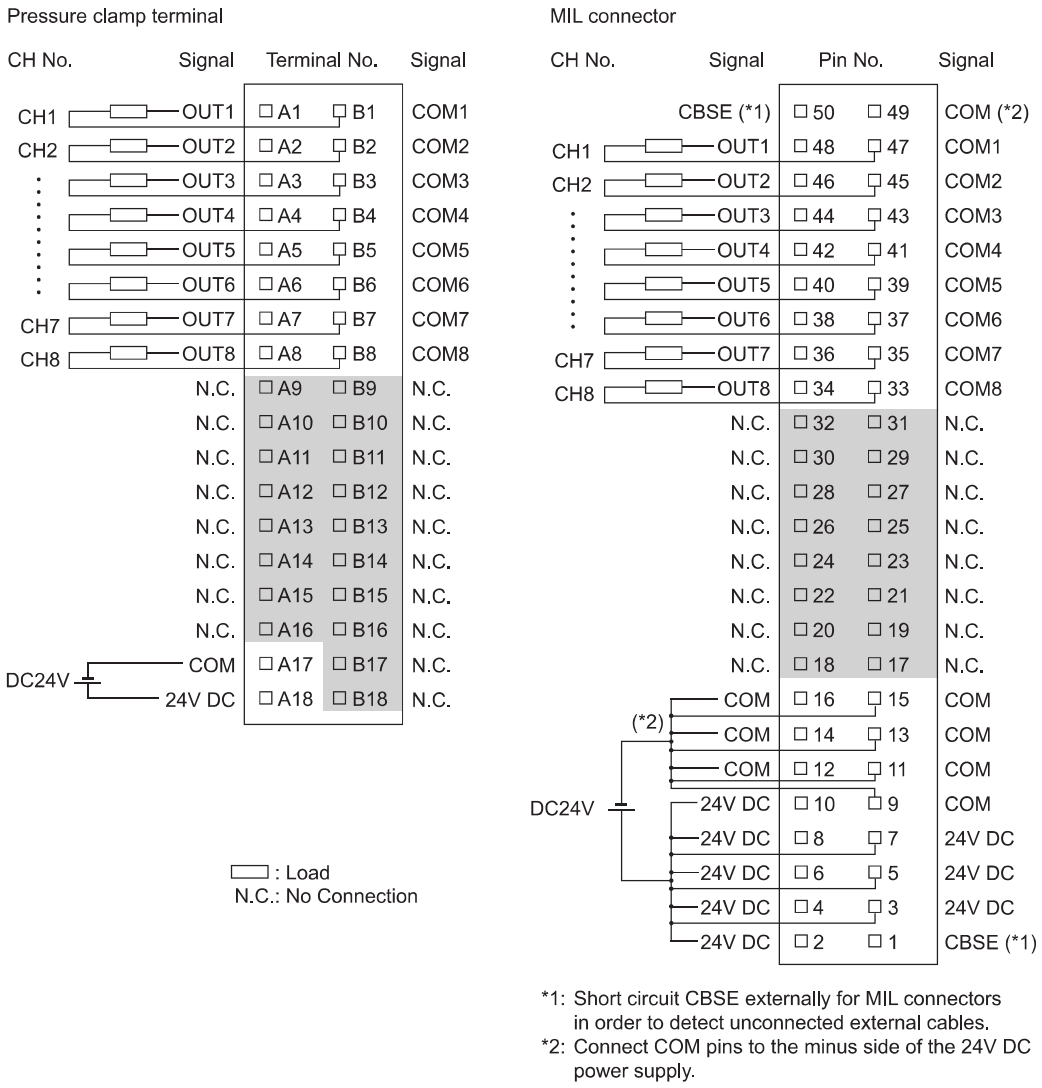


Figure D1.3.1-4 SDV531/L1DV531 signal connection

Output terminal numbers and signal names of SDV541/L1DV541

The following figure shows the pressure clamp terminal numbers, MIL connector pin numbers, and signal names of SDV541/L1DV541.

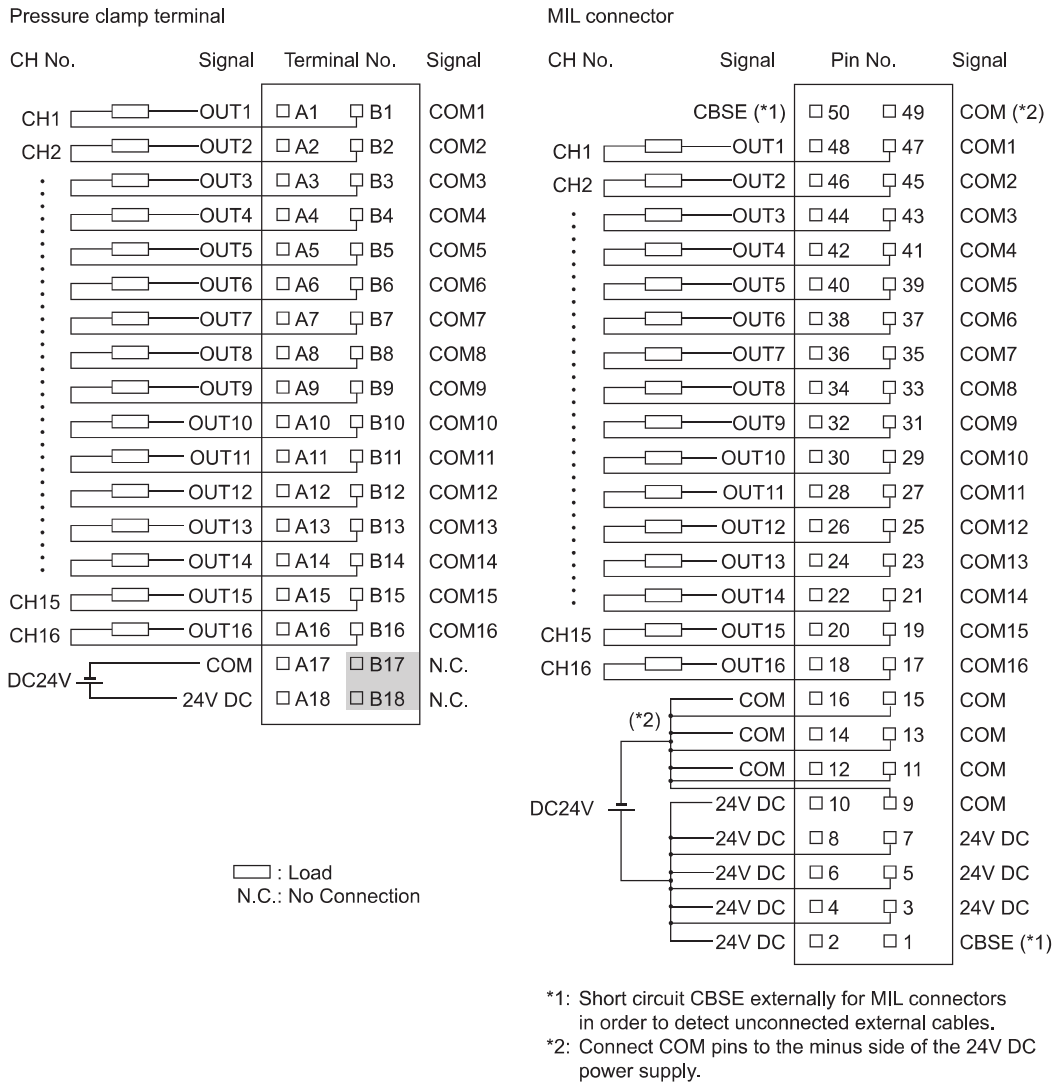


Figure D1.3.1-5 SDV541/L1DV541 signal connection

D1.3.2 Terminal numbers and signal names of the terminal board for digital I/O modules

This section describes the terminal numbers and signal names of the terminal board for digital I/O modules. The following table shows the modules that you can connect to the terminal board.

Table D1.3.2-1 Relationship between terminal boards and digital Input/Output modules

Terminal board (type)	Connectable analog I/O module (type)	
	For SCSs that support SIL 3	For SCSs that support SIL 2
SED2D	SDV521	L1DV521
SED3D	SDV53A	L1DV53A
SED4D	SDV144, SDV531, SDV541	L1DV144, L1DV531, L1DV541
SWD2D	SDV526	L1DV526
SBD2D	SDV521	L1DV521
SBD3D	SDV531, SDV53A	L1DV531, L1DV53A
SBD4D	SDV144, SDV541	L1DV144, L1DV541

Signal cable connection of SED2D

SED2D has four sets of 4 channels of field wiring terminals. You can connect to an output module with a non-redundant or dual-redundant configuration. For a non-redundant configuration, you can connect CN1, CN3, CN5, or CN7 to a module through a signal cable. For a dual-redundant configuration, you can connect CN1 and CN2, CN3 and CN4, CN5 and CN6, or CN7 and CN8 to a module through a signal cable.

The following figure shows the connectors for signal cables and field wiring terminals of SED2D.

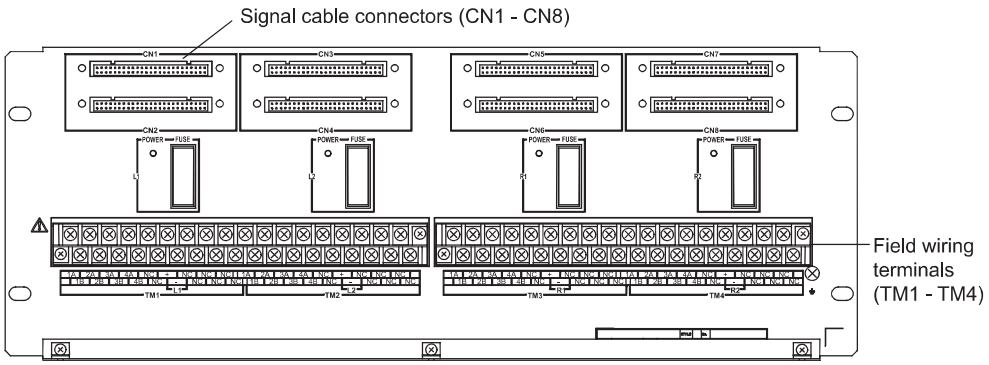


Figure D1.3.2-1 SED2D terminal board

Terminal numbers and signal names when connecting SDV521/L1DV521

The following figure shows the terminal numbers and signal names of the terminal board when connecting SDV521/L1DV521.

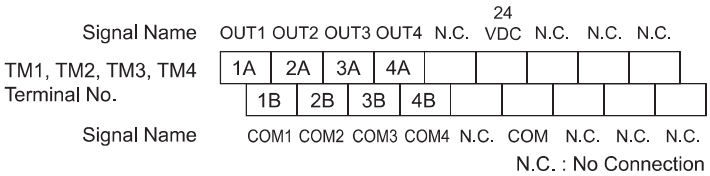


Figure D1.3.2-2 Terminal numbers and signal names when connecting SDV521/L1DV521

Signal cable connection of SED3D

SED3D has four sets of 8 channels of field wiring terminals. You can connect to an output module with a non-redundant or dual-redundant configuration. A non-redundant module should be connected to CN1, CN3, CN5, or CN7 by using a signal cable. A redundant pair of modules should be connected to CN1 and CN2, CN3 and CN4, CN5 and CN6, or CN7 and CN8 by using signal cables.

The following figure shows the connectors for signal cables and field wiring terminals of SED3D.

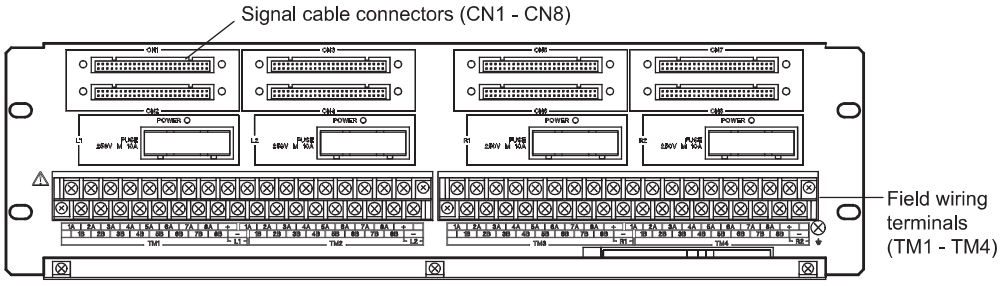


Figure D1.3.2-3 SED3D terminal board

Terminal numbers and signal names when connecting SDV53A/L1DV53A

The following figure shows the terminal numbers and signal names of the terminal board when connecting SDV53A/L1DV53A. You must connect a 48 V DC power supply between the 48 V DC and COM terminals.

Signal Name	OUT1	OUT2	OUT3	OUT4	OUT5	OUT6	OUT7	OUT8	48 V DC
TM1, TM2, TM3, TM4 Terminal No.	1A	2A	3A	4A	5A	6A	7A	8A	+
	1B	2B	3B	4B	5B	6B	7B	8B	–
Signal Name	COM1	COM2	COM3	COM4	COM5	COM6	COM7	COM8	COM

Figure D1.3.2-4 Terminal numbers and signal names when connecting SDV53A/L1DV53A

SED4D signal cable connection

SED4D has two sets of 16 channels of field wiring terminals. I/O modules in non-redundant or dual-redundant configuration can be connected. A non-redundant module should be connected to CN1 or CN3 by using a signal cable. A redundant pair of modules should be connected to CN1 and CN2, or CN3 and CN4 by using signal cables.

The following figure shows the connectors for signal cables and field wiring terminals of SED4D.

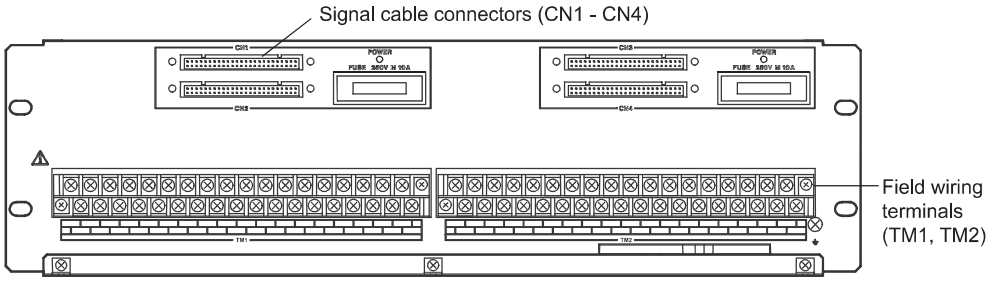


Figure D1.3.2-5 SED4D terminal board

Terminal numbers and signal names when connecting SDV144/L1DV144

The following figure shows the terminal numbers and signal names of the terminal board when connecting SDV144/L1DV144. You must connect a 24 V DC power supply between the 24 V DC and COM terminals.

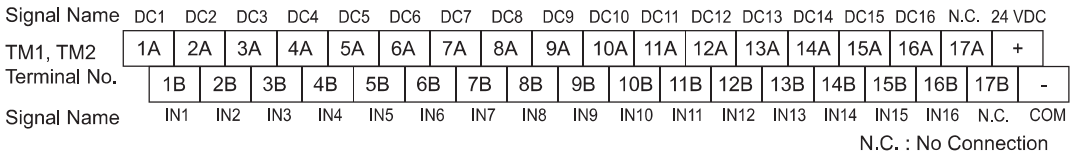


Figure D1.3.2-6 Terminal numbers and signal names when connecting SDV144/L1DV144

Terminal numbers and signal names when connecting SDV531/L1DV531

The following figure shows the terminal numbers and signal names of the terminal board when connecting SDV531/L1DV531. You must connect a 24 V DC power supply between the 24 V DC and COM terminals.

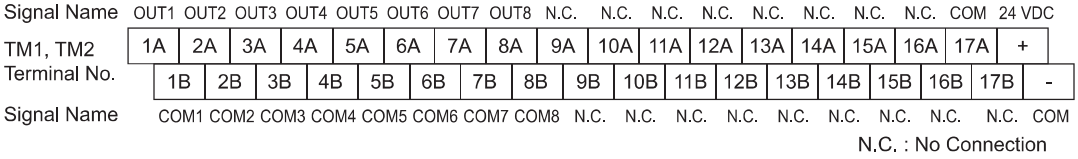


Figure D1.3.2-7 Terminal numbers and signal names when connecting SDV531/L1DV531

Terminal numbers and signal names when connecting SDV541/L1DV541

The following figure shows the terminal numbers and signal names of the terminal board when connecting SDV541/L1DV541. You must connect a 24 V DC power supply between the 24 V DC and COM terminals.

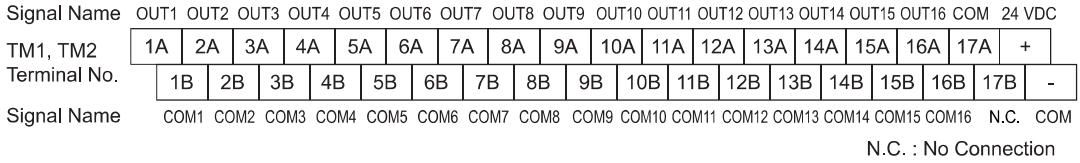


Figure D1.3.2-8 Terminal numbers and signal names when connecting SDV541/L1DV541

Signal cable connection of SWD2D

SWD2D has four sets of 4 channels of field wiring terminals. You can connect to an output module with a non-redundant or dual-redundant configuration. A non-redundant module should be connected to CN1, CN3, CN5, or CN7 by using a signal cable. A redundant pair of modules should be connected to CN1 and CN2, CN3 and CN4, CN5 and CN6, or CN7 and CN8 by using signal cables.

The following figure shows the connectors for signal cables and field wiring terminals of SWD2D.

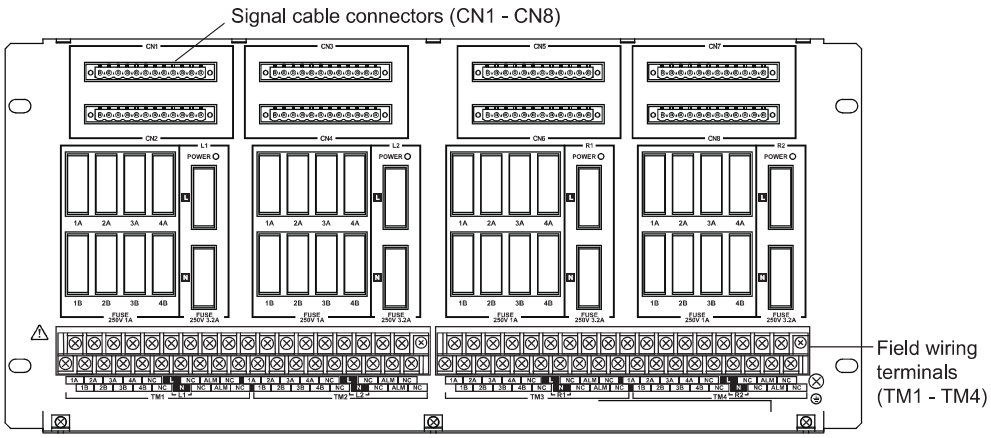


Figure D1.3.2-9 SWD2D terminal board

Terminal numbers and signal names when connecting SDV526/L1DV526

The following figure shows the terminal numbers and signal names of the terminal board when connecting SDV526/L1DV526.

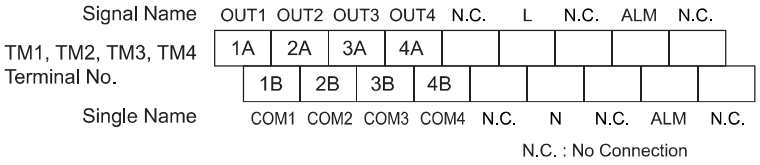


Figure D1.3.2-10 Terminal numbers and signal names when connecting SDV526/L1DV526

You must connect an external power supply between the L and N terminals.

WARNING

Before you connect cables to the terminals, turn off the external power supply and check with a tester that the electricity is not flowing through the cables.

SEE ALSO

For more information about SDV526 output specifications and external supply power specifications, refer to:

ProSafe-RS Digital I/O Modules (for FIO) (GS 32Q06K40-31E)

For more information about L1DV526 output specifications and external supply power specifications, refer to:

ProSafe-RS Lite Digital I/O Modules (GS 32P56K40-01EN)

Signal cable connection of SBD2D

SBD2D has 4 channels of field wiring terminals. You can connect to an output module with a non-redundant or dual-redundant configuration. For a non-redundant configuration, you can connect CN1 to a module through a signal cable. For a dual-redundant configuration, you can connect CN1 and CN2 to a module through a signal cable.

The following figure shows the connectors for signal cables and field wiring terminals of SBD2D.

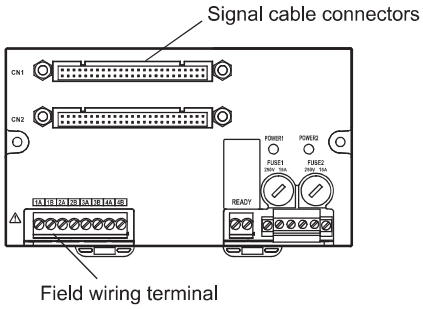


Figure D1.3.2-11 SBD2D terminal board

● Terminal numbers and signal names when connecting SDV521/L1DV521

The following figure shows the terminal numbers and signal names of the terminal board when connecting SDV521/L1DV521.

You must connect a 24 V DC power supply between 24 V DC and COM.

Signal Name	OUT1	COM1	OUT2	COM2	OUT3	COM3	OUT4	COM4
Terminal No.	1A	1B	2A	2B	3A	3B	4A	4B

Signal Name	READY
Terminal No.	READY

Signal Name	24V DC	COM	24V DC	COM
Terminal No.	1+	1-	2+	2-

Figure D1.3.2-12 Terminal numbers and signal names when connecting SDV521/L1DV521

■ Signal cable connection of SBD3D

SBD3D has 8 channels of field wiring terminals. You can connect to an output module with a non-redundant or dual-redundant configuration. For a non-redundant configuration, you can connect CN1 to a module through a signal cable. For a dual-redundant configuration, you can connect CN1 and CN2 to a module through a signal cable.

The following figure shows the connectors for signal cables and field wiring terminals of SBD3D.

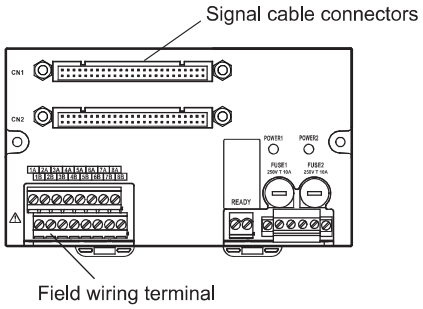


Figure D1.3.2-13 SBD3D terminal board

● Terminal numbers and signal names when connecting SDV531/L1DV531

The following figure shows the terminal numbers and signal names of the terminal board when connecting SDV531/L1DV531.

You must connect a 24V DC power supply between the 24V DC and COM terminals.

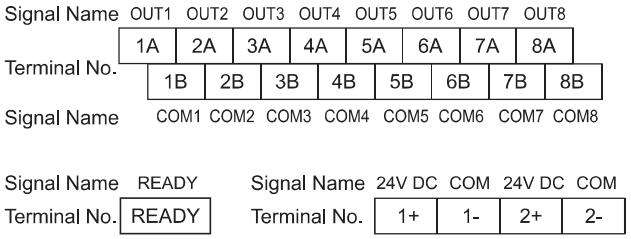


Figure D1.3.2-14 Terminal numbers and signal names when connecting SDV531/L1DV531

● Terminal numbers and signal names when connecting SDV53A/L1DV53A

The following figure shows the terminal numbers and signal names of the terminal board when connecting SDV53A/L1DV53A.

You must connect a 48V DC power supply between the 48V DC and COM terminals.

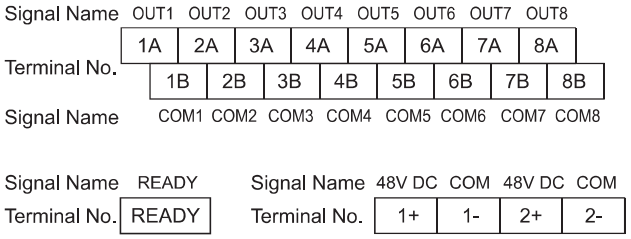


Figure D1.3.2-15 Terminal numbers and signal names when connecting SDV53A/L1DV53A

■ SBD4D signal cable connection

SBD4D has 16 channels of field wiring terminals. I/O modules in non-redundant or dual-redundant configuration can be connected. A non-redundant module should be connected to CN1 by using a signal cable. A redundant pair of modules should be connected to CN1 and CN2 by using signal cables.

The following figure shows the connectors for signal cables and field wiring terminals of SBD4D.

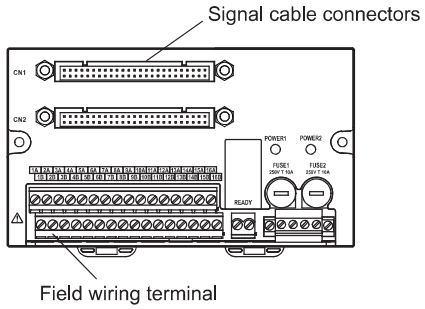


Figure D1.3.2-16 SBD4D terminal board

● Terminal numbers and signal names when connecting SDV144/L1DV144

The following figure shows the terminal numbers and signal names of the terminal board when connecting SDV144/L1DV144.

You must connect a 24V DC power supply between the 24V DC and COM terminals.

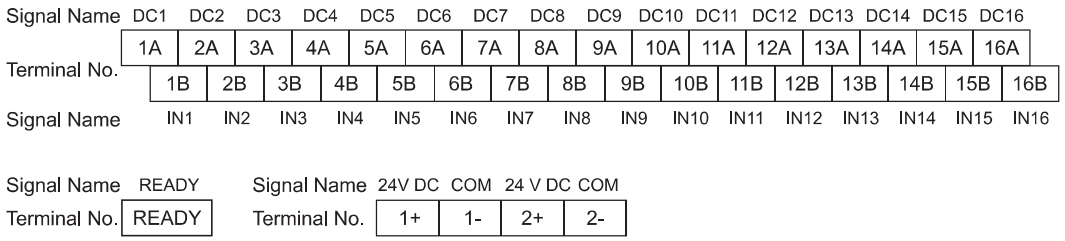


Figure D1.3.2-17 Terminal numbers and signal names when connecting SDV144/L1DV144

Terminal numbers and signal names when connecting SDV541/L1DV541

The following figure shows the terminal numbers and signal names of the terminal board when connecting SDV541/L1DV541.

You must connect a 24V DC power supply between the 24V DC and COM terminals.

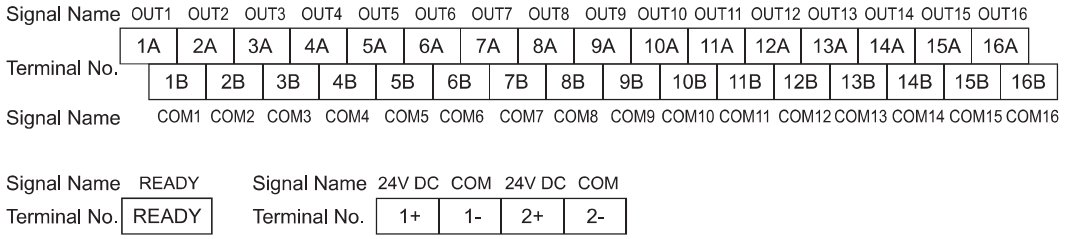


Figure D1.3.2-18 Terminal numbers and signal names when connecting SDV541/L1DV541

D1.3.3 Relay board terminal numbers and signal names

This section describes the terminal numbers and signal names on relay boards.

Signal cable connection of SRM53D

SRM53D receives signals from two pairs of redundant 8-channel digital output modules and sends contact output signals to the field devices. The actual relay output status can be read back by connecting a 16-channel digital input module.

SRM53D terminal numbers and signal names

CAUTION

- Connect a 24 V DC power supply to the "+" and "-" terminals in TM3.
- After completing the power supply wiring, put back the protective cover for the terminals.
- Provide mediate switches or breakers in the power supply wiring so that the power supply for each relay board can be shutoff individually during maintenance.

The following figure shows the connectors and terminals of SRM53D.

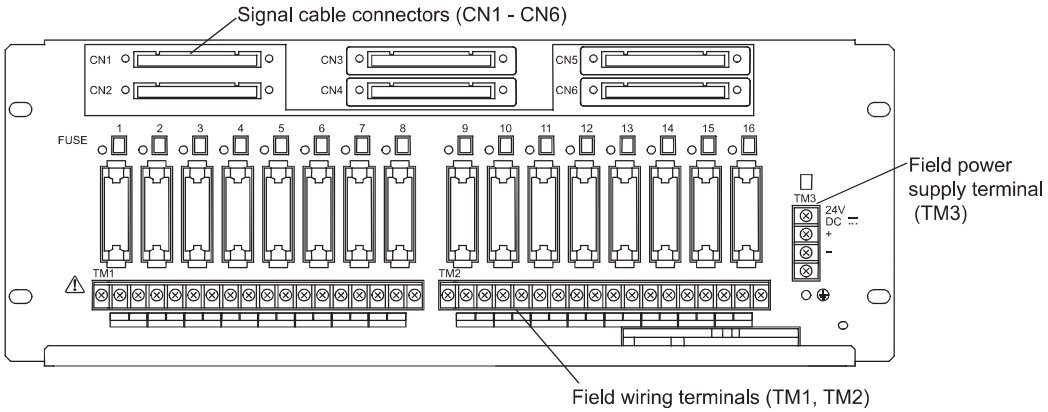


Figure D1.3.3-1 SRM53D relay board

The following figure shows the terminal numbers and signal names of SRM53D.

TM1	Signal Name	OUT1		OUT2		OUT3		OUT4		OUT5		OUT6		OUT7		OUT8	
	Terminal No.	1		2		3		4		5		6		7		8	
		A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B

TM2	Signal Name	OUT1		OUT2		OUT3		OUT4		OUT5		OUT6		OUT7		OUT8	
	Terminal No.	1		2		3		4		5		6		7		8	
		A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B

Figure D1.3.3-2 SRM53D terminal numbers and signal names

Signal connection between SRM53D and digital I/O modules

The following table shows the relation between the digital I/O module connectors and the connected field wiring terminal numbers.

Table D1.3.3-1 Connector numbers and connected field wiring terminal numbers

Connector number	Connection	Field wiring terminal numbers	Remarks
CN1	SDV531/ L1DV531	TM1 (1-8)	CN1/CN2 redundancy
CN2			
CN3	SDV144/ L1DV144	TM1 (1-8), TM2 (1-8)	Readback; CN3/CN4 redundancy
CN4			
CN5	SDV531/ L1DV531	TM2 (1-8)	CN5/CN6 redundancy
CN6			

The following table shows the relation among the relay numbers, the field wiring terminal numbers, and the channel numbers of digital I/O modules.

Table D1.3.3-2 Relay numbers/field wiring terminal numbers/channel numbers

Relay number (*1)	Field wiring terminal numbers		CN1	CN2	CN3	CN4	CN5	CN6
			Channel numbers of digital I/O modules					
			SDV531/L1DV531		SDV144/L1DV144		SDV531/L1DV531	
1	TM1	1A/1B	ch1	ch1	ch1	ch1	-	-
2	TM1	2A/2B	ch2	ch2	ch2	ch2	-	-
3	TM1	3A/3B	ch3	ch3	ch3	ch3	-	-
4	TM1	4A/4B	ch4	ch4	ch4	ch4	-	-
5	TM1	5A/5B	ch5	ch5	ch5	ch5	-	-
6	TM1	6A/6B	ch6	ch6	ch6	ch6	-	-
7	TM1	7A/7B	ch7	ch7	ch7	ch7	-	-
8	TM1	8A/8B	ch8	ch8	ch8	ch8	-	-
9	TM2	1A/1B	-	-	ch9	ch9	ch1	ch1
10	TM2	2A/2B	-	-	ch10	ch10	ch2	ch2
11	TM2	3A/3B	-	-	ch11	ch11	ch3	ch3
12	TM2	4A/4B	-	-	ch12	ch12	ch4	ch4
13	TM2	5A/5B	-	-	ch13	ch13	ch5	ch5
14	TM2	6A/6B	-	-	ch14	ch14	ch6	ch6
15	TM2	7A/7B	-	-	ch15	ch15	ch7	ch7
16	TM2	8A/8B	-	-	ch16	ch16	ch8	ch8

*1: The relay number is the number printed on the SRM53D metal body above each relay.

The following table shows the statuses of digital output (DO) modules, status lamps, field wiring terminals, and digital input (DI) modules.

Table D1.3.3-3 Statuses of DO modules, status lamps, and DI modules

DO module output status (*1)	Status lamp	Field wiring terminal status	DI module input status(*1)
OFF	OFF (*2)	OFF (Open)	ON (Close)
ON	ON	ON (Close)	OFF (Open)

*1: The output contacts are A type (NO: Normally Open), while the contacts for DI modules are B type (NC: Normally Close).
*2: If the ON pulse diagnosis for SDV531/L1DV531 is enabled and the output status is set to OFF, the LED goes ON for each ON pulse output.

IMPORTANT

When SDV144/L1DV144 is connected to SRM53D, Detect Disconnection and Detect Short Circuit should be set to "No" on I/O Parameter Builder.

SEE ALSO For more information about settings on I/O Parameter Builder, refer to:

Appendix 1.3.4, “Settings for the DI channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Signal cable connection of SRM54D

SRM54D receives signals from a 16-channel digital output module and sends contact output signals to the external devices. The actual relay output status can be read back by connecting a 16-channel digital input module.

SRM54D terminal numbers and signal names

CAUTION

- Connect a 24 V DC power supply to the "+" and "-" terminals in TM3.
- After completing the power supply wiring, put back the protective cover for the terminals.
- Provide mediate switches or breakers in the power supply wiring so that the power supply for each relay board can be shutoff individually during maintenance.

The following figure shows the connectors and terminals of SRM54D.

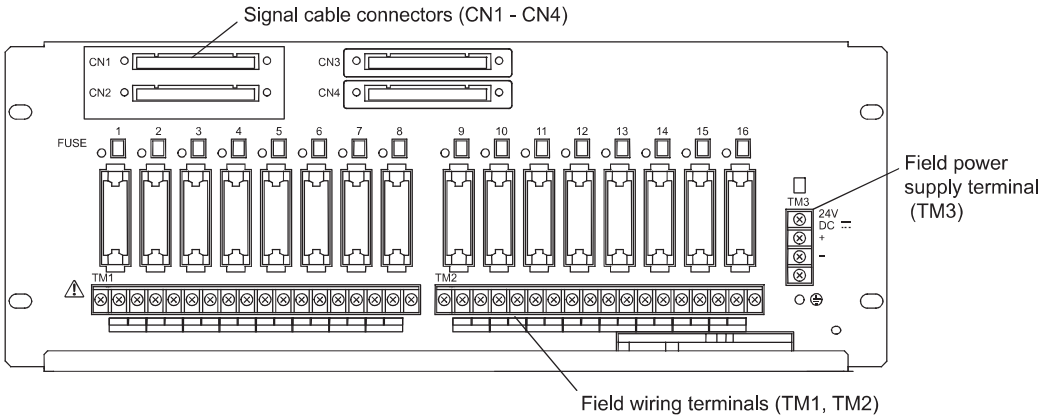


Figure D1.3.3-3 SRM54D relay board

The following figure shows the terminal numbers and signal names of SRM54D.

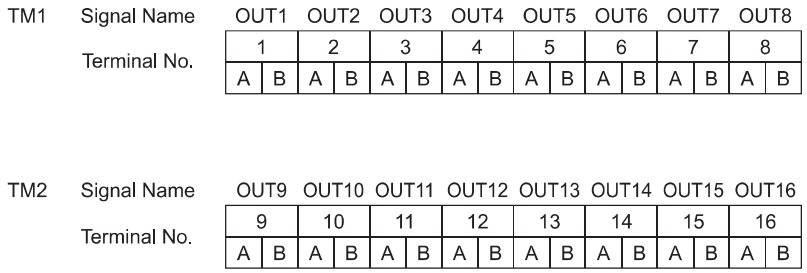


Figure D1.3.3-4 SRM54D terminal numbers and signal names

Signal connection between the SRM54D and digital I/O modules

The following table shows the relation between the digital I/O module connector numbers and the connected field wiring terminal numbers.

Table D1.3.3-4 Connector numbers and connected field wiring terminal numbers

Connector number	Connection	Field wiring terminal numbers	Remarks
CN1	SDV541/ L1DV541	TM1 (1-8), TM2 (9-16)	CN1/CN2 redundancy
CN2			
CN3	SDV144/ L1DV144	TM1 (1-8), TM2 (9-16)	Readback; CN3/CN4 redundancy
CN4			

The following table shows the relation among the relay numbers, the field wiring terminal numbers, and the channel numbers of digital I/O modules.

Table D1.3.3-5 Relay numbers/field wiring terminal numbers/channel numbers

Relay number (*1)	Field wiring terminal numbers		CN1	CN2	CN3	CN4
			Channel numbers of digital I/O modules			
			SDV541/L1DV541		SDV144/L1DV144	
1	TM1	1A/1B	ch1	ch1	ch1	ch1
2	TM1	2A/2B	ch2	ch2	ch2	ch2
3	TM1	3A/3B	ch3	ch3	ch3	ch3
4	TM1	4A/4B	ch4	ch4	ch4	ch4
5	TM1	5A/5B	ch5	ch5	ch5	ch5
6	TM1	6A/6B	ch6	ch6	ch6	ch6
7	TM1	7A/7B	ch7	ch7	ch7	ch7
8	TM1	8A/8B	ch8	ch8	ch8	ch8
9	TM2	9A/9B	ch9	ch9	ch9	ch9
10	TM2	10A/10B	ch10	ch10	ch10	ch10
11	TM2	11A/11B	ch11	ch11	ch11	ch11
12	TM2	12A/12B	ch12	ch12	ch12	ch12
13	TM2	13A/13B	ch13	ch13	ch13	ch13
14	TM2	14A/14B	ch14	ch14	ch14	ch14
15	TM2	15A/15B	ch15	ch15	ch15	ch15
16	TM2	16A/16B	ch16	ch16	ch16	ch16

*1: The relay number is the number printed on the SRM54D metal body above each relay.

The following table shows the statuses of digital output (DO) modules, status lamps, and digital input (DI) modules.

Table D1.3.3-6 Statuses of DO modules, status lamps, and DI modules

DO module output status (*1)	Status lamp	Field wiring terminal status	DI module input status (*1)
OFF	OFF(*2)	OFF (Open)	ON (Close)
ON	ON	ON (Close)	OFF (Open)

*1: The output contacts are A type (NO: Normally Open), while the contacts for DI modules are B type (NC: Normally Close).
*2: If the ON pulse diagnosis for SDV541/L1DV541 is enabled and the output status is set to OFF, the LED goes ON for each ON pulse output.

IMPORTANT

When SDV144/L1DV144 is connected to SRM54D, Detect Disconnection and Detect Short Circuit should be set to "No" on I/O Parameter Builder.

SEE ALSO

For more information about settings on I/O Parameter Builder, refer to:

Appendix 1.3.4, “Settings for the DI channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Signal cable connections of SBM54D

SBM54D receives signals from a 16-channel digital output module and sends contact output signals to the external devices.

SBM54D terminal numbers and signal names

CAUTION

- You can use dual power supplies. Connect a 24V DC power supply to the "1+" "1-" terminals and "2+" "2-" terminals each.
- Provide mediate switches or breakers in the power supply wiring so that the power supply for each relay board can be shutoff individually during maintenance.

The following figure shows the connectors and terminals of SBM54D.

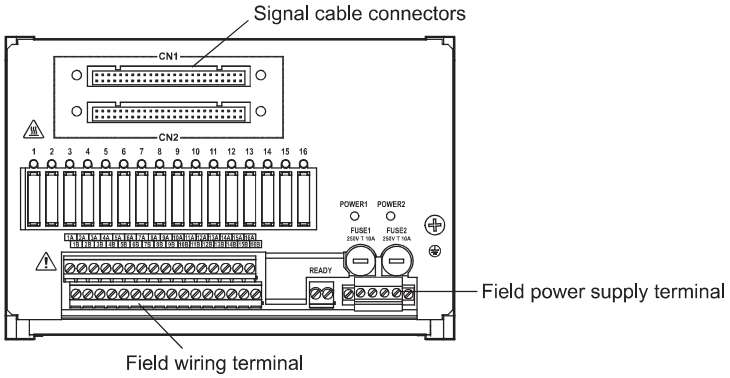


Figure D1.3.3-5 SBM54D relay board

The following figure shows the terminal numbers and signal names of SBM54D.

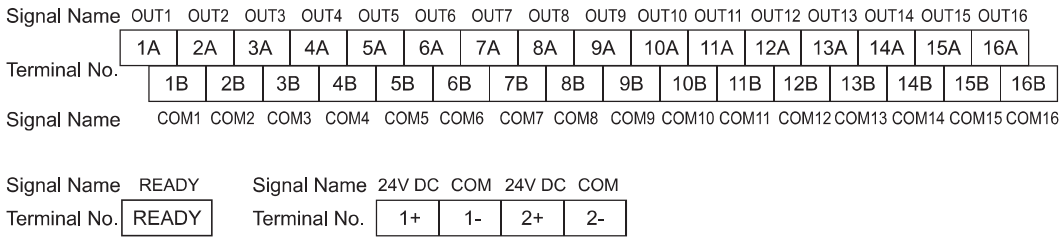


Figure D1.3.3-6 SBM54D terminal numbers and signal names

Signal connections between SBM54D and digital I/O modules

The following table shows the relation between the digital I/O module connector numbers and the connected field wiring terminal numbers.

Table D1.3.3-7 Connector numbers and connected field wiring terminal numbers

Connector number	Connection	Field wiring terminal number	Remarks
CN1	SDV541/ L1DV541	1 to 16	CN1/CN2 redundancy
CN2			

The following table shows the relation among the relay numbers, the field wiring terminal numbers, the digital I/O module connectors, and the SDV541/L1DV541 channel numbers.

Table D1.3.3-8 Relay numbers/field wiring terminal numbers/channel numbers

Relay number (*1)	Field wiring terminal number	CN1	CN2
		SDV541/L1DV541 channel number	
1	1A/1B	ch1	ch1
2	2A/2B	ch2	ch2
3	3A/3B	ch3	ch3
4	4A/4B	ch4	ch4
5	5A/5B	ch5	ch5
6	6A/6B	ch6	ch6
7	7A/7B	ch7	ch7
8	8A/8B	ch8	ch8
9	9A/9B	ch9	ch9
10	10A/10B	ch10	ch10
11	11A/11B	ch11	ch11
12	12A/12B	ch12	ch12
13	13A/13B	ch13	ch13
14	14A/14B	ch14	ch14
15	15A/15B	ch15	ch15
16	16A/16B	ch16	ch16

*1: The relay number is the number printed on the SRM54D metal body above each relay.

The following table shows the statuses of SDV541/L1DV541 outputs, channel status lamps, and field wiring terminals.

Table D1.3.3-9 Statuses of SDV541/L1DV541 outputs, channel status lamps, and field wiring terminals

SDV541/L1DV541 output status	Channel status display lamp	Field wiring terminal status
OFF	OFF	OFF (Open)
ON	ON	ON (Close)

IMPORTANT

When SDV541/L1DV541 is connected to SBM54D, Detect Disconnection, Pulse Test (OFF), and Pulse Test (ON) should be set to "No" on I/O Parameter Builder.

SEE ALSO For more information about settings on I/O Parameter Builder, refer to:

Appendix 1.3.5, “Settings for the DO channel” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Protecting the contact when an inductive load is connected to the contact output

When connecting an inductive load to the contact output, you must connect a protection circuit in parallel with the load. In general, a diode is used as a protection circuit for DC power supply and a series-connected CR is used as a protection circuit for AC power supply.

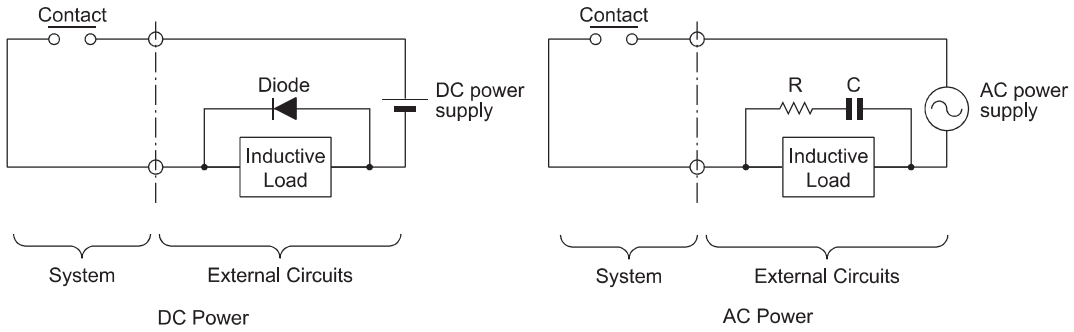


Figure D1.3.3-7 Example of connecting a protection circuit

D1.4 Connection of communication modules

This section describes how to connect communication modules to external devices. The communication modules support Modbus slave communication, subsystem communication, and safety subsystem communication. In Modbus slave communication, an external device acts as the master and SCS acts as a slave. In subsystem communication and safety subsystem communication, SCS acts as the master and external devices act as slaves.

The following communication modules are available:

- ALR111: Serial communication module (RS-232C)
- ALR121: Serial communication module (RS-422/RS-485)
- ALE111: Ethernet communication module
- S2LP131: Fire and gas communication module

D1.4.1 Connection of the serial communication module (RS-232C)

This section describes how to connect the communication cable of the serial communication module (RS-232C) (Model: ALR111).

The following figure shows the communication connectors.

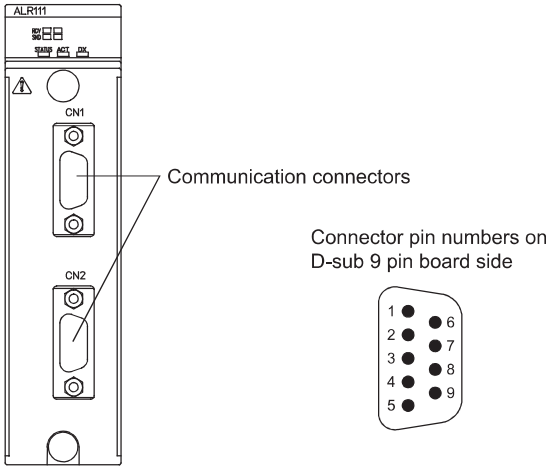


Figure D1.4.1-1 ALR111

The following table shows the pin numbers and signal names of the communication connectors.

Table D1.4.1-1 Pin numbers and signal names of the RS-232C communication connector

CN1 and CN2 pin numbers	Abbrev.	Signal name	Signal direction at the ALR111 side
1	CD	Carrier Detect	Input
2	RD	Receive Data	Input
3	SD	Send Data	Output
4	ER	Equipment Ready	Output
5	SG	Signal Ground	Signal ground
6	DR	Data Set Ready	Input
7	RS	Request to Send	Output
8	CS	Clear to Send	Input
9	-	N.C.	-

Connecting external devices to ALR111

It is recommended to relay through a modem when you connect to the ALR111 and the external device. If the distance between the ALR111 and the external device is less than 15 meters, you can connect to the external device directly. If the distance is more than 15 meters, you must relay through a modem. The methods of connecting to the external device are as follows:

- Connection with modem
- Connecting to the external device by using the RS-232C D-sub 25-pin connector (direct connection)
- Connecting to the external device by using the RS-232C D-sub 9-pin connector (direct connection)

Connection with modem

The following figure shows an example of the cable connections when connecting the ALR111 to the external device through a modem. The length of the RS-232C cable between the ALR111 and the model should be less than 15 meters. You must connect the FG of the modem to the protective grounding system.

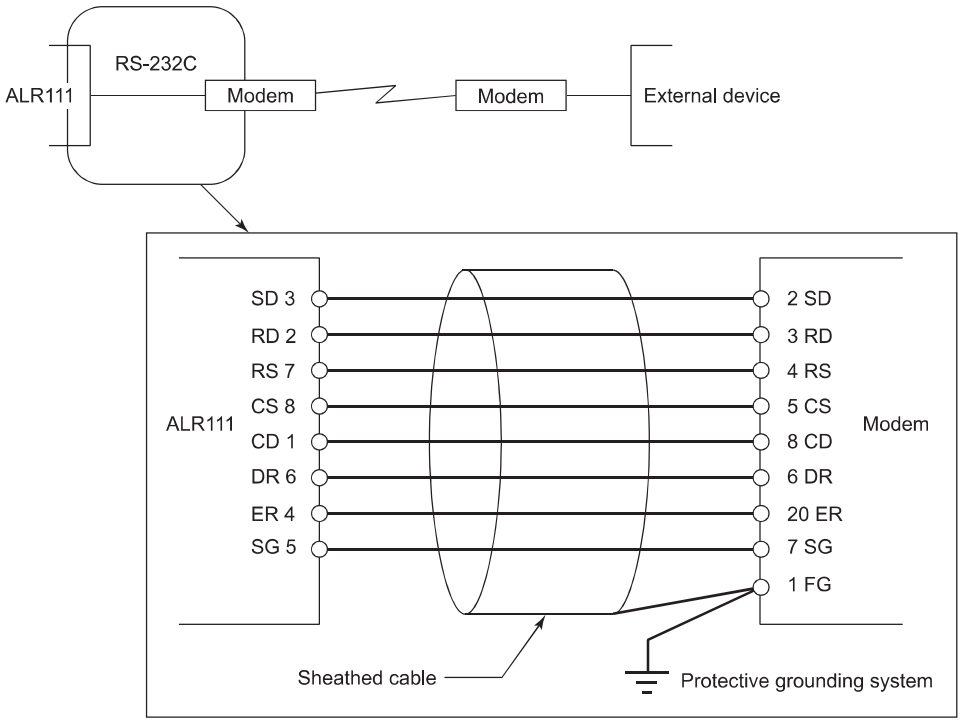


Figure D1.4.1-2 Cable connection when the ALR111 and the external device are connected using modems

Directly connecting to the external device with the RS-232C D-sub 25-pin connector

The following figure shows an example of the cable connections when directly connecting the ALR111 and the external device with the RS-232C D-sub 25-pin connector. The RS-232C cable should be less than 15 meters. If the cable is longer than 15 meters, you must connect through a modem.

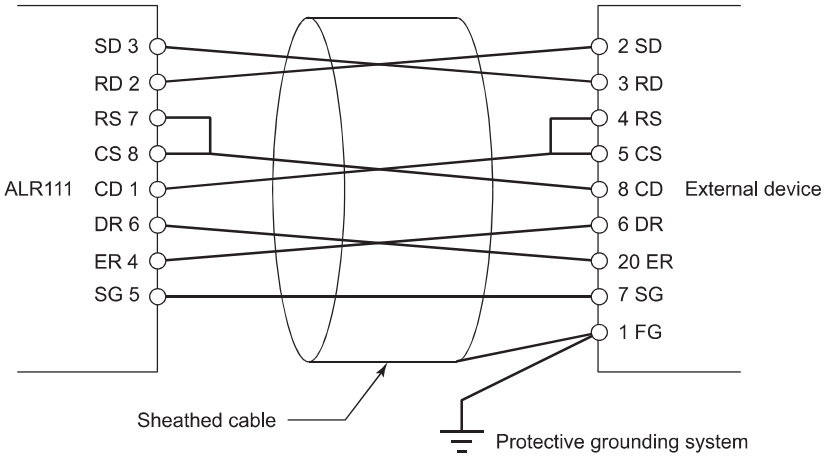


Figure D1.4.1-3 Cable connection when directly connecting the ALR111 and the external device (RS-232C D-sub 25-pin)

Directly connecting to the external device with the RS-232C D-sub 9-pin connector

The following figure shows an example of the cable connections when directly connecting the ALR111 and the external device with the RS-232C D-sub 9-pin connector. The RS-232C cable should be less than 15 meters when directly connecting the ALR111 to the external device. If the cable is longer than 15 meters, you must connect through a modem.

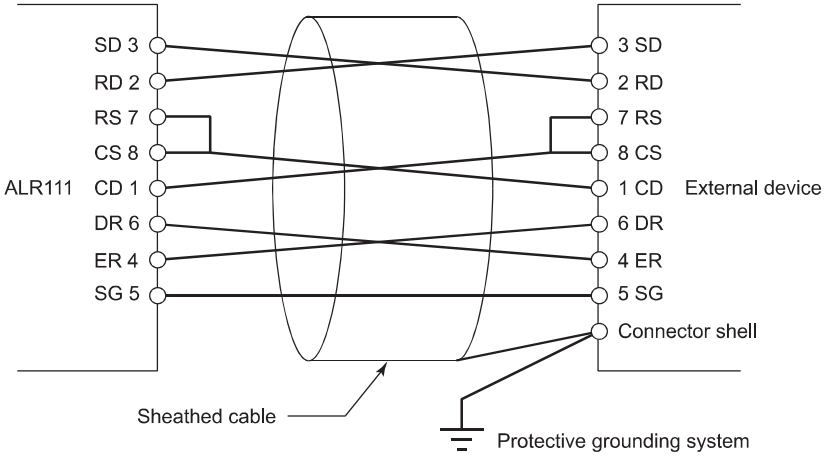


Figure D1.4.1-4 Cable connection when directly connecting the ALR111 and the external device (RS-232C D-sub 9-pin)

RS-232C communication module cables

The following table and figure show the RS-232C communication cables that are provided by our company.

Table D1.4.1-2 List of communication cables

Model	Cable Name	Remarks
AKB131	RS-232C Modem cable	Between the ALR111 and the modem (for RS circuit insulation) (9-25pin)
AKB132	RS-232C Null modem cable	Between the ALR111 and the RS-232C device (for RS circuit insulation) (9-25pin)
AKB135	RS-232C Modem cable	Between ALR111 to modem (9-25pin)
AKB136	RS-232C Null modem cable	Between ALR111 to RS-232C equipment (9-25pin)

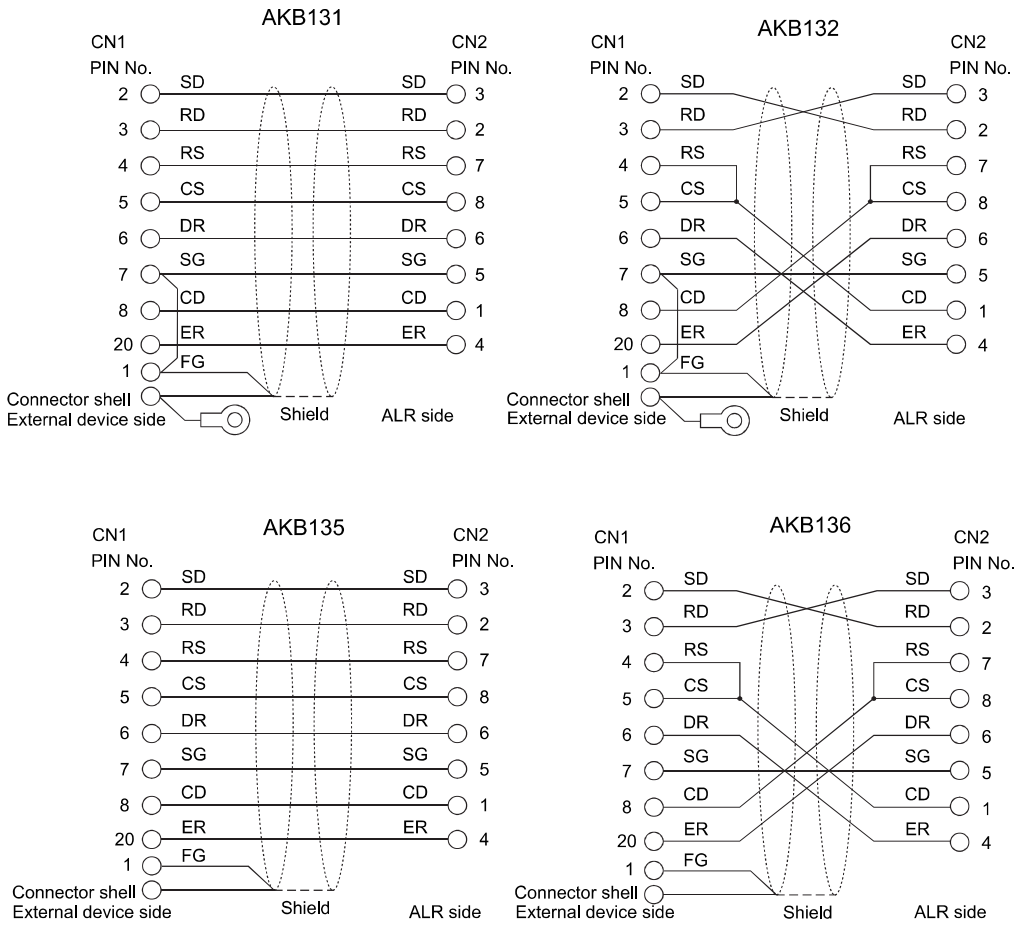


Figure D1.4.1-5 Internal connection of the RS-232C interface cable

FG connection of the RS-232C communication

IMPORTANT

The ALR111 isolates the RS-232C interface circuit. To improve noise resistance, the following requirements must be satisfied:

- On the external device side, connect the FG to the protective grounding system.
- Connect the FG to the SG of the RS-232C circuit (pin No. 7 for D-sub25, and pin No. 5 for D-sub9) at the external device.
- Ground the cable shielding wires at the external device side.
- If you use a cable that is not supplied by YOKOGAWA, the cable must be a twisted pair cable in which a signal wire and SG are paired.

The following figure shows an example of an FG connection.

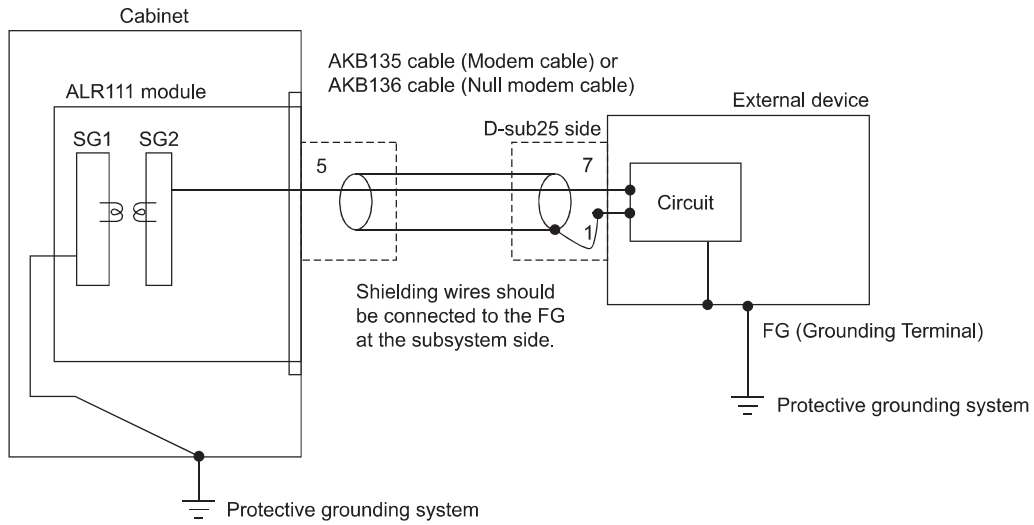


Figure D1.4.1-6 FG connection

When there is a short circuit on the external device side that uses a jumper pin on the FG and SG, you must short the circuit. The following figure shows an example of a short circuit that uses a jumper pin (J1).

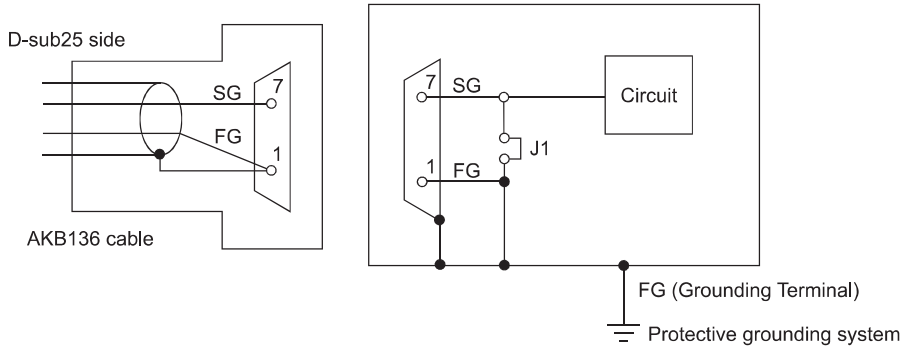


Figure D1.4.1-7 Example of a configuration with a jumper pin

FG connections that uses AKB131 and AKB132 cables

When the external device insulates the RS-232C communication circuit, communication circuits at both the ALR111 and external device are floating, and thereby lowering noise resistance severely. To prevent this, use an AKB131 or AKB132 cable.

You must forcibly connect pin No. 1 (for the frame ground) and pin No. 7 (for the signal ground) together at the external device side. When pin No. 1 (FG) is open at the external device, you must connect the cable shield to the FG terminal of the external device.

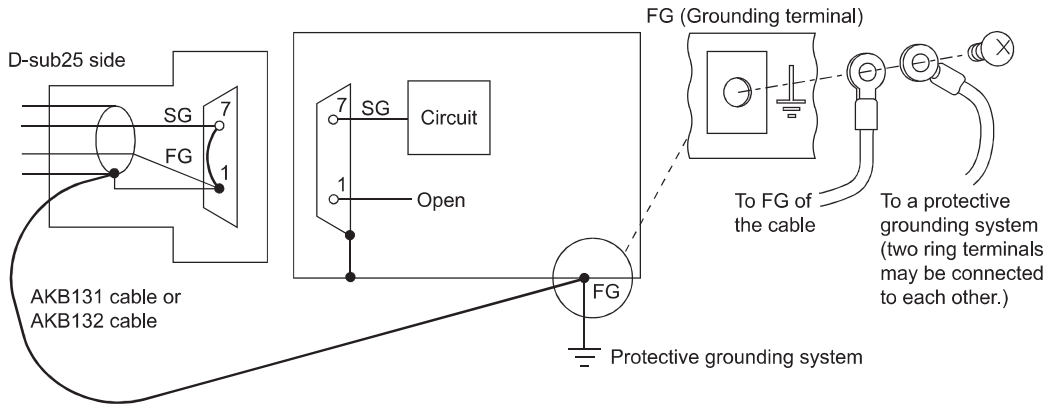


Figure D1.4.1-8 Cable connection for insulated communications circuit

D1.4.2 Connection of the serial communication module (RS-422/RS-485)

This section describes how to connect the communication cable of the serial communication module (RS-422/RS-485) (Model: ALR121).

The following figure shows the communication terminals.

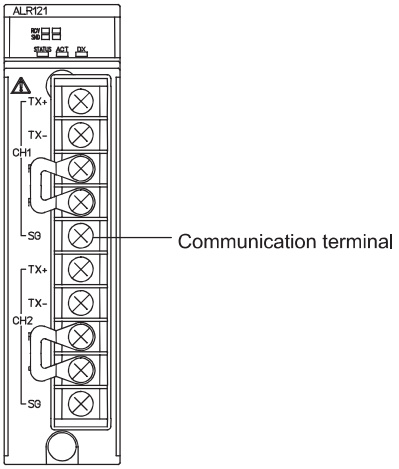


Figure D1.4.2-1 ALR121

The following table shows the terminal names and signal names of the communication terminals.

Table D1.4.2-1 RS-422/RS-485 interface terminal block placement

Terminal name	Signal name	Remarks
TX+	Send Data	Transmitting data (non-inverted)
TX-	Send Data	Transmitting data (inverted)
RX+	Receive Data	Receiving data (non-inverted)
RX-	Receive Data	Receiving data (inverted)
SG	Signal Ground	Signal ground

SEE ALSO

For more information about connections for each external device model when connecting to the ALR121, refer to:

The instruction manuals of the external devices

System configuration of ALR121 and external devices

When the external device acts as the master, 1 to 1 connections for a single ALR121 unit and 1 to n connections for multiple ALR121 units are available.

When the ALR121 acts as the master, 1 to 1 connections for a single external device unit and 1 to n connections for multiple external device units are available.

The maximum value for n is 32.

The following figure shows an example of the system configuration of the ALR121 and the external device.

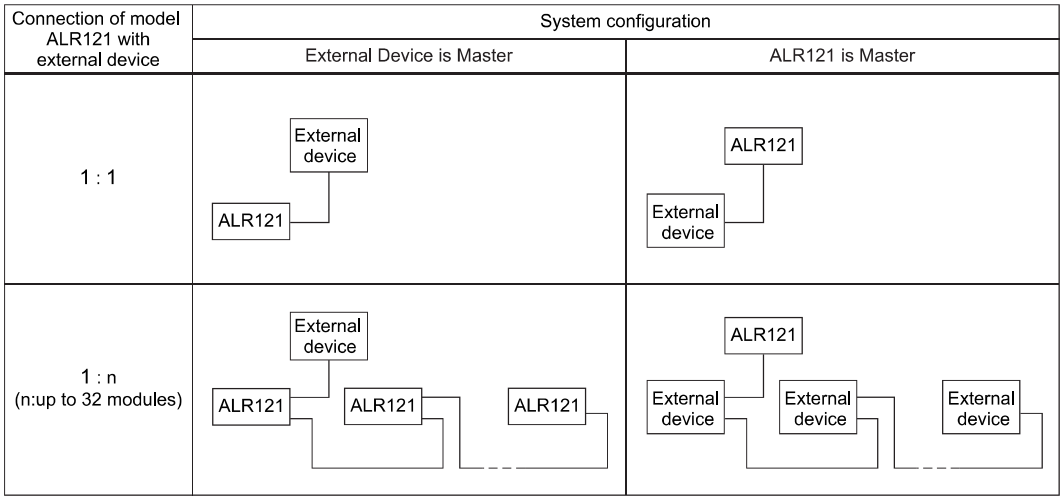


Figure D1.4.2-2 System configuration when connecting external device with model ALR121

RS-422/RS-485 communication cables

The following table shows the RS-422/RS-485 communication cables that are provided by YOKOGAWA.

Table D1.4.2-2 RS-422/RS-485 communication cables

Model	Cable Name	Remarks
AKB161	RS-422/RS-485 cable	Between the ALR (M4 terminal) and the external device (M3 terminal)
AKB162	RS-422/RS-485 cable	Between the ALR (M4 terminal) and the external device (M4 terminal)

FG connection of the RS-422/RS-485 communication cable

You must connect the FG to the protective grounding system on the external device side. You must connect the cable shield to the FG at the external device side. FG terminals are not available on the ALR121.

The following figure shows an example of an FG connection.

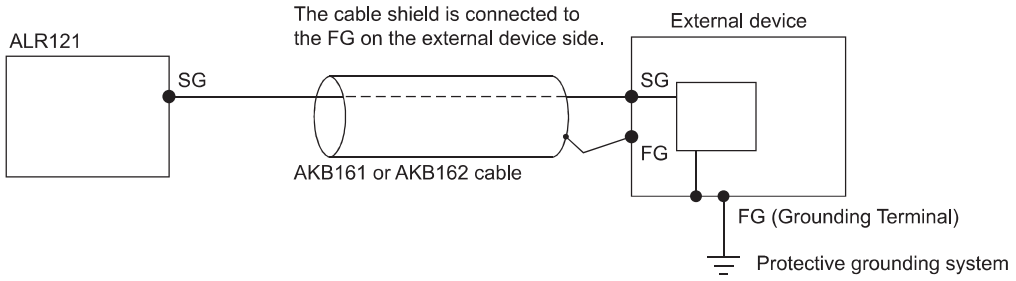
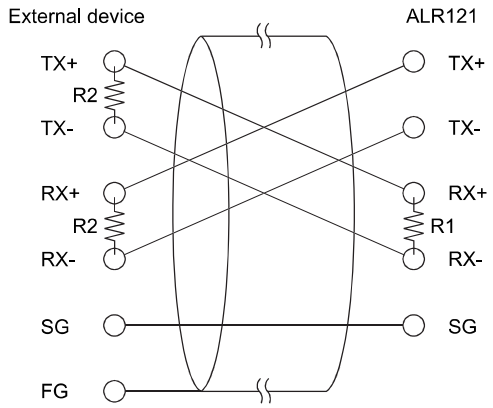


Figure D1.4.2-3 FG connection

Signal connections when the external device acts as the master

When the external device acts as the master, 1 to 1 connections for a single ALR121 unit and 1 to n connections for multiple ALR121 units are available. These connections are in four-wire type.

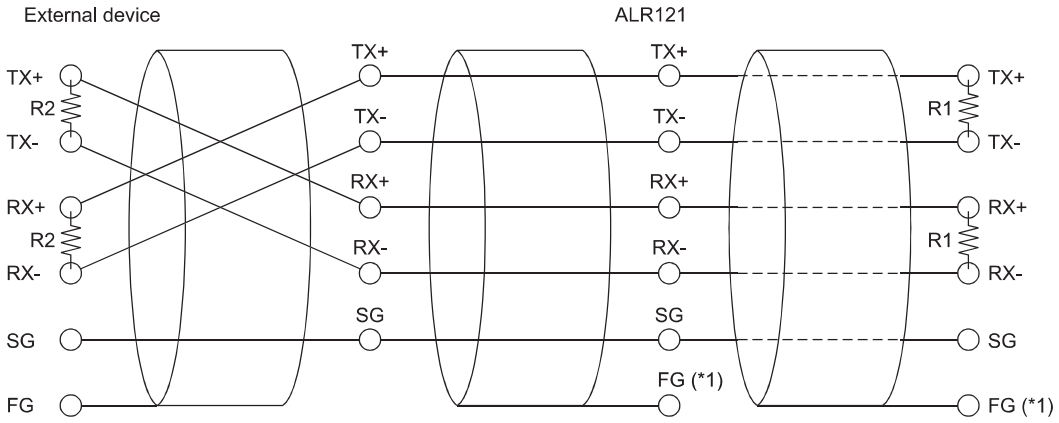
The following figure shows the 1 to 1 connection in four-wire type.



R1: Termination resistance of 120 ohm
R2: According to the instruction on the external device side

Figure D1.4.2-4 1 to 1 connection in 4-wire type

The following figure shows the 1 to n connection in four-wire type.



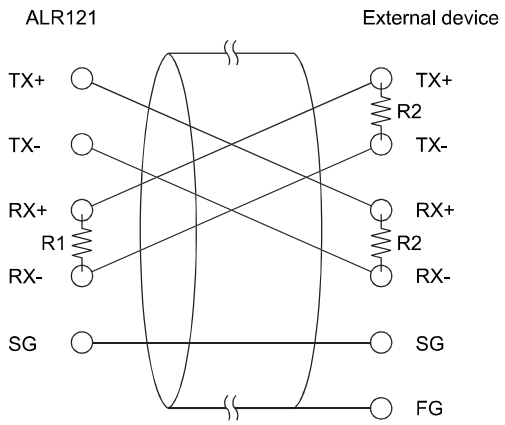
R1: Termination resistance of 120 ohm
R2: According to the instruction on the external device side
*1: Connect to the grounding terminal(FG) of the unit where ALR121 installed

Figure D1.4.2-5 1 to n connection in a four-wire type

Signal connections when the ALR121 acts as the master

When the ALR121 acts as the master, 1 to 1 connections for a single external device unit and 1 to n connections for multiple external device units are available. Four-wire and two-wire connections are supported.

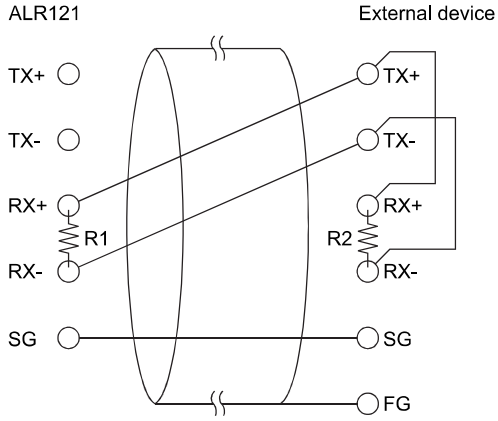
The following figure shows how to do a 1 to 1 connection in a four-wire type.



R1: Termination resistance of 120 ohm
R2: According to the instruction on the subsystem side

Figure D1.4.2-6 1 to 1 connection in 4-wire type

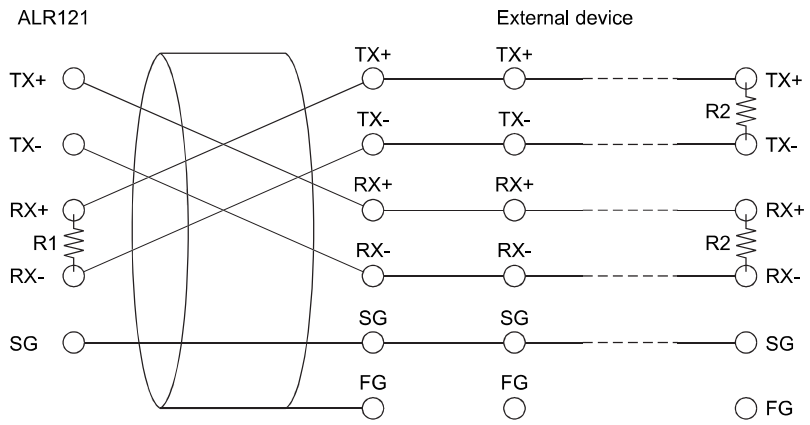
The following figure shows how to do a 1 to 1 connection in a two-wire type.



R1: Termination resistance of 120 ohm
R2: According to the instruction on the subsystem side

Figure D1.4.2-7 1 to 1 connection in a 2-wire type

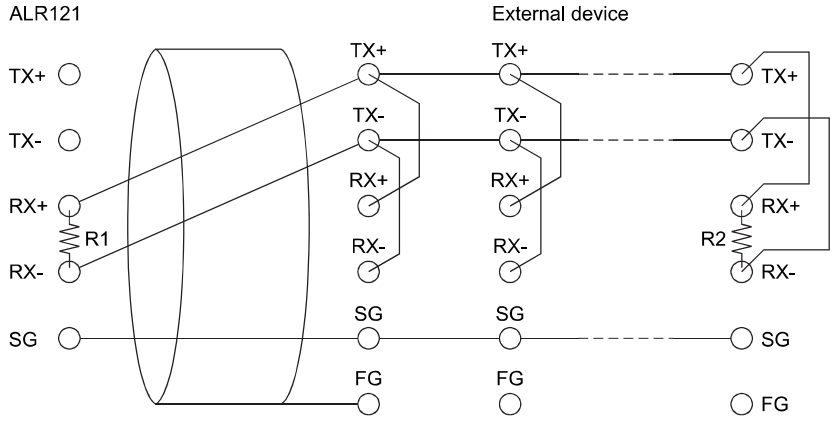
The following figure shows how to do a 1 to n connection in a four-wire type.



R1: Termination resistance of 120 ohm
R2: According to the instruction on the subsystem side

Figure D1.4.2-8 1 to n connection in a four-wire type

The following figure shows how to do a 1 to n connection in a two-wire type.



R1: Termination resistance of 120 ohm
R2: According to the instruction on the subsystem side

Figure D1.4.2-9 1 to n connection in a two-wire type

D1.4.3 Signal connection of the Ethernet communication module

The signal connection of the Ethernet communication modules (model name: ALE111) uses 10BASE-T twisted-pair cables. The communication connector type is RJ-45.

The following figure shows the position of the communication connector.

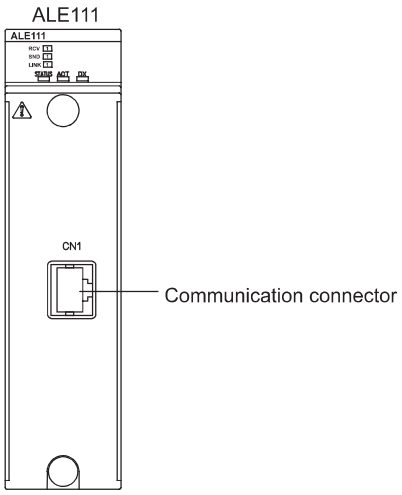


Figure D1.4.3-1 Ethernet communication module

D1.4.4 Connection of the fire and gas communication module

For signal connection of the fire and gas communication module (Model: S2LP131), use a PROFINET-compliant cable and connector. The communication connector type is RJ-45.

The following figure shows the position of the communication connector.

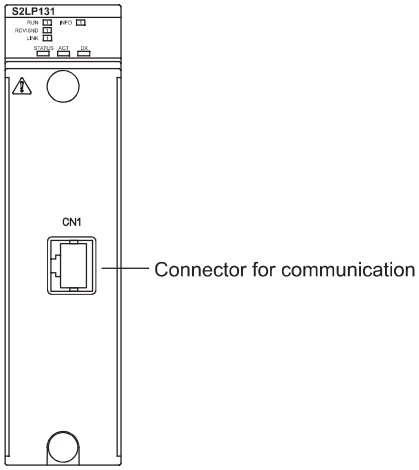


Figure D1.4.4-1 Fire and gas communication module

SEE ALSO For more information about the cable specifications, refer to:

ProSafe-RS Fire and Gas Communication Module (GS 32P06K52-01EN)

D2. Signal wiring between an N-IO I/O unit and field devices

This section describes the signal wiring between the N-IO I/O unit and field devices. Signal connection is available by directly connecting signal cables of field device to the base plate for N-IO I/O unit or by connecting through a terminal board.

If you want to connect directly, connect the signal cables to the terminal block of the base plate or to the signal terminals of barriers.

If you want to connect through a terminal board, use a dedicated signal cable to connect a connector type of base plate with disconnecting terminals with a terminal board and connect the signal cables with field wiring terminals of the terminal board.

SEE ALSO For more information about the electrical specifications of signals, refer to:

ProSafe-RS I/O Module (for N-IO) (GS 32P06K30-01EN, GS 32P06K31-01EN)

Connecting a base plate and a terminal board

When you connect a connector type of base plate with disconnecting terminals with a terminal board, you must use dedicated cables (Model: AKB331, AKB651). Connect the shield cable of the signal cable to the grounding terminal for shield cable on the base plate.

The following figure shows the connection of a base plate and a terminal board.

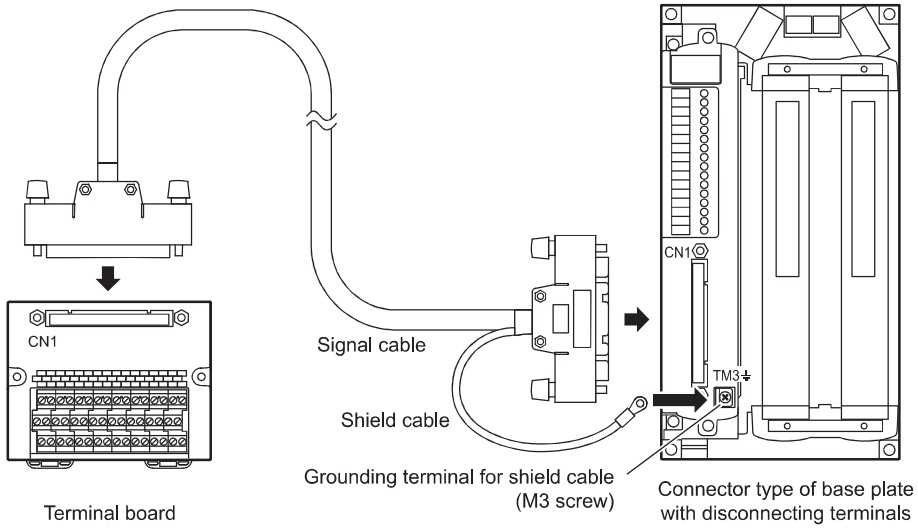


Figure D2-1 Connecting a base plate and a terminal board

SEE ALSO For more information about the signal cable specifications, refer to:

- ProSafe-RS/ProSafe-RS Lite Cables (GS 32Q06M10-31E)
- ProSafe-RS Base Plate (for N-IO) (GS 32P06K20-01EN)

Connecting to a base plate

Follow these steps to connect a signal cable to a connector type of base plate with disconnecting terminals:

1. Insert the signal cable to the signal cable connector of a base plate and tighten it with two screws on the cable.

2. Connect the shield cable to the grounding terminal for shield cable on a base plate.
   An M3 screw is used for the grounding terminal.

Connecting to a terminal board

Follow this step to connect a signal cable to a terminal board.

- Insert the signal cable to the signal cable connector of a terminal board and tighten it with two screws on the cable.

Signal wiring cables

Recommended cable thickness is 0.5 to 2.5 mm^2. When spring clamp terminals are used with sleeves, the cable thickness should be 1.5 mm^2 at maximum.

SEE ALSO For more information about examples of compatible lines for signal wiring, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

Cable termination

IMPORTANT

- Use sleeves that conform to the following DIN standards.
  - Sleeves without insulating cover: DIN 46 228/1
  - Sleeves with insulating cover: DIN 46 228/4
- Use sleeves and a tool that are of the same make and match the thickness of the wire.
- Insert the cables deep into the terminals and make sure they are securely installed.
- Fasten the cables securely to cable clamps or the like so that the terminals do not need to carry the weight of the cables.

At the end of the signal cables to the base plate, provide the following cable termination:

- When using a sleeve
  At the cable end, peel off the coating and attach a sleeve. The sleeve dimensions differ depending on the cable thickness. You must provide cable termination according to the following figure and table:

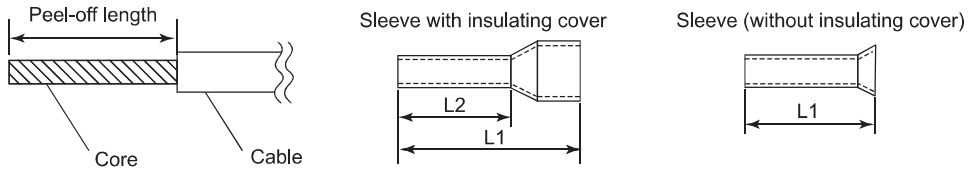


Figure D2-2 Cable termination (for pressure clamp terminals)

Table D2-1 Sleeve dimensions

Cable thickness (mm^2)	When using a sleeve with insulating cover			When using a sleeve (without insulating cover)	
	Peel-off length (mm)	Sleeve dimensions (mm)		Peel-off length (mm)	Sleeve dimensions (mm)
		L1	L2		L1
0.5	10	14	8	6	6

Continues on the next page

Table D2-1 Sleeve dimensions (Table continued)

Cable thickness (mm^2)	When using a sleeve with insulating cover			When using a sleeve (without insulating cover)	
	Peel-off length (mm)	Sleeve dimensions (mm)		Peel-off length (mm)	Sleeve dimensions (mm)
		L1	L2		L1
0.75	10	14	8	6	6
1.0	10	14	8	6	6
1.5	10	14	8	7	7
2.5	10	14	8	7	7

- When not using a sleeve
  The peel-off length should be 8 mm for pressure clamp terminals and 7 mm for spring clamp terminals. The peel-off length should be 7 mm for a terminal board (for N-IO).

TIP

It is recommended to use a sleeve when you connect a cable with a thickness smaller than 1 mm^2 to a spring clamp terminal.

Connecting to pressure clamp terminals

IMPORTANT

- When you connect cables to pressure clamp terminals, use a flat-blade screwdriver that conforms to the DIN 5264B standard having a thickness at the tip of 0.6 mm and a body shaft diameter of 3.5 mm.
- Do not overstress the pressure clamp terminals with a tool such as a driver.
- The screw tightening torque of the pressure clamp terminals should be 0.5 to 0.6 N·m.
- Fasten the cables securely to cable clamps or the like so that the terminals do not need to carry the weight of the cables.

Follow these steps to connect cables to pressure clamp terminals:

1. Insert the cables to the pressure clamp terminals and tighten the screws.
2. Pull the cable gently to check that it is fixed securely.

TIP

The terminal type of base plate with disconnecting terminals has a cover on its terminal block. Close the cover during operation.

Connecting to spring clamp terminals

IMPORTANT

Fasten the cables securely to cable clamps or the like so that the terminals do not need to carry the weight of the cables.

Follow these steps to connect cables to spring clamp terminals:

1. Expand the spring clamp terminal by using a flat-blade screwdriver.
2. Insert a cable without pulling out the screwdriver.

3. Pull out the flat-blade screwdriver.
4. Pull the cable gently to check that it is fixed securely.

TIP

The terminal type of base plate with disconnecting terminals has a cover on its terminal block. Close the cover during operation.

D2.1 Signal connection to the base plate with disconnecting terminals

For signal connections to the base plate with disconnecting terminals (Model: S2BN1D), you must connect analog or digital I/O signals to the connection terminal on a base plate or a terminal board and configure the signal types by using the software.

For a terminal type base plate, connect the signal cables of field devices to the terminal blocks of a base plate. You cannot connect signals that use a terminal C because the terminal blocks do not have a terminal C. The following figure shows the terminal numbers of the terminal block.

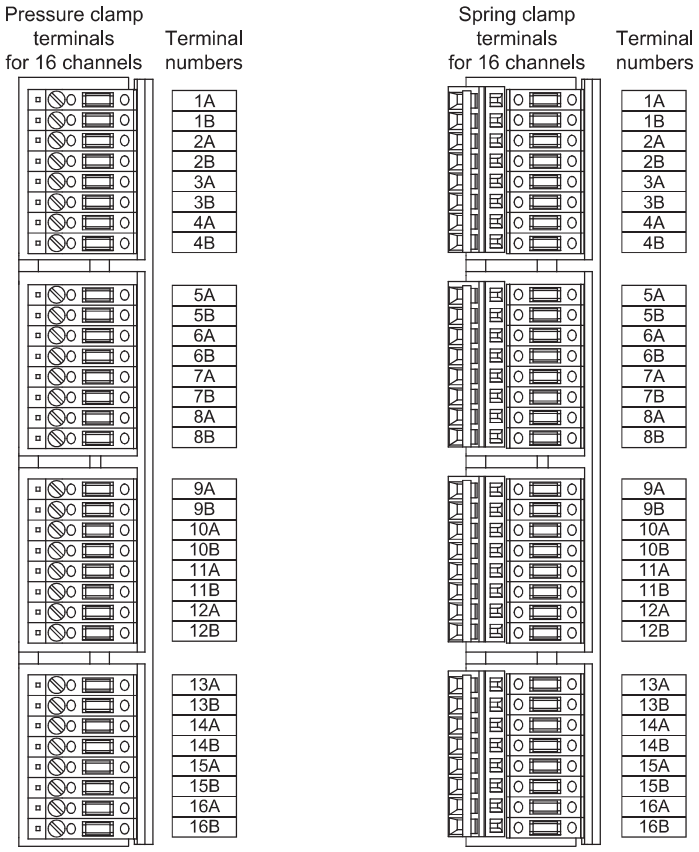


Figure D2.1-1 Terminal numbers of the terminal block

For a connector type base plate, use a dedicated signal cable to connect the base plate to a terminal board and connect the signal cables to field wiring terminals of the terminal board. The following figure shows the field wiring terminals of a terminal board.

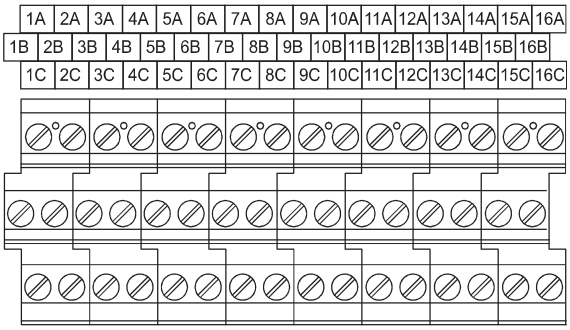


Figure D2.1-2 Field wiring terminals of a terminal board.

The following table shows the relationship between signal types and terminal numbers of channels.

Table D2.1-1 Terminal numbers and signal types

Configuration	Terminal number (*1)	Signal type (*2)(*3) (*4)(*5)			
Analog input Analog output	□A	2-wire transmitter input +	4-wire current input +	Current output +	3-wire current input +
	□B	2-wire transmitter input -	4-wire current input -	Current output -	3-wire current input -
	□C	NC	NC	NC	3-wire power supply +
Digital input Digital output	□A	Dry contact input +	Voltage output +	-	-
	□B	Dry contact input -	Voltage output -	-	-
	□C	NC	NC	-	-

*1: □: 1 to 16
*2: NC: Not to be connected
*3: For 3-wire current input, you must connect the field power supply to the base plate and specify 4-wire as the connection type by using the software.
*4: For voltage output, you must connect the field power supply to the base plate.
*5: -: Not applicable

Signal connections of analog I/O signals

The following figure shows the connection of an analog I/O signal.

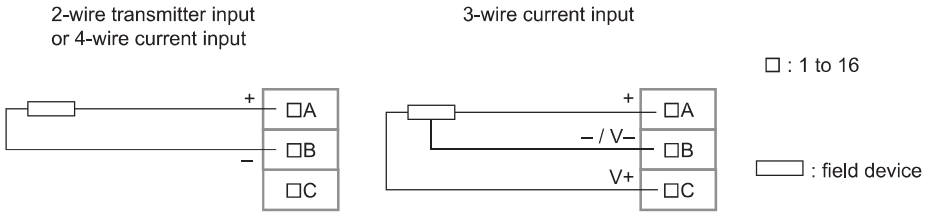


Figure D2.1-3 Connecting an analog I/O signal

You can use 3-wire current input for a connector type base plate. For 3-wire current input, you must connect the field power supply to the base plate and specify 4-wire as the connection type by using the software.

Signal connections of digital input signals

The following figure shows the connection of a digital input signal.

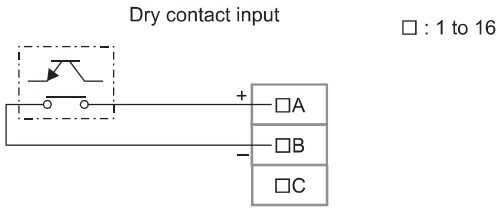


Figure D2.1-4 Connecting a digital input signal

Signal connections of digital output signals

The following figure shows the connection of a digital output signal. You must connect the field power supply to the base plate.

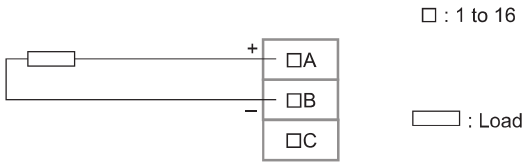


Figure D2.1-5 Connecting a digital output signal

CAUTION

If you connect an inductive load to the base plate in which S2MMM843 or S2MDV843 of style S1 is installed, you must connect a diode in parallel with the load to protect the contact.

The following figure shows an example of signal connection for high current output where an external terminal block is used. You can connect 2 or 3 channels in parallel.

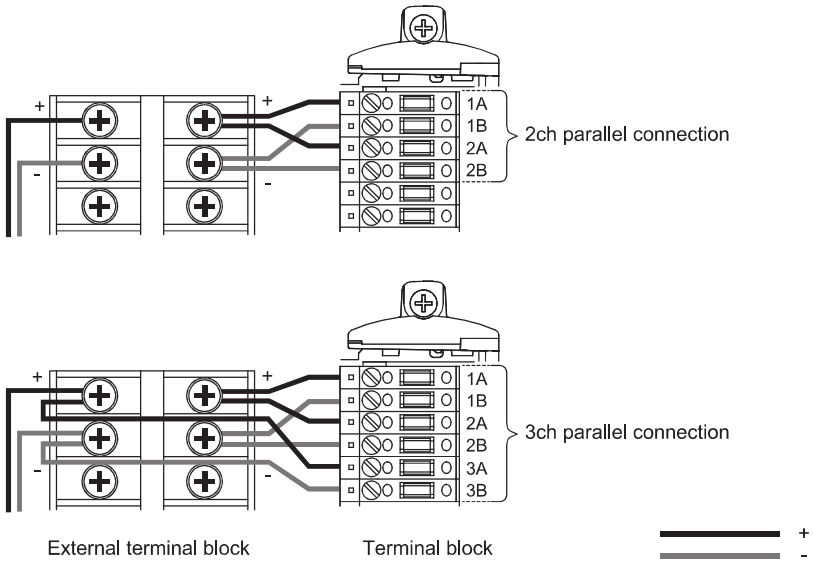


Figure D2.1-6 Example of signal connection when using the high current output function

SEE ALSO

For more information about connecting diodes when using an inductive load, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

For more information about settings on the I/O Parameter Builder when using high current output function, refer to:

"■ Changing the signal category of channels (only for universal type I/O modules)" in E1.6, "Precautions for online change download of N-IO" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about signal connections when using high current output function, refer to:

ProSafe-RS Installation Guidance (TI 32P01J10-01EN)

D2.2 Signal connections of the base plate for barrier: S2BN4D

CAUTION

The signal wiring to the field devices that is intrinsic safety circuits must be installed so that they are electrically separated from the wiring of non-intrinsic safety circuits, including the in-cabinet wiring. You must install the wiring according to the IEC 60079-14 standards or the requirements for explosion-proof wiring of the country where the system is used.

There are no signal terminals installed in the base plate for barrier (Model: S2BN4D). Signal terminals are installed in the intrinsic safety barriers.

SEE ALSO For more information about type of intrinsic safety barrier, refer to:

Base Plates for Barrier (for N-IO) (GS 32P06P10-01EN)

D2.3 Signal connections to the base plate for barriers: S2BN5D

CAUTION

The signal wiring to the field devices that is intrinsic safety circuits must be installed so that they are electrically separated from the wiring of non-intrinsic safety circuits, including the in-cabinet wiring. You must install the wiring according to the IEC 60079-14 standards or the requirements for explosion-proof wiring of the country where the system is used.

The following figure shows the signal terminal numbers of S2BN5D.

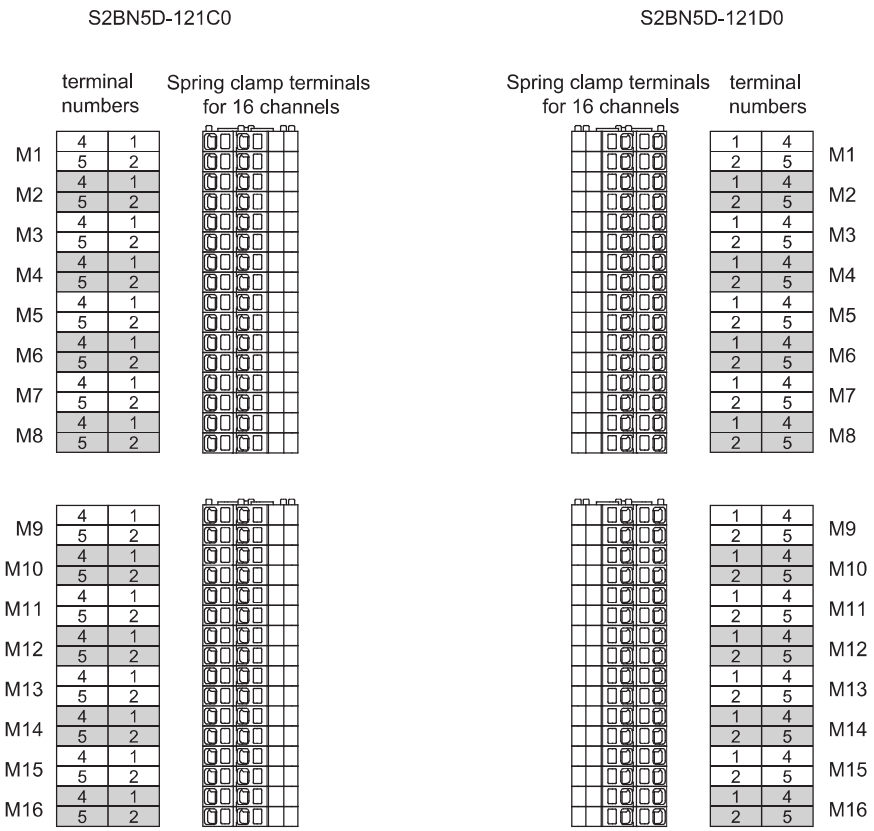


Figure D2.3-1 Signal terminal numbers of S2BN5D

In signal connections to the base plate for barriers (model name: S2BN5D), signal cables must be connected to different terminals depending on the type of signals. To prevent damage to devices, you must connect signal cables to the appropriate terminals depending on the type of signals.

The following table shows the relationship between signal types and terminal numbers of channels.

Table D2.3-1 Terminal numbers and signal types

Intrinsic safety barriers	Terminal number	Signal type(*1)					
For analog input	1	Two-wire transmitter input +	Current input +	---	---	---	---
	2	---	---	---	---	---	---
	4	Two-wire transmitter input -	---	---	---	---	---
	5	---	Current input -	---	---	---	---
For analog output	1	Analog output +	---	---	---	---	---
	2	---	---	---	---	---	---
	4	Analog output -	---	---	---	---	---
	5	---	---	---	---	---	---
For digital input	1	Digital input +	---	---	---	---	---
	2	---	---	---	---	---	---
	4	Digital input -	---	---	---	---	---
	5	---	---	---	---	---	---
For digital output	1	Digital output +	---	---	---	---	---
	2	---	---	---	---	---	---
	4	Digital output -	---	---	---	---	---
	5	---	---	---	---	---	---
For temperature input	1	RJC connection	---	RTD four-wire type current source +	RTD three-wire type current source +	RTD two-wire type current source +	Skid resistance current source +
	2	Thermocouple input +	Voltage input +	RTD four-wire type input +	---	---	---
	4	RJC connection	---	RTD four-wire type current source -	RTD three-wire type current source -	RTD two-wire type current source -	Skid resistance current source -
	5	Thermocouple input -	Voltage input -	RTD four-wire type input -	RTD three-wire type input -	---	Skid resistance input -

*1: "- - -" denotes that the terminal is not used. Do not connect any signal to it.

SEE ALSO For more information about type of intrinsic safety barrier, refer to:

Base Plates for Barrier (for N-IO) (GS 32P06P10-01EN)

D3. Signal connection of the external alarm input terminals of the node interface unit

The external alarm input terminals that are provided on the base plate for node interface unit are pressure clamp terminals. For the signal wiring, use cables with a nominal cross-sectional area of 0.5 to 2.5 mm^2.

SEE ALSO For more information about the specifications of the signal for the external alarm input, refer to:

ProSafe-RS Node Interface Unit (for N-IO) (GS 32P06F20-01EN)

Cable termination

IMPORTANT

- Use sleeves that conform to the following DIN standards:
  - Sleeves without insulating cover: DIN 46 228/1
  - Sleeves with insulating cover: DIN 46 228/4
- Use sleeves and a tool from the same manufacturer that match the thickness of the wire.
- Insert the cables deep into the terminals and make sure they are securely installed.

At the end of the signal cables to the base plate, provide the following cable termination:

- When using a sleeve
  At the cable end, peel off the coating and attach a sleeve. The sleeve dimensions differ depending on the cable thickness. You must provide cable termination according to the following figure and table:

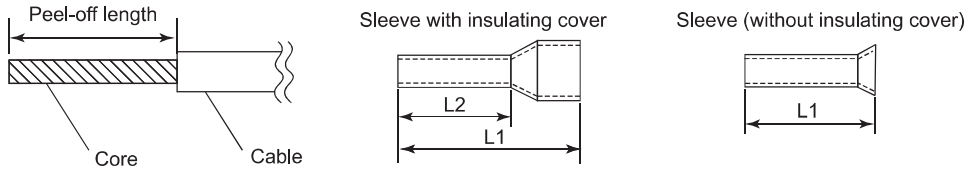


Figure D3-1 Cable termination

Table D3-1 Sleeve dimensions

Cable thickness (mm^2)	When using a sleeve with insulating cover			When using a sleeve (without insulating cover)	
	Peel-off length (mm)	Sleeve dimensions (mm)		Peel-off length (mm)	Sleeve dimensions (mm)
		L1	L2		L1
0.5	10	14	8	6	6
0.75	10	14	8	6	6
1.0	10	14	8	6	6
1.5	10	14	8	7	7
2.5	11	14	8	7	7

- When not using a sleeve
  The peel-off length should be 8 mm.

Connecting to pressure clamp terminals

IMPORTANT

- When you connect cables to pressure clamp terminals, use a flat-blade screwdriver that conforms to the DIN 5264B standard having a thickness at the tip of 0.6 mm and a body shaft diameter of 3.5 mm.
- The screw tightening torque of the pressure clamp terminals should be 0.4 to 0.5 N·m.

Follow these steps to connect cables to pressure clamp terminals:

1. Confirming the cable polarity, insert the cable to the pressure clamp terminal and tighten the screw.
2. Pull the cable gently to check that it is fixed securely.

E. Maintaining the SCS

This section describes the following maintenance work for the SCS:

- Routine maintenance
- Parts with defined life spans and replacement parts
- Replacing the component devices

CAUTION

- When the power is on, do not install or remove any devices, cables, or connectors unless it is clearly stated in this manual that you are allowed to do so.
- When performing maintenance work, wear a wrist strap to take measure against electrostatic discharge (ESD).

IMPORTANT

If dust or dirt is found on the devices, clean them with a vacuum cleaner or dry soft cloth. If the stain is tough and cannot be removed easily, wipe it with soft cloth soaked in water or mild soap water after wringing it tightly.

E1. Precautions during maintenance work

This section describes the precautions that you must take during maintenance work.

Precautions against static electricity during maintenance work

When performing maintenance work, observe the following precautions to prevent electrostatic interference.

- When storing or carrying maintenance parts, be sure to enclose them in an antistatic bag.

TIP For shipment, these parts are enclosed in an antistatic bag labeled with precautions against electrostatic charge.

- During maintenance work, wear a wrist strap with a 1 M ohm grounding resistor. Connect the wrist strap to the grounding terminal or unpainted part of the grounded frame.
- When working on a bench, place the parts or device on a conductive sheet that is grounded through a 1 M ohm resistor. While you work, you must wear a wrist strap. Keep away any plastic and other materials that can easily be charged from the work bench.
- Do not touch any maintenance parts without using a wrist strap or conductive sheet.
- During the maintenance work for S2CP471/L1CP471 on a conductive sheet, remove the battery. During the maintenance work for SCP461 or SCP451, turn off the battery ON/OFF switch or remove the battery.

The following figure shows an example of using a wrist strap and conductive sheet.

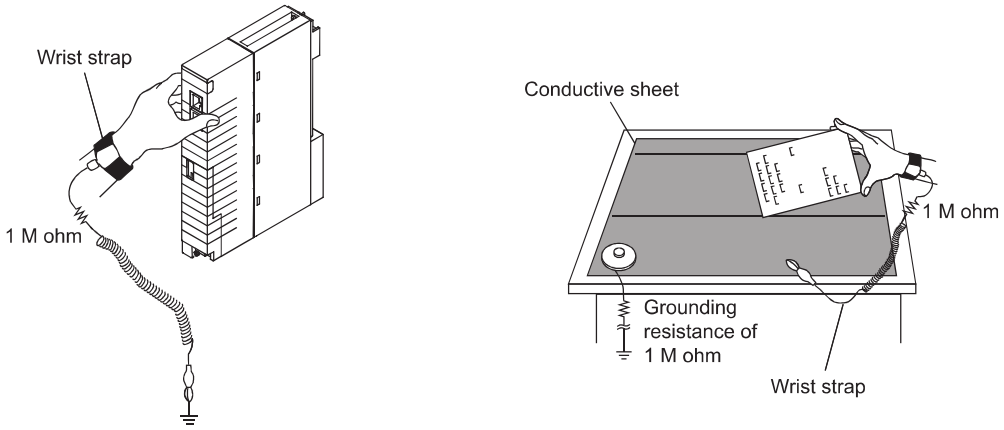


Figure E1-1 Example of using a wrist strap and conductive sheet

Precautions when maintaining node units that are connected on N-ESB bus or optical ESB bus

In the following explanation, N-IO nodes, safety node unit (SNU), and unit for optical ESB bus repeater module are collectively called node units.

- The N-ESB bus modules that are mounted on an N-IO node have the function to relay communications on the N-ESB bus or optical ESB bus. If both N-ESB bus modules fail or power to the N-ESB bus modules fails, not only the N-IO node but also the node units that are connected under that N-IO node become unable to communicate with the SCU. Therefore, you must be careful when you turn off the power to the N-IO nodes.

- If both optical ESB bus repeater modules, which are mounted on an SNU or a unit for optical ESB bus repeater module, fail or power to the optical ESB bus repeater modules fails, not only the node unit but also the node units that are connected under that node unit become unable to communicate with the SCU. Therefore, you must be careful when you turn off the power to the SNUs or units for optical ESB bus repeater module.
- If an error occurs on one of the paired power supply modules that are mounted on a unit for optical ESB bus repeater module, a notification is provided as an error of an ESB bus interface module that is mounted on a lower-level node unit of this node unit.

SEE ALSO

For more information about behaviors when an error occurs on one of the paired power supply modules of a unit for optical ESB bus repeater module, refer to:

G2.2.7, “Actions taken at error occurrence for optical ESB bus repeater devices” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

E2. Routine maintenance

You can perform routine maintenance by visually checking the status lamps of the equipment or by checking the SCS State Management window.

SEE ALSO For more information about the SCS State Management window, refer to:

H1.2, “SCS State Management window” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Inspection by checking status lamps

The following table describes the status lamps that you can refer to in order to determine normal or error status of the devices.

Table E2-1 Status lamps and operating status of the devices

Device	Lamp	Redundancy setting	Normal	Error	Remarks
Power supply module	SYS	-	On	Off	Indicates the status of +5 V output.
	FLD	-	On	Off	Indicates the status of +24 V output.
Processor module	HRDY	-	On	Off	Indicates the hardware status.
	RDY	-	On	Off	Indicates the status of hardware and software.
	CTRL	Redundant	On (active module) Off (standby module)	Off (active module) (*1)	Indicates the control status.
		Non-redundant	On	Off	
ESB bus interface module	STATUS	-	On	Off	Indicates the hardware status.
Optical ESB bus repeater module	STATUS	-	On	Off	Indicates the hardware status.
N-ESB bus coupler module	RDY	-	On	Off	Indicates the hardware status.
FIO I/O module	STATUS	-	On	Off	Indicates the hardware status.
	ACT	Redundant	On (active module) Off (standby module)	Off (active module) (*2)	Indicates the operating status. (*3)
		Non-redundant	On	Off	

Continues on the next page

Table E2-1 Status lamps and operating status of the devices (Table continued)

Device	Lamp	Redundancy setting	Normal	Error	Remarks
Serial communication module Ethernet communication module	STATUS	-	On	Off	Indicates the hardware status.
	ACT	Redundant	On (active module) Off (standby module)	Off (active module) (*2)	Indicates the operating status.
		Non-redundant	On	Off	
	DX	Redundant	On	Off	Indicates the status in dual-redundant configuration. The lamp is always off in single configuration.
	LINK	-	On	Off	Indicates the link status.
Fire and gas communication module	STATUS	-	On	Off	Indicates the hardware status.
	ACT	-	On	Off	Indicates the operating status.
	RUN	-	On	Off	Indicates the communication status.
	LINK	-	On	Off	Indicates the link status.
	INFO	-	Off	On or flashing	Indicates the communication setting status.
Power supply unit (N-IO)	POWER	-	On	Off	-
N-ESB bus module	STAT	-	On	Off	Indicates the hardware status.
Base plate with disconnecting terminals	FUSE STATUS	-	Off	On	Indicates the fuse status.
N-IO I/O module	STATUS	-	On	Flashing or off	Indicates the hardware status.
	Channel status (for DIO)	-	On (active module, when DIO is on) Off (active module, when DIO is off) Off (standby module)	Flashing (*4)	Indicates the on/off status or wiring error for each channel.

*1: The CTRL lamp goes off when an error occurs in the active module. The standby module takes over to become the active module.
*2: The ACT lamp goes off when an error occurs in the active module. The standby module takes over to become the active module.
*3: The ACT lamp turns off while the current input module (SAI143 style S4 or later/L1AI143) is resetting the error detection status of Smoke and Heat Detector.
*4: When a wiring error is detected, the corresponding channel status lamp flashes.

SEE ALSO

For more information about the descriptions related to status lamps of the devices, refer to:

- B4., “FIO node devices” on page B4-1
- B5., “N-IO node devices” on page B5-1

For more information about the function to reset the error detection status of Smoke and Heat Detector by the current input module (SAI143 style S4 or later/L1AI143), refer to:

A3.4.1, “Device reset function with FIO” in Engineering Guide Vol. 2 (IM 32P01C20-01EN)

E3. Parts with defined life spans and replacement parts of SCS

The SCS has parts with defined life spans that must be replaced periodically and replacement parts such as fuses.

The parts with defined life spans that can be replaced by the customer are available as spare parts or consumables. Purchase and replace them as necessary.

IMPORTANT

Precautions for parts with defined life spans

- The term “parts with defined life spans” refers to parts that are expected to wear out or break down within 10 years from initial use under normal conditions of use. Therefore, parts with expected life spans of 10 years or more are excluded here.
- The recommended replacement cycle is the cycle estimated for preventive maintenance. It provides no guarantee against the accidental failures.
- The recommended replacement cycle is merely a reference, and varies depending on the usage conditions.
- The recommended replacement cycle is subject to change according to actual field results.

Periodic replacement parts with defined life spans

The following tables describe the recommended replacement cycles of the parts with defined life spans.

Table E3-1 Recommended replacement cycles of parts with defined life spans for FIO nodes (excluding relay boards)

Part name	Part number	Recommended replacement cycle	Replacement by user	Remarks
Power supply module (100-120 V AC)	SPW481/ L1PW481	8 years	Yes	At the average ambient temperature (*1) of 40 deg. C or lower
Power supply module (220-240 V AC)	SPW482/ L1PW482	8 years	Yes	At the average ambient temperature (*1)of 40 deg. C or lower
Power supply module (24 V DC)	SPW484/ L1PW484	8 years	Yes	At the average ambient temperature (*1)of 40 deg. C or lower
Battery (for S2CP471 or L1CP471)	S9450FE	3 years (*2)	Yes	At the average ambient temperature of 30 deg. C or lower
		1.5 years (*2)	Yes	At the average ambient temperature of 50 deg. C or lower
		1 year (*2)	Yes	At the average ambient temperature of 70 deg. C or lower
Battery (for SCP461 or SCP451)	S9185FA	3 years (*2)	Yes	At the average ambient temperature of 30 deg. C or lower
		1.5 years (*2)	Yes	At the average ambient temperature of 40 deg. C or lower
		9 months (*2)	Yes	At the average ambient temperature of 50 deg. C or lower

Continues on the next page

Table E3-1 Recommended replacement cycles of parts with defined life spans for FIO nodes (excluding relay boards) (Table continued)

Part name	Part number	Recommended replacement cycle	Replacement by user	Remarks
Aluminum electrolytic capacitor (in a power supply module)	-	8 years	No (*3)	For SPW48□/L1PW48□ At the average ambient temperature of 40 deg. C or lower
Fuse (in a power supply module)	-	8 years	No (*3)	For SPW48□/L1PW48□
Fan unit	AIP602	4 years	Yes	At the average ambient temperature of 60 deg. C or lower
Power supply unit for fan unit	S9159FA	8 years	Yes	100-120 V AC, 220-240 V AC At the average ambient temperature of 40 deg. C or lower
	S9160FA	8 years	Yes	24 V DC At the average ambient temperature of 40 deg. C or lower
Optical ESB bus repeater module (Style S1 only)(*4)	SNT401	4 years	Yes	This cycle assumes the use in G3 environments.
	SNT501			
	L1NT401			
	L1NT501			
	L1NT411			
	L1NT511			
Optical ESB bus repeater module (Style S1 and S2)(*5)	SNT411	4 years	Yes	This cycle assumes the use in G3 environments.
	SNT511			

*1: The ambient temperature when the FIO node is installed in a cabinet is the temperature inside the cabinet, not outside the cabinet.
*2: The replacement cycle for batteries includes the period during which the batteries remain unused.
*3: Parts indicated by a "No" in the "Replacement by user" column cannot be replaced by the user, so please contact YOKOGAWA sales or service agents to request replacement work.
*4: Not applicable to styles S2 and later.
*5: Not applicable to styles S3 and later.

Table E3-2 Recommended replacement cycles of parts with defined life spans for N-IO nodes

Part name	Model	Recommended replacement cycle	Replace-ment by user	Remarks
Power supply unit (100-240 V AC input)	S2PW503	8 years	Yes	At the average ambient temperature (*1) of 40 deg. C or lower
Power supply unit (24 V DC input)	S2PW504	8 years	Yes	At the average ambient temperature (*1)of 40 deg. C or lower
N-ESB bus module (Style S1 only)(*2)	S2EN501-S1□□□□	4 years	Yes	This cycle assumes the use in G3 environments.
	S2EN501-S2□□□□			
	S2EN501-S□1□□□			
	S2EN501-S□2□□□			

*1: The ambient temperature when the N-IO node is installed in a cabinet is the temperature inside the cabinet, not outside the cabinet.
*2: Not applicable to styles S2 and later.

The relays that are used in relay boards have defined service lives. The following table shows the switching service lives of relays.

Table E3-3 Switching service lives of relays used in relay boards

Model	Style number	Part number	Switching service life	Remarks
SRM53D	S1 and later	A1772MR	100000 times on/off	-
SRM54D				
SBM54D	S1, S2	A1589MR	100000 times on/off	4 A with a resistive load
	S3 and later	A1893MR	100000 times on/off	3 A with a resistive load
			75000 times on/off	4 A with a resistive load

E3.1 Replacing the battery of the processor module

This section describes replacement of battery placed in the processor module.

CAUTION

- Use only the battery specified by Yokogawa Electric Corporation.
- Wear a wrist strap when handling a battery.

IMPORTANT

- Replace the battery before the validity period expires.
- Order a new battery at least one month before the validity period expires.
- Do not short-circuit the battery terminals.
- Do not heat the battery or throw the battery in a fire. The problems of leaking, overheating or breaking may occur.
- Do not disassemble or modify the battery.
- Do not use the battery to the products other than YOKOGAWA designated devices.
- When discarding the battery, you must handle it very carefully to avoid polluting environment.

SEE ALSO For more information about the processor modules, refer to:

B4.2, “Processor module” on page B4-4

Battery expiration date label

You can check the expiration date of the battery on the label that is affixed to the front cover of the processor module. Keep in mind that the average ambient temperature affects the battery life.

The following figure shows the battery life label.

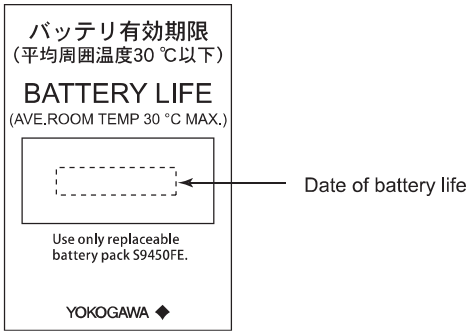


Figure E3.1-1 Example of the battery expiration date label

SEE ALSO For more information about battery replacement, refer to:

"■ Periodic replacement parts with defined life spans" on page E3-1

■ Replacing the S2CP471 or L1CP471 battery

This section describes the replacement of the S2CP471 or L1CP471 battery.

The following figure shows the processor module with the battery removed.

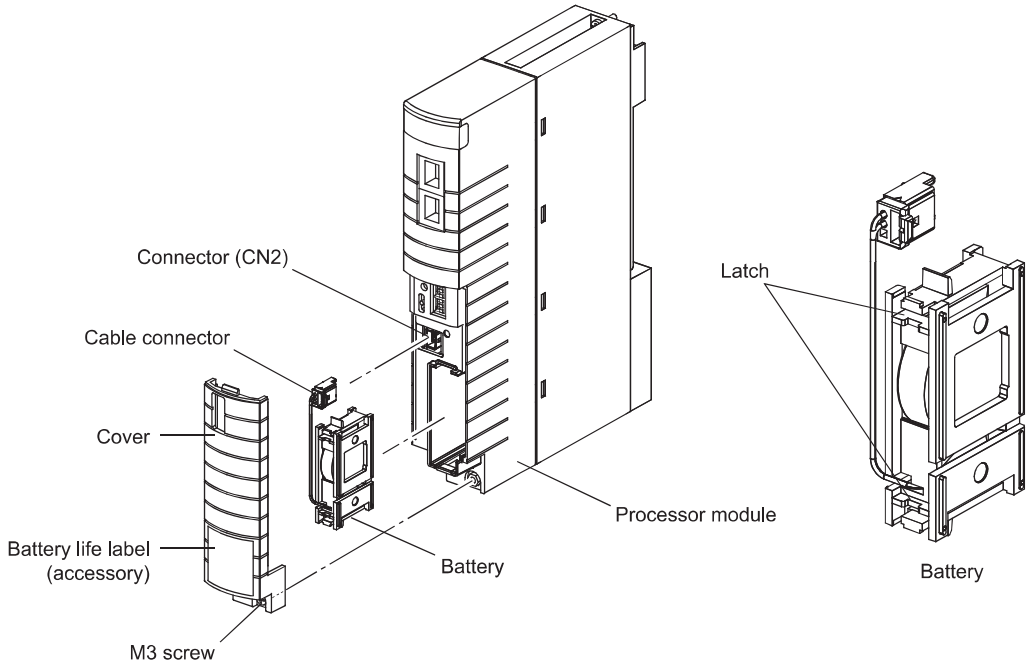


Figure E3.1-2 Processor module with the battery removed

● Removing the battery

IMPORTANT

If you want to maintain the real time data of RTC, you must leave the power to the SCU turned on while you replace the battery. If you remove the battery while the power is turned off, the real time data is initialized.

Follow these steps to remove the battery from the processor module:

1. Loosen the M3 screw that fixes the front cover of the module and remove the cover.
2. Disconnect the cable connector of the battery from the CN2 connector of the module.
3. Squeeze two latches on upper and lower side of the battery together with your thumb and fingers, and pull the battery from the module.

TIP

The following explanation is about the EU Battery Directive/Regulation and the UK Battery Regulation, and only valid in the EEA and the UK. The batteries are used in the processor modules. When you remove batteries from the processor modules, you must dispose the batteries in accordance with the domestic law concerning waste battery disposal. Take a right action on waste batteries, because the collection system in the EEA and the UK on waste batteries are regulated.

Battery type: Carbon monofluoride lithium batteries



Figure E3.1-3 The symbol marked on battery

The symbol on the battery means that the battery must be separately collected as regulated by the EU Battery Directive/Regulation or the UK Battery Regulation.

Installing the battery

Follow these steps to install the battery in the processor module:

1. Push the new battery until it is fully seated on the module.
2. Connect the cable connector of the battery to the CN2 connector of the module. Insert the connector plug securely, ensuring that the plug is properly oriented.
3. Put the front cover back and fix it with the M3 screw.

IMPORTANT

The tightening torque of the screws should be approximately 0.5 N·m.

4. Stick the battery life label that came with the battery to the front cover.

Replacing the SCP461 or SCP451 battery

This section describes replacement of the SCP461 or SCP451 battery.

The following figure shows SCP461 with the battery removed.

The battery of SCP451 is housed horizontally in the module.

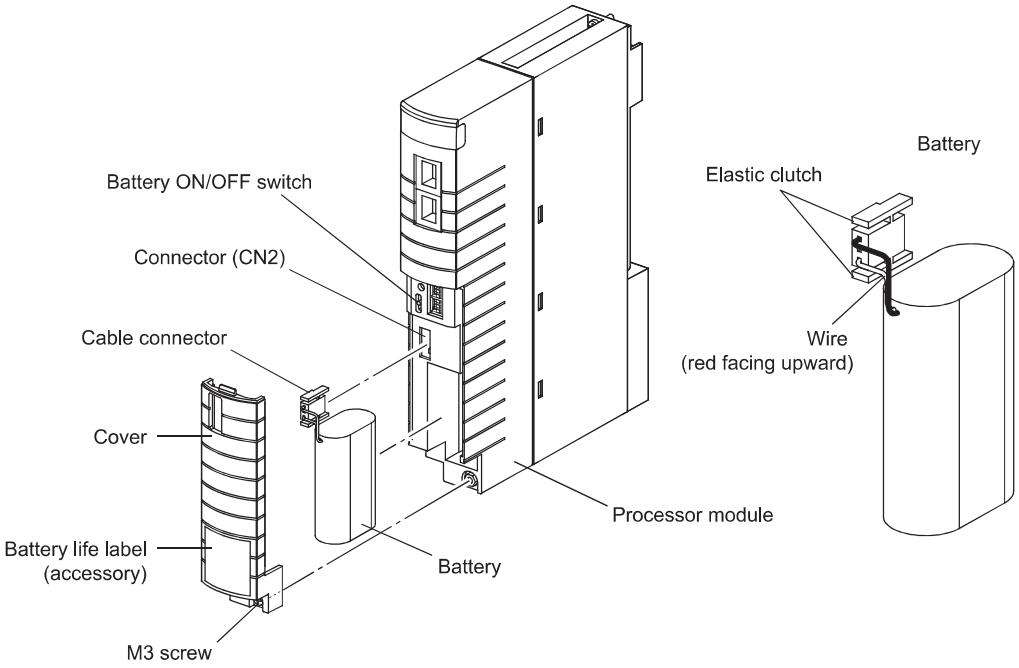


Figure E3.1-4 SCP461 with the battery removed

Removing the battery

IMPORTANT

If you want to save the management information of the processor module, you must leave the power to the SCU turned on while you replace the battery. If you turn off the battery ON/OFF switch while the power is turned off, the management information of the module (the operation data of NVRAM and the real time data of RTC) is lost.

Follow these steps to remove the battery from the processor module:

1. Set the battery ON/OFF switch to the OFF position. A non-conductive stick should be used to set the switch.
2. Loosen the M3 screw that fixes the front cover of the module and remove the cover.
3. Disconnect the cable connector of the battery from the CN2 connector of the module. The battery cable connector has a self-locking elastic clip. When pulling out the connector, you must push the clip to unlock it.
4. Pull out the battery to remove it from the module.

TIP

The following explanation is about the EU Battery Directive/Regulation and the UK Battery Regulation, and only valid in the EEA and the UK. The batteries are used in the processor modules. When you remove batteries from the processor modules, you must dispose the batteries in accordance with the domestic law concerning waste battery disposal. Take a right action on waste batteries, because the collection system in the EEA and the UK on waste batteries are regulated.

Battery type: Lithium Thionyl Chloride Batteries



Figure E3.1-5 The symbol marked on battery

The symbol on the battery means that the battery must be separately collected as regulated by the EU Battery Directive/Regulation or the UK Battery Regulation.

Installing the battery

Follow these steps to install the battery in the processor module:

1. Place the new battery to the specified position on the module.
2. Connect the cable connector of the battery to the CN2 connector of the module. Insert the connector plug securely, ensuring that the plug is properly oriented.
3. Put the front cover back and fix it with the M3 screw.

IMPORTANT

The tightening torque of the screws should be approximately 0.5 N·m.

4. Set the battery ON/OFF switch to the ON position. A non-conductive stick should be used to set the switch.
5. Stick the battery life label that came with the battery to the front cover.

E3.2 Replacing the parts of the node fan unit

The wide range temperature type SCU has a node fan unit. This section describes how to replace components of the node fan unit.

- Fan unit
- Fuse for fan power supply unit
- Power supply unit for fan unit

Replacing fan unit

IMPORTANT

You can replace the fan units without stopping the system. In this case, you must replace the fan units one by one so as not to remove both units at the same time. You must insert the fan unit slowly, making sure that there is no impact on the fan unit. Always replace the fan unit as a whole.

The following figure shows the node fan unit with one fan unit removed.

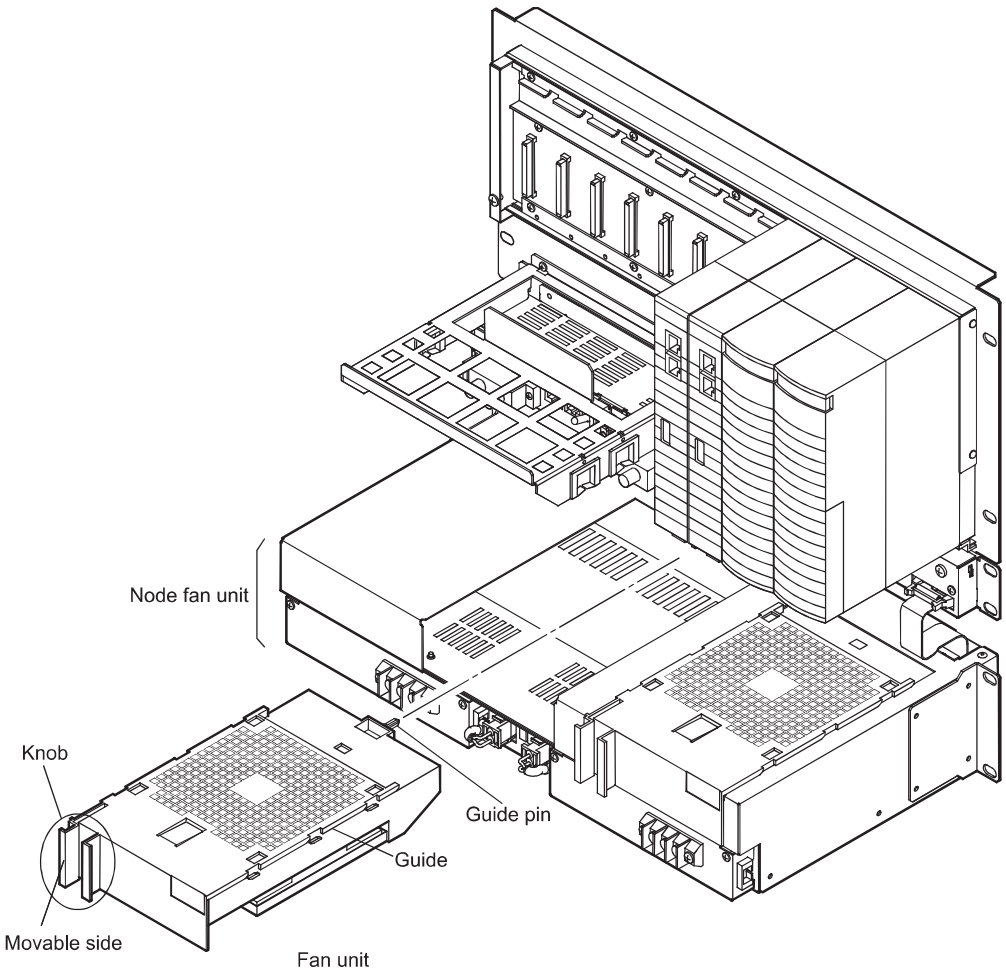


Figure E3.2-1 Replacing a fan unit (an example of SCU without an air deflector)

Follow these steps to replace a fan unit:

1. Pinch the knob with your thumb and index finger and unlock the movable side.
2. Pull the fan unit toward you. The fan unit is removed.
3. If the air deflector is not attached to the fan unit, go to the step 5. If the air deflector is attached, disengage the rear locking claws by pressing the opposite side of the air deflector with your fingers, and lift the air deflector to disengage the front locking claws.

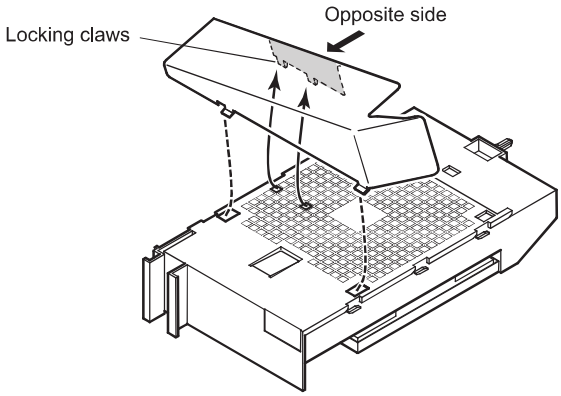


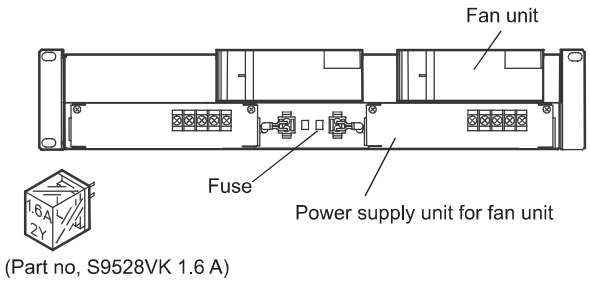
Figure E3.2-2 Detaching the air deflector

4. Insert the right and left front locking claws of the air deflector into the new fan unit, and press the opposite side of the air deflector with your fingers to fasten it to the fan unit.
5. Match the guide of the fan unit to the rail of the node fan unit.
6. Insert the fan unit slowly, making sure that there is no impact on the fan unit, until the connectors of the fan unit and the node fan unit are connected.
7. Check if the fan is rotating properly.

Replacing fuse for fan power supply unit

This section describes how to replace the fuse for fan power supply unit. You can replace the fuse without stopping the system.

The following figure shows the location of the fuse for fan power supply unit.



(Part no, S9528VK 1.6 A)

Figure E3.2-3 Fuse for fan power supply unit

1. Remove the fuse. If the fuse is hard to remove by hand, use a radio pliers and pull it out toward you.
2. Make sure that the new fuse has the same nominal current as the one you have removed, and insert the fuse with its imprints facing up.
3. Check if the fan is rotating properly.

Replacing power supply unit for fan unit

The following figure shows the mounting position of the fan power supply unit. The power supply output connector for N1 is located at the right-hand side of the fan power supply unit. On the other hand, the power supply output connector for N2 is located at the left-hand side of the fan power supply unit.

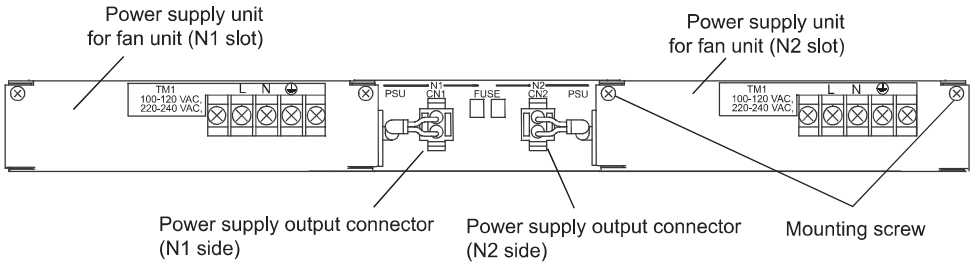


Figure E3.2-4 Power supply unit for fan unit

The following figure shows the output cable wiring of the power supply unit for fans.

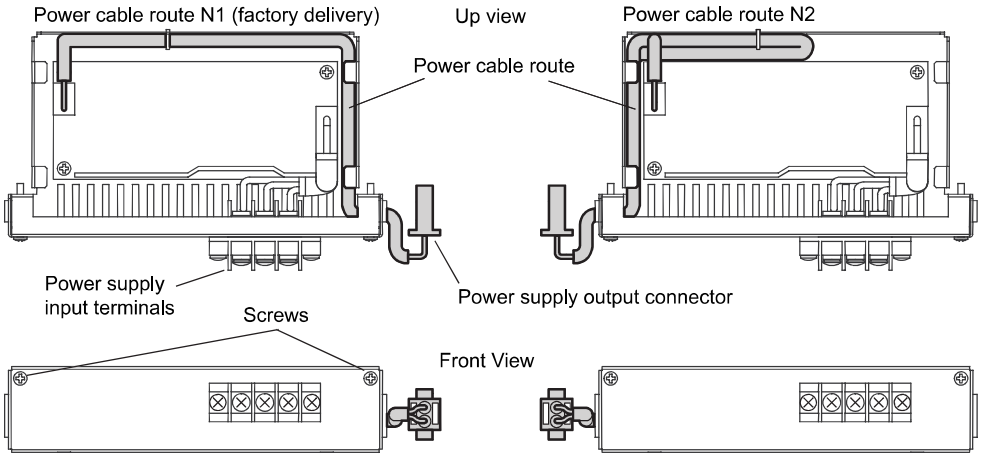


Figure E3.2-5 Power cable route of power supply unit for fan unit

The route of the power cable inside the power supply unit for fans is set to the N1 wiring route (shaded area) at shipment. When replacing the fan power supply unit on the N2 side, you must change the wiring route from N1 to N2.

Follow these steps to replace the fan power supply unit:

1. Disconnect the power supply to the power supply unit for fan unit to be replaced.
2. Remove the power supply output connector from the node fan unit.
3. Remove the screws and pull out the power supply unit.
4. Install a new power supply unit.
5. Connect the power supply output connector to the node fan unit.
6. Supply the power.
7. Check if the fan is rotating properly.

E3.3 Replacing the fuse of digital input module

In order to protect the module from the over current damage caused by short circuit between the input channel and the ground, a fuse is provided in the front of the digital input module (Model: SDV144 style S1, S2, S3). When the fuse is blown up by the short circuit, the fuse can be changed online without pulling the whole module out from its slot.

The following figure shows the location of the fuse.

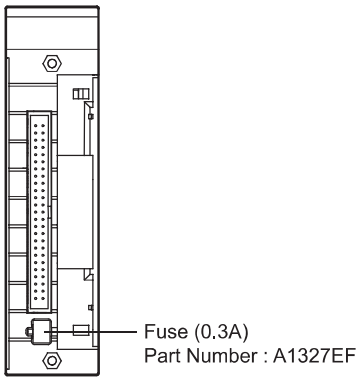


Figure E3.3-1 Front of SDV144 style S1, S2, and S3

IMPORTANT

In the case of dual-redundant modules, if the fuses of both the active and the standby modules are blown, alarm messages for both modules recover even if only one fuse is replaced. However, you must replace both fuses.

Follow these steps to replace the fuse:

1. Make sure that the input terminal does not have short circuit.
2. Disconnect the signal cable from the module.
3. Pull out the fuse to be replaced. Using a long-nose pliers can easily pull out the fuse.
4. Before putting the new fuse, make sure it has the same nominal current as the replaced one.
5. Insert the fuse with the imprints facing up.
6. Connect the signal cable to the module connector, and then check if the module is working properly.

E3.4 Replacing the fuse of terminal boards (for FIO node)

WARNING

- Do not put any tool on the terminal board during maintenance so as to prevent electric shock or other accidents.
- To prevent electric shock, do not insert or remove fuses while voltage is applied or current is being conducted to the terminals. If you must insert or remove fuses while electrified, contact YOKOGAWA sales or service agents.

IMPORTANT

Parts must be purchased and replaced in accordance with the laws and regulations of each country or region.

The following table describes the fuses for replacement for terminal boards.

Table E3.4-1 Fuses for replacement for terminal boards

Model	Style number	Part number	Remarks
SED2D	S1 and later	A1583EF	250 V/15 A
SED3D SED4D	S1 and later	A1618EF or A1034EF	250 V/10 A
SWD2D	S1 and later	S9536VK	250 V/3.2 A
		S9533VK	250 V/1 A
SBD2D	S1	A1602EF	250V/15A
	S2 and later	S9504VK	250V/15A
SBD3D	S1 and later	A1603EF	250V/10A
SBD4D	S1 and later	A1603EF	250V/10A
S1BB4D	S1 and later	A1603EF	250V/10A
		S9117FE	125V/0.63A

Replacing the fuse in the DIN rail terminal board

This section describes the replacement of fuse in SBD2D, SBD3D, SBD4D, and S1BB4D.

Follow these steps to remove the fuse:

1. Insert a flathead screwdriver into the groove in the fuse holder cap.
2. Turn the screwdriver anti-clockwise.
   The fuse holder cap comes out.
3. Remove the fuse from the fuse holder cap.

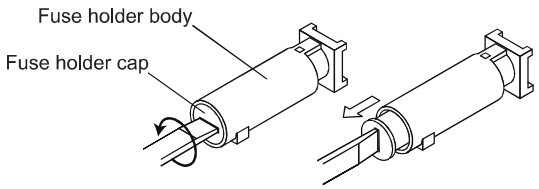


Figure E3.4-1 Removing a fuse

Follow these steps to install the fuse:

1. Insert a fuse into the fuse holder cap.
2. Insert the fuse holder cap into the fuse holder.
3. Press the fuse holder cap into the fuse holder while rotating it clockwise with a flathead screwdriver.

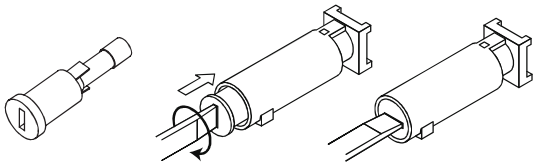


Figure E3.4-2 Installing a fuse

E3.5 Replacing the relays on relay boards

CAUTION

- Do not put any tool into the relay board during maintenance so as to prevent electric shock or other abnormalities.
- To prevent electric shock, do not insert or remove relays while voltage is applied or current is being conducted to the terminals. If you must insert or remove relays while electrified, contact YOKOGAWA sales or service agents.
- Be aware that the relay may be hot.

SEE ALSO For more information about Relay for relay board replacement, refer to:

"■ Periodic replacement parts with defined life spans" on page E3-1

■ Removing a relay of SBM54D (style S3 or later)

For SBM54D of style S3 or later, use a dedicated relay removal tool to remove relays.

IMPORTANT

After using the relay removal tool about 50 times, you need to replace it with a new one. The part number of the tool is T9084SX.

Follow these steps to remove a relay:

1. With the levers of the relay removal tool tilted inside, put the tool deeply on the relay so as to fully cover it.

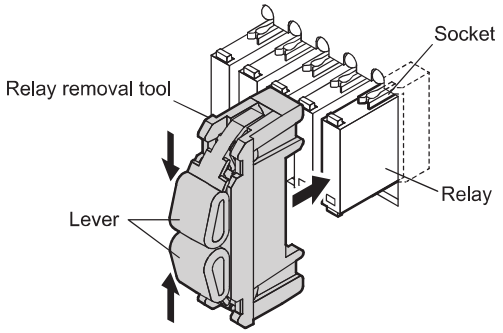


Figure E3.5-1 Placing the relay removal tool

2. Pinch the upper and lower levers with your fingers and open them outward, applying force evenly. The relay leaves the socket.

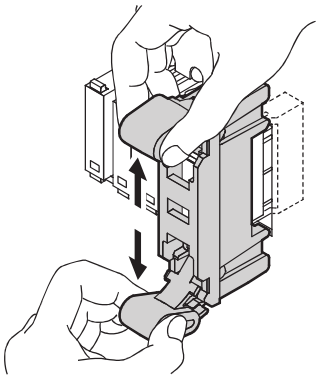


Figure E3.5-2 Removing a relay from the socket - 1

3. With the levers opened, pull out the tool and the relay together.

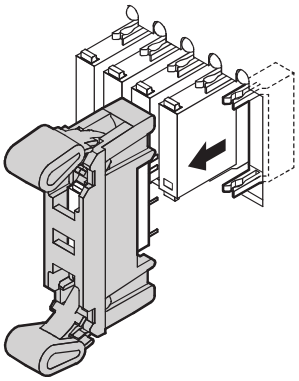


Figure E3.5-3 Removing a relay from the socket - 2

4. Tilt the levers inside to release the relay from the tool.

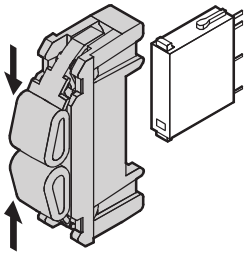


Figure E3.5-4 Releasing the relay from the tool

Installing a relay of SBM54D (style S3 or later)

Fit the pins of the relay to the holes on the socket, and insert the relay all the way seated.

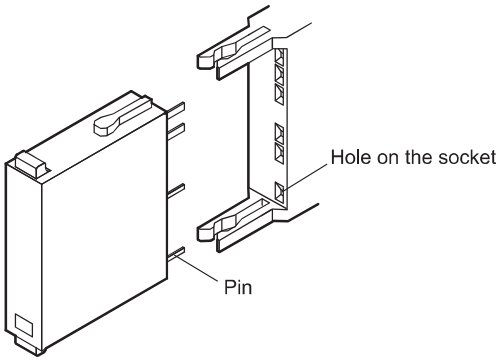


Figure E3.5-5 Installing a relay

E3.6 Replacing the fuse of relay boards

CAUTION

- Do not put any tool into the relay board during maintenance so as to prevent electric shock or other accidents.
- To prevent electric shock, do not insert or remove fuses while voltage is applied or current is being conducted to the terminals. If you must insert or remove fuses while electrified, contact YOKOGAWA sales or service agents.

The following table describes the fuses for replacement for relay boards.

Table E3.6-1 Fuses for replacement for relay boards

Model	Style number	Part number	Remarks
SRM53D SRM54D	S1 and later	A1327EF	125 V/0.3 A, 16 pcs
SBM54D	S1 and later	A1603EF	250 V/10 A, 2 pcs

SEE ALSO For more information about replacing fuses in SBM54D, refer to:

"■ Replacing the fuse in the DIN rail terminal board" on page E3-13

E3.7 Replacing the fuses of the base plate for barrier

CAUTION

To prevent electric shock, do not insert or remove fuses while voltage is applied or current is being conducted to the terminals. If you must insert or remove fuses while electrified, contact the service department of YOKOGAWA.

The following table describes the fuses for replacement for base plates for barrier.

Table E3.7-1 Fuses for replacement for base plates for barrier

Model	Style number	Part number	Remarks
S2BN4D	S1 and later	A1559EF	250 V/2.5 A
S2BN5D	S1 and later	A1624EF	250 V/3.15 A

E3.8 Replacing the fuses of base plate with disconnecting terminals

CAUTION

- Do not put any tool into the base plate during maintenance so as to prevent electric shock or other accidents.
- To prevent electric shock, do not insert or remove fuses while voltage is applied or current is being conducted to the terminals. If you must insert or remove fuses while electrified, contact YOKOGAWA sales or service agents.

IMPORTANT

Parts must be purchased and replaced in accordance with the laws and regulations of each country or region.

Fuses rated for 2A (Part number: A1643EF) are installed in a connector type base plate with disconnecting terminals.

The following figure shows the replacement of a fuse.

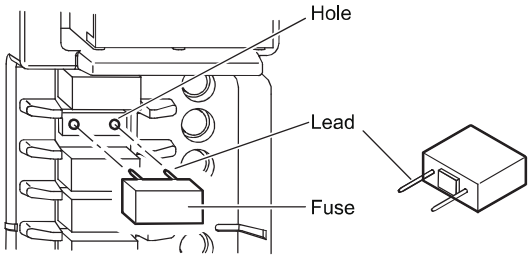


Figure E3.8-1 Replacing a fuse

Follow these steps to replace a fuse:

1. Hold the right and left ends of fuse with a tool and pull the fuse straight out.
   The portion of tool that touches the fuse must be made of non-conductive material.
2. Hold the right and left ends of new fuse with the tool and push the leads of the fuse straight into the holes.

E4. Replacing FIO node components

This section describes how to replace the FIO node components. The dual-redundant module can be removed and installed without disconnecting the power supply for the SCU, SNU, and the unit for optical ESB bus repeater module.

- Power Supply Module
- Processor Module
- ESB Bus Coupler Module
- N-ESB bus coupler module
- ESB Bus Interface Module
- Optical ESB Bus Repeater Module
- FIO I/O module
- SNU

CAUTION

Before replacing a device in dual-redundant configuration, you must make sure that the other device is working normally.

SEE ALSO

For more information about replacing the V net coupler unit, refer to:

Safety Control Stations (Hardware) (IM 32Q06C10-31E)

E4.1 Replacing power supply module

WARNING

Switch off the power supply before removing the power supply modules, and make sure that the status lamps of the power supply module are off.

The following figure shows replacement of the power supply module.

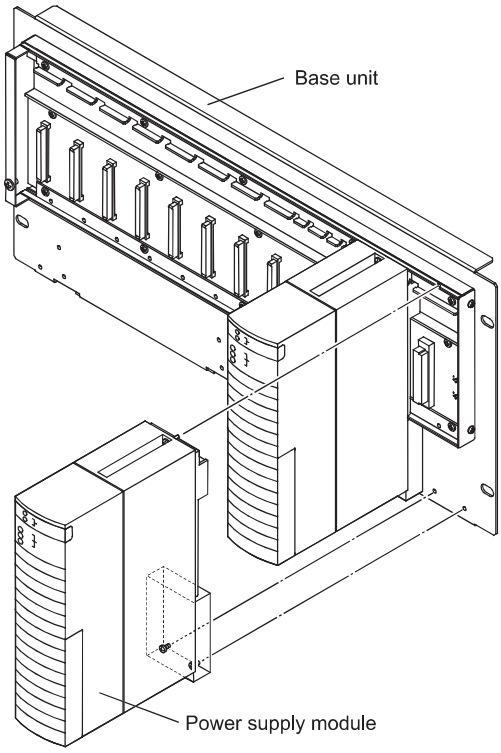


Figure E4.1-1 Replacing power supply module

TIP

You must use dual-redundant configuration for the power supply module of the SNU in the ProSafe-RS. You must observe the following note if the processor module of the SCU or at least one of the processor modules of the dual-redundant safety control unit is as follows:

SCP451 of unit version "U:4" or earlier

If an error occurs and only one of the paired modules powers up, or a power failure occurs on one module, and you have no choice but to continue in the non-redundant state, the diagnostic information message (No.0065) for the ESB bus interface module (SSB401) error might be generated for that node. After about one second the system recovers. This phenomenon occurs very rarely and it does not indicate the abnormality of SSB401 module and the related ESB bus and devices. It does not harm communication either.

Prevention:

The power supply modules should be kept in dual-redundant configuration.

Restoration:

If the abnormality indication disappears in a second, there is no need to do anything about it.

If one of the paired power supply modules fails, the failed module should be replaced as soon as possible so as to return to the normal state (dual-redundant power supply configuration).

Removing a power supply module

Follow these steps to remove the power supply module:

1. Stop the power supply of the module to be replaced.
2. Disconnect the power cable from the power supply input terminals.
3. Loosen the three M3 screws and remove the power supply module.

Installing a power supply module

Follow these steps to install the power supply module:

1. Mount the power supply module on the base unit by tightening the three M3 screws.

IMPORTANT

The tightening torque of the screws should be approximately 0.5 N·m.

2. Connect the power cable to the power supply input terminals.
3. Turn on the power supply.
   The status lamps of the power supply module turn on.

E4.2 Replacing processor module

This section describes how to replace the processor module.

IMPORTANT

If you want to replace SCP461 to S2CP471, contact YOKOGAWA sales or service agents for replacement instead of doing it yourself.

The following figure shows replacement of the processor module.

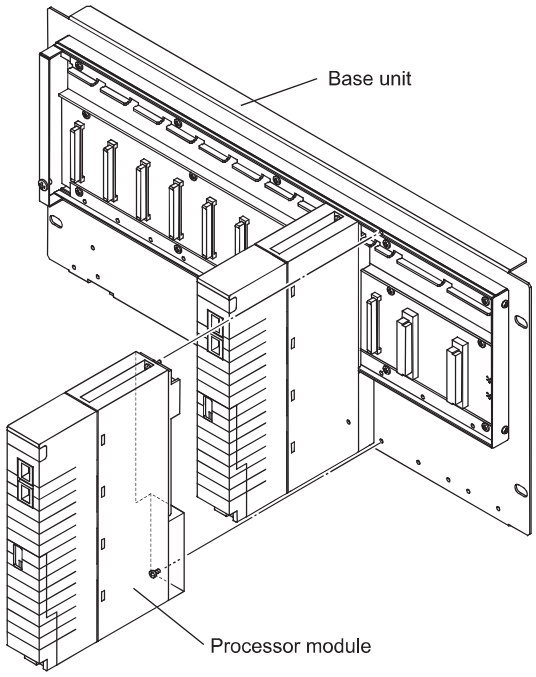


Figure E4.2-1 Replacing processor module

SEE ALSO For more information about disconnecting the cables for Vnet/IP, refer to:

C3.1, “Connecting cables for Vnet/IP” on page C3-2

For more information about front lamps of the processor module, refer to:

“● Status lamps” on page B4-6

For more information about master database offline download, refer to:

I4.4, “Master database offline download” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

For more information about operating condition of S2CP471 and mountable SCU, refer to:

ProSafe-RS Processor Module (for SSC60 and S2SC70), Processor Module Upgrade Kit (for SSC60 and S2SC70) (GS 32P06D20-01EN)

Removing a processor module

IMPORTANT

When you remove the processor module while the system is running, you should not disconnect the cables for Vnet/IP from the processor module.

Follow these steps to remove the processor module:

1. Make sure that the RDY lamp on the processor module to be removed is turned off. If the RDY lamp is turned on, push the START/STOP switch to turn it off.
2. Loosen the two M3 screws that fix the processor module, and remove it.
3. Disconnect the cables for BUS1 and BUS2 from the front of the processor module. There is no need to disconnect the cables from the Layer2 Switch.

Precautions when replacing the processor module with one that was used in another system

When replacing the processor module with a processor module that was used in another system, you must clear the configuration information in the module, depending on the system configuration of the system where the module will be used.

- For ProSafe-RS system integrated with CENTUM
  There is no need to clear the configuration information in the module.
- For ProSafe-RS stand-alone system
  Before installing the processor module, you must clear the configuration information in the module. Follow these steps to clear the configuration information:
  1. Set the domain number setting switches of the processor module as follows:

Table E4.2-1 Setting of the domain number setting switches

Bit 1	Parity	1
Bit 2		1
Bit 3		0
Bit 4	MSB	0
Bit 5		0
Bit 6		0
Bit 7		0
Bit 8	LSB	1

  2. Set the station number setting switches of the processor module as follows:

Table E4.2-2 Setting of the station number setting switches

Bit 1	Parity	0
Bit 2	MSB	0
Bit 3		0
Bit 4		0
Bit 5		0

Continues on the next page

Table E4.2-2 Setting of the station number setting switches (Table continued)

Bit 6		0
Bit 7		0
Bit 8	LSB	1

3. Make sure that the setting switches in the front of the processor module are all set to the OFF position.

Table E4.2-3 Setting of the front setting switches

Bit 6		OFF
Bit 5	FIX	OFF
Bit 4	PORT	OFF
Bit 3		OFF
Bit 2	DOMN	OFF
Bit 1	STA	OFF

4. Without connecting the cables for Bus1 and Bus2, install the processor module to the base unit.
5. Push the START/STOP switch on the processor module immediately, and make sure that the HRDY lamp is OFF.
6. Keep the processor module at this status for about a minute.
7. Remove the processor module from the base unit.

SEE ALSO For more information about the setting switches, refer to:

"■ Elements on the processor module" on page B4-4

■ Installing a processor module

This section describes how to install a processor module.

● Installing S2CP471 or L1CP471

Follow these steps to install S2CP471 or L1CP471:

1. Make sure that the domain number and station number settings and the front setting switches on the processor module to be installed are the same as those set on the module that you removed.
2. Set the operation data reset switch to the RESET position.
3. Connect the cables to both ports of BUS1 and BUS2. There is no need to turn off the power of the Layer2 Switch.
4. Mount the processor module on the base unit by tightening the two M3 screws.

IMPORTANT

The tightening torque of the screws should be approximately 0.5 N·m.

5. Make sure that the HRDY lamp on the processor module is turned on, and set the operation data reset switch to the HOLD position.

6. Make sure that the process module is working normally by checking the lighting of the status lamps and the SCS State Management window in the SCS Maintenance Support Tool.
   In the diagnostic information window on the SENG, ensure that no diagnostic information message for an error is generated.
7. In the single configuration, perform master database offline download after you install the processor module.
   In the dual-redundant configuration, the program is copied automatically, and the status changes to standby after copying.

Installing SCP461 or SCP451

Follow these steps to install the processor module:

1. Make sure that the domain number and station number settings and the negotiation setting of the front setting switches on the processor module to be installed are the same as those set on the module that you removed.
2. Set the battery ON/OFF switch to the OFF position.
3. Connect the cables to both ports of BUS1 and BUS2. There is no need to turn off the power of the Layer2 Switch.
4. Mount the processor module on the base unit by tightening the two M3 screws.

IMPORTANT

The tightening torque of the screws should be approximately 0.5 N·m.

5. Set the battery ON/OFF switch to the ON position.
6. Make sure that the process module is working normally by checking the lighting of the status lamps and the SCS State Management window in the SCS Maintenance Support Tool.
   In the diagnostic information window on the SENG, ensure that no diagnostic information message for an error is generated.
7. In the single configuration, perform master database offline download after you install the processor module.
   In the dual-redundant configuration, the program is copied automatically, and the status changes to standby after copying.

SEE ALSO For more information about precautions when installing the processor module, refer to:

"■ Precautions when replacing the processor module with one that was used in another system" on page E4-5

E4.3 Replacing ESB bus coupler module

This section describes how to replace the ESB bus coupler module.

Removing an ESB bus coupler module

Follow these steps to remove the ESB bus coupler module:

1. Loosen the two M3 screws and remove the ESB bus coupler module.
2. Loosen the two screws and disconnect the ESB bus cable.

Installing an ESB bus coupler module

Follow these steps to install the ESB bus coupler module:

1. Connect the ESB bus cable to the connector of the ESB bus coupler module and tighten the two screws on the connector.

IMPORTANT

The tightening torque of the cable connector fixing screws should be approximately 0.3 N·m.

2. Install the ESB bus coupler module on the base unit securely by tightening the two M3 screws.

IMPORTANT

The tightening torque of the module fixing screws should be approximately 0.5 N·m.

3. Make sure that the replaced ESB bus coupler module is working properly by checking the SCS State Management window.

E4.4 Replacing the N-ESB bus coupler module

This section describes the replacement of the N-ESB bus coupler module.

Removing an ESB bus coupler module

Follow these steps to remove the N-ESB bus coupler module:

1. Loosen the two M3 screws and remove the N-ESB bus coupler module.
2. Disconnect the N-ESB bus cables.

Installing an N-ESB bus coupler module

Follow these steps to install the N-ESB bus coupler module:

1. Connect the cables for N-ESB bus to the N-ESB bus coupler module.
2. Install the N-ESB bus coupler module on the base unit by tightening the two M3 screws.

IMPORTANT

The tightening torque of the screws should be approximately 0.5 N·m.

3. Make sure that the replaced N-ESB bus coupler module is working properly by checking the SCS State Management window.

E4.5 Replacing ESB bus interface module

This section describes the replacement of the ESB bus interface module.

Removing an ESB bus interface module

Follow these steps to remove the ESB bus interface module.

1. Loosen the two M3 screws and remove the ESB bus interface module.
2. Loosen the two M3 screws and remove the connector unit for ESB bus of the unmounted ESB bus interface module. Do not disconnect the ESB bus cable that is connected to the connector unit for ESB bus.

Installing an ESB bus interface module

Follow these steps to install the ESB bus interface module:

1. Set the ESB bus address of the ESB bus interface module to be the same address as the removed ESB bus interface module.
2. Tighten the two M3 screws to install the connector unit for ESB bus to the ESB bus interface module.

IMPORTANT

The tightening torque of the screws for fixing the connector unit for ESB bus should be approximately 0.5 N·m.

3. Tighten the two M3 screws to install the ESB interface module to the base unit.

IMPORTANT

The tightening torque of the module fixing screws should be approximately 0.5 N·m.

4. Confirm that the replaced ESB bus interface module is working normally by checking the status lamps and the SCS State Management window.

E4.6 Replacing optical ESB bus repeater module

This section explains the replacement of the optical ESB bus repeater module.

Removing an optical ESB bus repeater master module

Follow these steps to remove the optical ESB bus repeater master module:

1. Remove the fiber-optic cable that is connected to the optical ESB bus repeater master module. Cap the cable to prevent dust infiltration.
2. Loosen the two M3 screws and removed optical ESB bus repeater module.
3. Loosen the two M3 screws and remove the connector unit for ESB bus of the unmounted optical ESB bus repeater module. Do not disconnect the ESB bus cable from the connector unit for ESB bus.

Installing an optical ESB bus repeater master module

Follow these steps to install the optical ESB bus repeater master module:

1. Tighten the two M3 screws to install the connector unit for ESB bus to the optical ESB bus repeater master module.

IMPORTANT

The tightening torque of the screws for fixing the connector unit for ESB bus should be approximately 0.5 N·m.

2. Tighten the two M3 screws to install the optical ESB bus repeater master module to the base unit.

IMPORTANT

The tightening torque of the module fixing screws should be approximately 0.5 N·m.

3. Uncap the fiber-optic cable and connect it to the optical ESB bus repeater master module. The fiber-optic cable has an IN end and an OUT end. Confirm that you have connected them correctly.
4. Make sure that the replaced module is working properly by checking the SCS State Management window.

Removing an optical ESB bus repeater slave module

Follow these steps to remove the optical ESB bus repeater slave module.

1. Remove the fiber-optic cable that is connected to the optical ESB bus repeater slave module. Cap the cable to prevent dust infiltration.
2. Loosen the two M3 screws and remove the optical ESB bus repeater slave module.
3. Disconnect the ESB bus cable from the unmounted optical ESB bus repeater slave module by loosening the two screws.

Installing an optical ESB bus repeater slave module

Follow these steps to install the optical ESB bus repeater slave module.

1. Connect the ESB bus cable to the optical ESB bus repeater slave module securely by tightening the two screws on the connector.

IMPORTANT

The tightening torque of the cable fixing screws should be approximately 0.3 N·m.

2. Install the optical ESB bus repeater slave module on the base unit securely by tightening the two M3 screws.

IMPORTANT

The tightening torque of the module fixing screws should be approximately 0.5 N·m.

3. Uncap the fiber-optic cable and connect it to the optical ESB bus repeater slave module. The fiber-optic cable has an IN end and an OUT end. Be sure you connect the correct end.
4. Make sure that the replaced optical ESB bus repeater slave module is working properly by checking the SCS State Management window.

E4.7 Replacing FIO I/O modules

The following procedures are available when replacing an FIO I/O module:

- Replacement procedure for a dual-redundant configuration
- Replacement procedure for a non-redundant configuration

The following figure shows the replacement of an FIO I/O module.

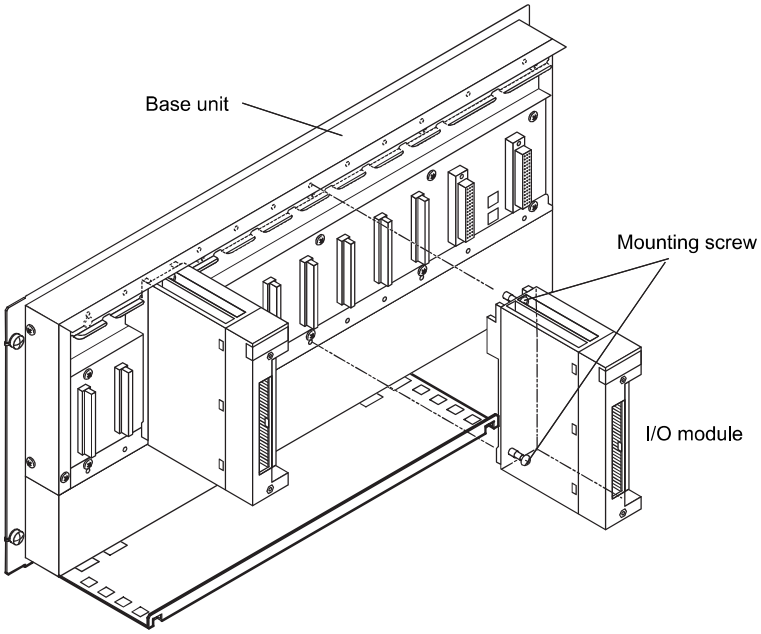


Figure E4.7-1 Replacing FIO I/O modules

SEE ALSO For more information about the behaviors and the recovery procedures when an error occurs, refer to:

G2., "Operations and recovery procedures during the SCS error occurrence" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Replacement procedure for a dual-redundant configuration

The procedure for replacing an FIO I/O module differs, depending on whether you replace a standby module or an active module.

When replacing a module on the standby side

Follow these steps to replace the standby module of a redundant pair of FIO I/O modules:

1. Confirm that the status lamps of the pair of redundant I/O modules are as follows:
   - The DX lamps of both modules are ON.
   - The ACT lamp is OFF on the module to be replaced, and ON on the active module.
2. Remove the front cable or the pressure clamp terminal blocks.
3. Loosen the two M3 screws and remove the module.
4. Mount the new module on the base unit securely by tightening the two M3 screws.

IMPORTANT

The tightening torque of the screws should be approximately 0.5 N·m.

5. Perform an IOM download for the replaced module. If Automatic IOM Download is set to [Enable] in the SCS Constants Builder, IOM download is performed automatically.

TIP

If it is not set to download automatically, perform the IOM download from the SCS State Management window of the SCS Maintenance Support Tool.

6. Make sure that the status lamps STATUS and DX of the replaced module are turned on, and the status lamp ACT is turned off.
7. Install the cable or the pressure clamp terminal blocks.
8. Make sure that the replaced module is working properly.

SEE ALSO

For more information about removing and installing the dual-redundant pressure clamp terminal blocks, refer to:

"■ Removing and installing the dual-redundant pressure clamp terminal blocks" on page E4-16

For more information about the SCS Constants Builder, refer to:

C1.2.6, "SCS Constants Builder" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

● When replacing a module on the active side

CAUTION

Do not remove the cables or terminal blocks on the active modules. If you perform dual-redundant switching by removing the cable or terminal block on the active side, IOP occurs and the relevant loops may be shutdown.

Follow these steps to replace the active module of a redundant pair of FIO I/O modules:

1. From the SENG, use the IOM Control Right Switching Tool and switch the adjacent module into active and the module to be replaced into standby. In this case, set the security level to "1".
2. Confirm that the status lamps of the pair of redundant I/O modules are as follows:
   - The DX lamps of both modules are ON.
   - The ACT lamp is OFF on the module to be replaced, and ON on the active module.
3. Remove the front cable or the pressure clamp terminal blocks.
4. Loosen the two M3 screws and remove the module.
5. Mount the new module on the base unit securely by tightening the two M3 screws.

IMPORTANT

The tightening torque of the screws should be approximately 0.5 N·m.

6. Perform an IOM download for the replaced module. If Automatic IOM Download is set to [Enable] in the SCS Constants Builder, IOM download is performed automatically.

TIP

If it is not set to download automatically, perform the IOM download from the SCS State Management window of the SCS Maintenance Support Tool.

7. Make sure that the status lamps STATUS and DX of the replaced module are turned on, and the status lamp ACT is turned off.
8. Install the cable or the pressure clamp terminal blocks.
9. Make sure that the replaced module is working properly.

SEE ALSO

For more information about removing and installing the dual-redundant pressure clamp terminal blocks, refer to:

"■ Removing and installing the dual-redundant pressure clamp terminal blocks" on page E4-16

For more information about the SCS Constants Builder, refer to:

C1.2.6, "SCS Constants Builder" in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

■ Replacement procedure for a non-redundant configuration

CAUTION

When using the digital output module, do not remove the front cable or the terminal block while the output signal is ON. Sparks may occur in the connectors. Sparks may affect the connection quality.

Follow these steps to replace the FIO I/O module in non-redundant configuration:

1. If you are replacing a digital output module, set the outputs on all channels to OFF.(To set the outputs to OFF, lock the module from the I/O Lock Window or set the output value by application logic.)
2. Separate the front cable or the pressure clamp terminal blocks.
3. Loosen the two M3 screws and remove the module.
4. Tighten the two M3 screws and install the new module to the base unit.

IMPORTANT

The tightening torque of the screws should be approximately 0.5 N·m.

5. For the replaced module, perform IOM downloading from the SCS State Management window of SCS Maintenance Support Tool.
6. Install the cable, the pressure clamp terminal blocks, or the MIL cable.
7. Make sure that the hardware of the replaced module is working properly.

SEE ALSO

For more information about removing and installing the pressure clamp terminal blocks and the cover of the MIL connector, refer to:

"■ Removing and installing the pressure clamp terminal blocks and the cover of the MIL connector" on page E4-17

Removing and installing the dual-redundant pressure clamp terminal blocks

This section describes the removal of the dual-redundant pressure clamp terminal blocks before replacing the I/O module, and installation after the replacement.

The following figure shows the removed dual-redundant pressure clamp terminal blocks.

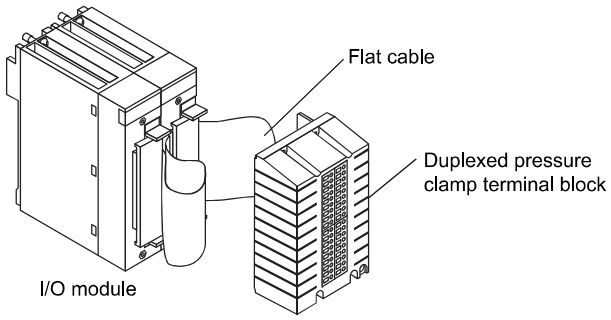


Figure E4.7-2 Connection of dual-redundant connection cables

The following figure shows the removed dual-redundant connecting cables of the dual-redundant pressure clamp terminal blocks.

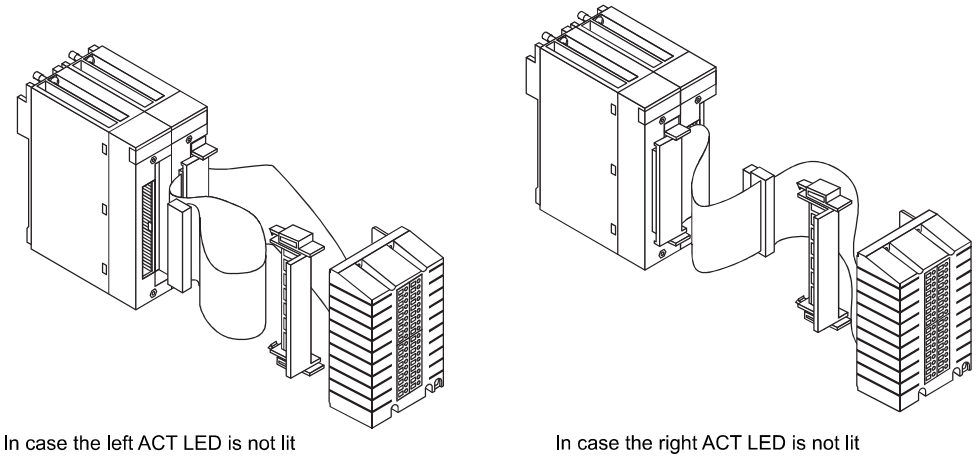


Figure E4.7-3 Removing the dual-redundant connection flat cable

Follow these steps to remove the dual-redundant pressure clamp terminal blocks:

1. Loosen the four M3 screws of the pressure clamp terminal block, and remove while supporting it so as not to apply too much stress to the flat cable.
2. While supporting the pressure clamp terminal blocks, remove the dual-redundant connection flat cable that is connected to the I/O module to be replaced.

Follow these steps to install the dual-redundant pressure clamp terminal blocks:

1. Reinstall the dual-redundant flat cable connector.
2. Install the pressure clamp terminal block by fixing the four M3 screws.

IMPORTANT

The tightening torque of the screws should be approximately 0.5 N·m.

Removing and installing the pressure clamp terminal blocks and the cover of the MIL connector

Follow this step to remove the pressure clamp terminal block or the MIL connector cover:

- Loosen the two M3 screws of the pressure clamp terminal blocks or the MIL connector cover to remove the item.

The following figure shows the I/O modules with the removed pressure clamp terminal block or MIL connector cover.

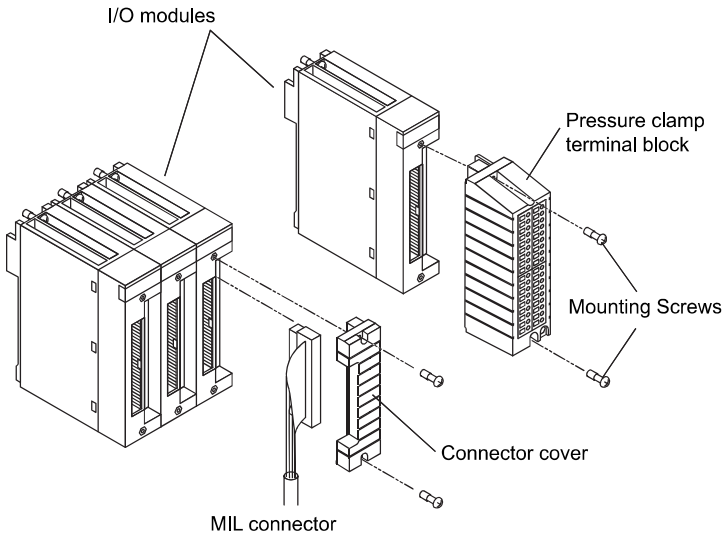


Figure E4.7-4 Removing the terminal block or MIL connector cover

Follow this step to install the pressure clamp terminal block or the MIL connector cover:

- Tighten the two M3 screws to install the pressure clamp terminal blocks or the MIL connector cover to the module.

IMPORTANT

The tightening torque of the screws should be approximately 0.5 N·m.

E4.8 Replacing, adding, and removing the SNU

This section describes the replacement, addition, and removal of the SNU when the SCU is in operation. When replacing the SNU, you must turn its power supply OFF.

E4.8.1 Replacing the SNU

When the SCU is in operation, you must follow these steps to replace the SNU:

1. Check the Bus1 and Bus2 status on the SCS state management window beforehand.
2. Switch off the power supply of the SNU to be replaced.
3. While the ESB bus cable is connected, remove the branch connector unit for ESB bus from the ESB bus interface module for Bus1.
4. Make sure that no error is found in the node units other than the SNU to be replaced by checking in the SCS State Management window.
5. While the ESB bus cable is connected, remove the branch connector unit for ESB bus from the ESB bus interface module for Bus2.
6. Replace the SNU. Make sure that the node address of the ESB bus interface module is correct.
7. Connect the branch connector unit for ESB bus to the ESB bus interface module of the new SNU.
8. Switch on the SNU power supply.
9. Make sure that the replaced SNU is running properly by checking in the SCS State Management window.

E4.8.2 Adding the SNU

This section describes how to add an SNU at the end of the ESB bus.

Follow these steps to add a new SNU when the SCU is in operation:

1. Before the operation, make sure that the status of both Bus1 and Bus2 that are set to dual-redundant is normal by checking in the SCS State Management window.
2. Remove the ESB bus coupler module for Bus1 of the SCU from the base unit by pulling it out toward you. Make sure that the ESB Bus1 is indicated as FAIL, and that the ESB Bus2 is normal.
3. For the existing SNU at the end of the ESB bus, remove the branch connector unit with a built-in terminator for ESB bus from the ESB bus interface module of Bus1 without disconnecting the ESB bus cable.

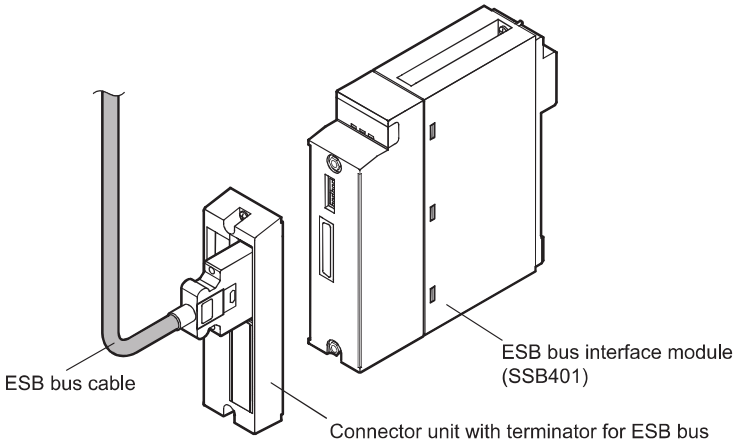


Figure E4.8.2-1 Removing the branch connector unit with a built-in terminator for ESB bus

4. Disconnect the ESB bus cable from the branch connector unit with a built-in terminator for ESB bus that is removed in step 3.
5. Connect the cable that is disconnected in step 4 to a branch connector unit without a terminator for ESB bus. The tightening torque of the screws on the ESB bus cable connector should be approximately 0.3 N·m.
6. Connect the branch connector unit with a built-in terminator for ESB bus that is disconnected in step 4 and the branch connector unit for ESB bus from step 5 with the ESB bus cable.
7. Make sure that the node address of the ESB bus interface module of the newly added SNU is correct.
8. Connect the branch connector unit for ESB bus in step 5 to the ESB bus interface module of the existing SNU.
9. Connect the branch connector unit with a built-in terminator for ESB bus in step 6 to the ESB bus interface module of the newly added SNU.
10. Put back the ESB bus coupler module of Bus 1 that is removed in step 2 to the base unit.
11. On the SCS State Management window, make sure that both ESB buses are working properly.
12. Follow steps 2 to 11 for the ESB Bus2 by reading the instructions for Bus1 as Bus2.
13. Install the I/O modules to the newly added SNU and then turn on the power supply for the newly added SNU.
14. Run online downloading to the I/O modules that are installed in the newly added SNU.

15. Connect the cables or terminal blocks to the I/O modules that are installed in the added newly added SNU.
16. Make sure that all added hardware components are working properly by checking the SCS State Management window.

SEE ALSO For more information about installing I/O modules, refer to:

E4.7, “Replacing FIO I/O modules” on page E4-13

E4.8.3 Removing the SNU

This section describes how to remove the SNU at the end of the ESB bus.

Follow these steps to remove the SNU when the SCU is in operation:

1. Before the operation, make sure that the status of both Bus1 and Bus2 that are set to dual-redundant is normal by checking in the SCS State Management window.
2. Delete (online) all the definitions related to the I/O modules of the SNU to be removed. Deleting the definition of I/O modules of the SNU also deletes the definition of the node.
3. Remove the signal cables or the terminal blocks of the I/O modules to be removed.
4. Remove two fixing screws at the upper part and at the lower part of the I/O module.
5. Pull out the I/O module toward you and remove it from the base unit.
6. Repeat step 3 to step 5 to remove all the I/O modules from the SNU to be removed.
7. Turn off the power supply to the SNU to be removed.
8. Remove the ESB bus coupler module for Bus1 of the SCU from the base unit by pulling it out toward you. Make sure that the ESB Bus1 is indicated as FAIL, and that the ESB Bus2 is normal.
9. For the SNU at the end of the ESB bus that is to be replaced, remove the branch connector unit with a built-in terminator for ESB bus from the ESB bus interface module of Bus1 without disconnecting the ESB bus cable.
10. For the SNU that now comes at the end of the ESB bus, remove the branch connector unit for ESB bus from the ESB bus interface module of Bus1 without disconnecting the ESB bus cable.
11. Disconnect the ESB bus cable from the branch connector unit with a built-in terminator for ESB bus that is removed in step 9.
12. Disconnect the ESB bus cable from the branch connector unit for ESB bus that is removed in step 10.
13. Connect the cable that is disconnected in step 12 to a branch connector unit with a built-in terminator for ESB bus. The tightening torque of the screws on the ESB bus cable connector should be approximately 0.3 N·m.
14. Connect the branch connector unit with a built-in terminator for ESB bus in step 13 to the ESB bus interface module of the SNU that now comes at the end of the ESB bus.
15. Put back the ESB bus coupler module of Bus 1 that is removed in step 8 to the base unit.
16. Make sure that no error is found on the ESB bus by checking in the SCS State Management window.
17. Follow steps 8 to 16 for the ESB Bus2 by reading the instructions for Bus1 as Bus2.

SEE ALSO For more information about installing I/O modules and mounting the terminal blocks, refer to:

E4.7, “Replacing FIO I/O modules” on page E4-13

E5. Replacing N-IO node components

This section describes how to replace the N-IO node components. You can remove and install equipment with dual-redundant configuration without disconnecting the power supply of the SCU.

- Power supply unit
- N-ESB bus module
- N-IO I/O module

CAUTION

- You cannot replace the base plate while the power is supplied to the node interface unit connected to the base plate.
- You cannot add a base plate while the power is supplied to the node interface unit that is going to be connected with the base plate.
- Before replacing a device in dual-redundant configuration, you must make sure that the other device is working normally.

E5.1 Replacing power supply units

WARNING

Before removing a power supply unit, you must shut off the power supply to the unit.

CAUTION

Be aware that the power supply units may be hot.

The following figure shows the replacement of a power supply unit.

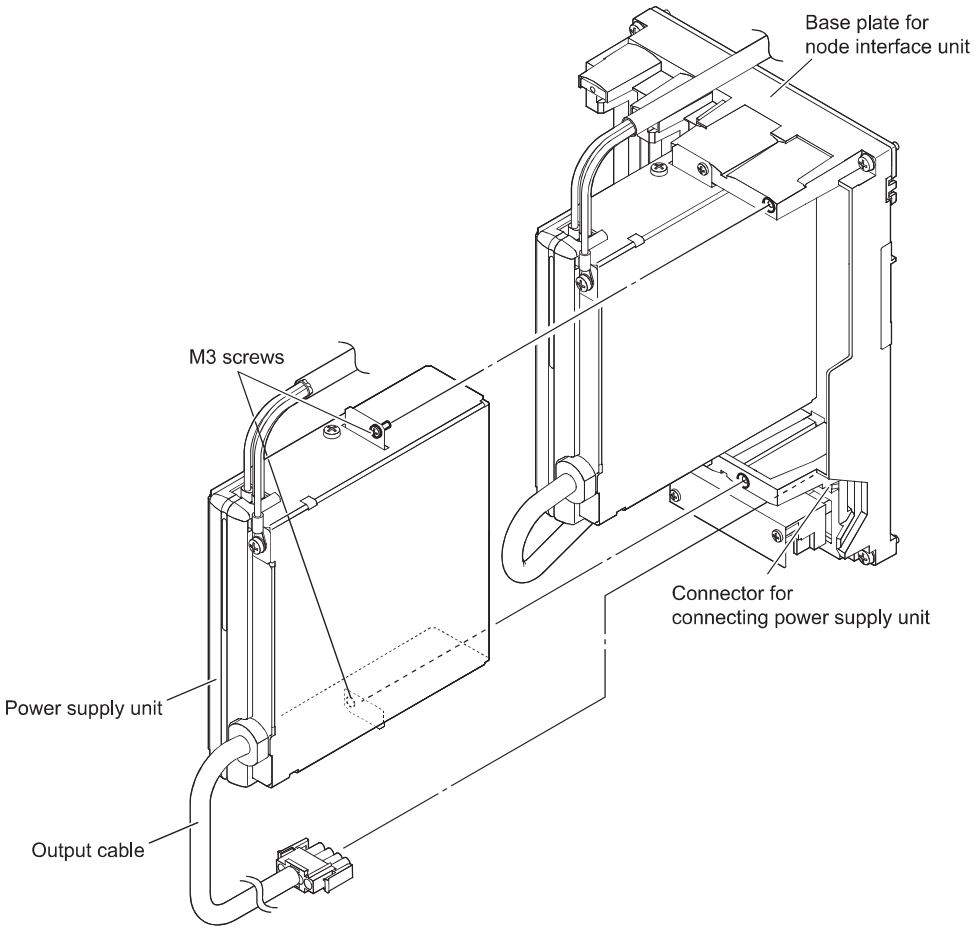


Figure E5.1-1 Replacing power supply units

Follow these steps to replace the power supply unit that has power supply:

1. Before removing a power supply unit, you must shut off the power supply to the unit. The power lamp turns off.
2. Remove the cover of the node interface unit.
3. Disconnect the output cable of the power supply unit from the connector for connecting power supply unit on the base plate for node interface unit.

4. Loosen the two M3 screws and remove the power supply unit.
5. Mount the new power supply unit on the base plate for node interface unit securely by tightening the two M3 screws.
6. Connect the output cable of the power supply unit to the connector for connecting power supply unit on the base plate for node interface unit.
7. Attach the cover of the node interface unit.
8. Supply power to the power supply unit.
   The power lamp turns on.

SEE ALSO For more information about removing and attaching the cover of the node interface unit, refer to:

"● Cover" on page B5-2

E5.2 Replacing N-ESB bus modules

CAUTION

Be aware that the N-ESB bus modules may be hot.

The following figure shows the replacement of an N-ESB bus module.

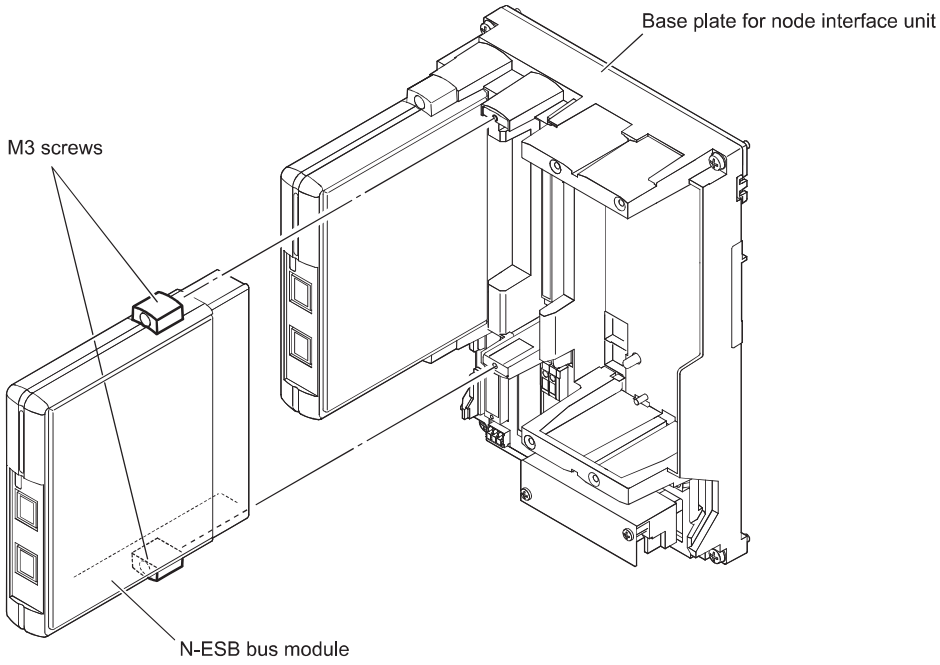


Figure E5.2-1 Replacing N-ESB bus modules

Follow these steps to replace an N-ESB bus module:

1. Disconnect the communication cable from the N-ESB bus module to be replaced.
   If the disconnected cable is a fiber-optic cable, put a cap to keep it away from dust.
2. Loosen the two M3 screws and remove the N-ESB bus module.
3. Mount a new N-ESB bus module on a base plate for node interface unit securely by tightening the two M3 screws.
   The STAT lamp turns on.
4. Make sure that the node number is set correctly.
5. Connect the communication cable to the N-ESB bus module.

TIP

When you mount the new N-ESB bus module, the node number is automatically copied from the other N-ESB bus module.

E5.3 Replacing N-IO I/O modules

The replacement of an N-IO I/O module is explained divided into two cases of dual-redundant configuration and non-redundant configuration.

Replacement procedure for a dual-redundant configuration

The procedure for replacing an N-IO I/O module differs depending on whether you replace a standby module or an active module.

When replacing a module on a standby side

This section describes how to replace the N-IO I/O module on the dual-redundant standby side. The procedure here assumes that the module that has a hardware error is installed in slot 1 of a base plate.

CAUTION

Be aware that the modules may be hot.

Follow these steps to replace a standby module:

1. Confirm that the status lamps of the N-IO I/O module are as follows:

	Slot 1	Slot 2
STATUS	Off	On
ACT	Off	On
DX	On	On

2. Loosen the two M3 screws and remove the module in the slot 1.

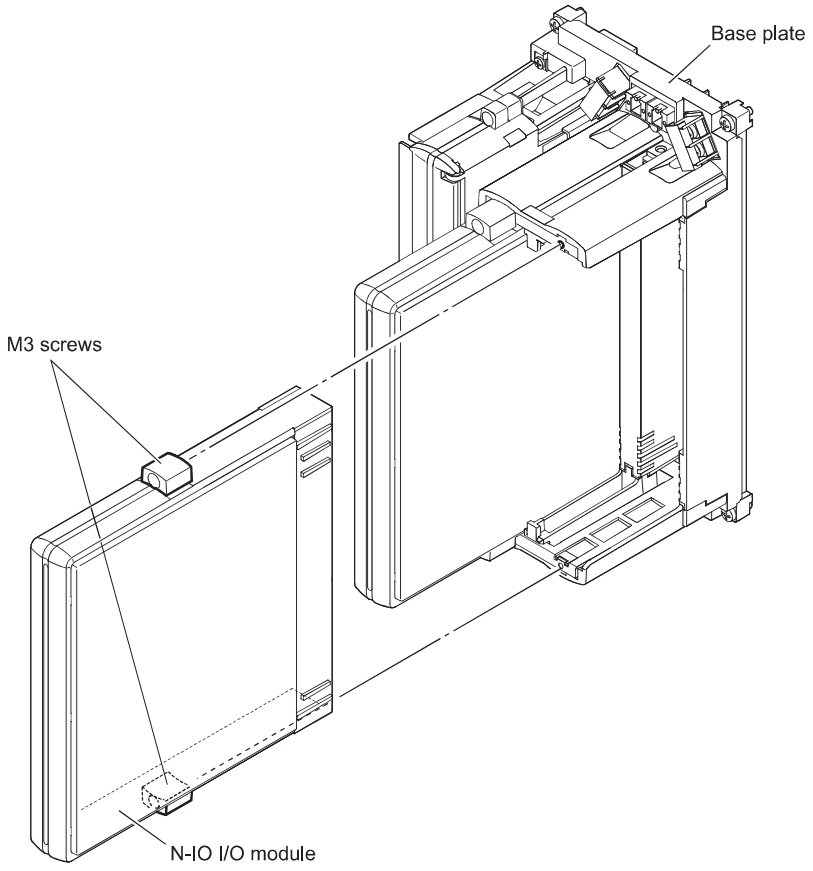


Figure E5.3-1 Example of replacing an N-IO I/O module

3. Tighten the two M3 screws and install the new module in slot 1 of the base plate. The STATUS lamp of the slot 1 module turns on.
4. Download an IOM for the module in the slot 1. If Automatic IOM Download is set to [Enable] in the SCS Constants Builder, IOM download is performed automatically.(*1) When the IOM download is complete and the module starts normally, the module in the slot 1 acts as the standby module.

*1: If it is not set to download automatically, execute the IOM download from the SCS State Management window of the SCS Maintenance Support Tool.

SEE ALSO For more information about the SCS Constants Builder, refer to:

C1.2.6, “SCS Constants Builder” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

When replacing a module on the active side

This section describes how to replace the active module of a redundant pair of N-IO I/O modules. The procedure here assumes that the active module is installed in slot 1 of a base plate.

CAUTION

Be aware that the modules may be hot.

Follow these steps to replace an active module:

1. Confirm that the status lamps of the N-IO I/O module are as follows:

	Slot 1	Slot 2
STATUS	On	On
ACT	On	Off
DX	On	On

2. For the module in slot 1, use the IOM Control Right Switching Tool to make a switchover to the standby module.
   The ACT lamp of the slot 1 module turns off, and the ACT lamp of the slot 2 module turns on.
3. Loosen the two M3 screws and remove the module in the slot 1.
4. Tighten the two M3 screws and install the new module in slot 1 of the base plate.
   The STATUS lamp of the slot 1 module turns on.
5. From the SENG, perform an IOM download for the module in the slot 1. If Automatic IOM Download is set to [Enable] in the SCS Constants Builder, IOM download is performed automatically.(*1)
   When the IOM download is complete and the module starts normally, the module in the slot 1 acts as the standby module.

*1: If it is not set to download automatically, execute the IOM download from the SCS State Management window of the SCS Maintenance Support Tool.

SEE ALSO For more information about the SCS Constants Builder, refer to:

C1.2.6, “SCS Constants Builder” in Engineering Guide Vol. 1 (IM 32P01C10-01EN)

Replacement procedure for a non-redundant configuration

Follow these steps to replace the N-IO I/O module in non-redundant configuration:

1. Confirm that the status lamps of the N-IO I/O module are as follows:

STATUS	Off
ACT	On
DX	Off

2. Loosen the two M3 screws and remove the module.
3. Tighten the two M3 screws and install the new module to the base plate.
   The STATUS lamp turns on.
4. From the SENG, perform an IOM download for the module.
5. Make sure that the hardware of the replaced module is working properly.

E6. Replacing the cables

This section describes how to replace the following cables:

- ESB bus cables
- Cables for optical ESB bus
- Cables for N-ESB bus

E6.1 Replacing ESB bus cables

Follow these steps to replace the ESB bus cable (Model: YCB301):

1. During replacement of ESB bus cables, the corresponding ESB bus becomes error. For an instance, when changing the Bus 1 cable, make sure that the communication to all SNUs and I/O modules on Bus 2 are working properly.
2. Disconnect the ESB bus cable from the ESB bus coupler module or the ESB bus interface module of Bus 1.
3. Exchange the ESB bus cables.
4. Connect the new ESB bus cable to the module. The tightening torque of the screws on the ESB bus cable connector should be 0.3 N·m.
5. Make sure that the replaced hardware is working properly.

E6.2 Replacing fiber-optic cables for optical ESB bus

Follow these steps to replace fiber-optic cables:

1. Disconnect the fiber-optic cable to be replaced from the module. Cap the cable to prevent dust infiltration.
2. Exchange the fiber-optic cables.
3. Uncap the replaced fiber-optic cable and connect it to the original port of the module. The connector for connecting fiber-optic cables has an IN port and an OUT port. Be sure you connect the cable to the correct port.
4. Check the diagnostic information window on the SENG for any errors.

E6.3 Replacing N-ESB bus cables

Follow these steps to replace the N-ESB bus cables:

1. Confirm that communication with all N-IO nodes is performed normally on the ESB bus that is not to be replaced.
2. Disconnect the N-ESB bus cable from the N-ESB bus coupler module or N-ESB bus module.
3. Connect the new cable to the original port of the module.
4. In the diagnostic information window on SENG, confirm that communication is performed normally on the N-ESB bus for which you have replaced the cable.

Hardware User's Guide

IM 32P06C10-01EN 9th Edition

INDEX

A

air deflector
- attach....C1-3

B

base plate
- base plate for barrier
  - configuration....B5-14
  - installation....C1-19
  - replacing the fuse....E3-19
  - signal connection to S2BN4D....D2-9
  - signal connection to S2BN5D....D2-10
- base plate with disconnecting terminals
  - configuration....B5-10
  - installation....C1-16
  - mounting on a DIN rail....C1-16
  - mounting/removal on/from a wall....C1-17
  - removal from a DIN rail....C1-16
  - replacing the fuse....E3-20
  - signal connection....D2-5
- field power supply or barrier power supply wiring....C2-16
- ground wiring....C2-13
- intrinsic safety barrier....B5-19
  - mounting....C1-24
- power supply cable for base plates....B5-21
- system power supply wiring....C2-15
- terminal block
  - connecting cables to pressure clamp terminals....D2-3, D3-2
  - connecting cables to spring clamp terminals....D2-3
  - mounting....C1-27

base plate for node interface unit
- configuration....B5-4
- external alarm input terminal
  - signal connection....D3-1
- ground wiring....C2-9

battery....B4-7
- replacement....E3-4-E3-6

C

connecting cables for Vnet/IP....C3-2

connector cover for MIL cable....B4-32

E

ESB bus
- cable connection....C3-4
- cable replacement....E6-2

ESB bus coupler module
- configuration....B4-12
- replacement....E4-8

ESB bus interface module
- configuration....B4-14
- replacement....E4-10

external interface unit....B4-41

F

F-SB bus cable
- configuration....B5-21
- connection....C3-17

FIO I/O module
- analog I/O module
  - configuration....B4-22
  - signal connection....D1-12
- communication module....B4-27
  - Ethernet communication module
    - configuration....B4-28, B4-29
    - signal connection....D1-53
  - fire and gas communication module
    - signal connection....D1-54
  - RS-232C communication module
    - configuration....B4-27
    - signal connection....D1-42
  - RS-422/RS-485 communication module
    - configuration....B4-27
    - signal connection....D1-48
- digital I/O module
  - configuration....B4-25

replacing the fuse of digital input module E3-12
signal connection....D1-22
replacement....E4-13
type of signal connection....D1-2

I

installing the field power supply unit....C1-29

M

MIL connector
signal connection....D1-6
terminal numbers and signal names
for analog I/O module....D1-13
for digital I/O module....D1-23

N

N-ESB bus
cable connection....C3-11
cable replacement....E6-4
N-ESB bus coupler module
configuration....B4-19
replacement....E4-9
N-ESB bus module
configuration....B5-6
replacing....E5-4
N-IO I/O module
configuration....B5-17
mounting....C1-22
replacement....E5-5
N-IO I/O unit
ground and power supply wiring....C2-13
installation....C1-15
signal connection....D2-1
N-IO node
components....B5-1
node fan unit....B4-42
fan unit
configuration....B4-42
replacement....E3-9
parts replacement....E3-9
power supply unit for fan unit
configuration....B4-42
ground wiring and power supply wiring....C2-3
replacement....E3-11
replacing the fuse....E3-10
node interface unit
configuration....B5-2
mounting on a DIN rail....C1-12
mounting/removal on/from a wall....C1-13
removal from a DIN rail....C1-13

O

optical ESB bus
cable connection (FIO node)....C3-5
cable connection (N-IO node)....C3-13
cable replacement....E6-3
optical ESB bus repeater module
configuration....B4-16
replacement....E4-11

P

parts with defined life spans....E3-1
power supply module
configuration....B4-2
ground wiring and power supply wiring....C2-2
replacement....E4-2
power supply unit
configuration....B5-5
ground wiring....C2-10
output wiring....C2-12
power supply wiring....C2-10
replacing....E5-2
precautions against static electricity during maintenance work....E1-1
pressure clamp terminal block
configuration....B4-31
signal connection....D1-4
terminal numbers and signal names
for analog I/O module....D1-13
for digital I/O module....D1-23
processor module
configuration....B4-4
replacement....E4-4
replacing the battery....E3-4-E3-6

R

relay board....B4-38
DIN rail mountable
configuration....B4-39
connecting the field power supply cable....C2-4
installation....C1-7
rack mountable
configuration....B4-38
installation....C1-5
replacing the fuse....E3-18
signal connection....D1-7
terminal numbers and signal names....D1-34
replacement parts....E3-1
routine maintenance....E1-1, E2-1

S

safety control station (SCS)
components....B-1
installation and wiring....C-1
maintenance....E-1
signal wiring....D-1
system configuration....A-1
safety control unit (SCU)
configuration....B1-1
ground wiring....C2-5
installation....C1-2
safety node unit (SNU)
addition....E4-20
configuration....B2-1
ground wiring....C2-5
installation....C1-2
removal....E4-22
replacement....E4-19

T

terminal board (for FIO node) B4-33
DIN rail mountable
configuration....B4-35
connecting the field power supply cable....C2-4
installation....C1-7
precautions for installation....C1-11
rack mountable
configuration....B4-33
installation....C1-5
replacing the fuse....E3-13
signal connection....D1-7
terminal numbers and signal names
for analog I/O module....D1-17
for digital I/O module....D1-27
terminal board (for N-IO node) B5-20
connecting cables to pressure clamp terminals....D2-3, D3-2
connecting with a base plate D2-1
installation C1-28

U

unit for optical bus repeater module
configuration....B3-1
ground wiring....C2-5
installation....C1-2

W

wiring check adapter for digital input....B6-2

Revision Information

Title : Hardware User's Guide

Manual No. : IM 32P06C10-01EN

Dec. 2023/9th Edition/R4.10 or later

Introduction	Deleted "■ Requirements for Installation" and "■ Measurement Categories" from "Installation and Maintenance Notes." Deleted "Guidelines for Selecting a Power Supply Unit."
E3	Updated the table of parts with defined life spans.

Jan. 2022/8th Edition/R4.07

Entire manual	Updated descriptions based on a notice of alterations.
E3.1	Added descriptions on waste batteries.

Feb. 2021/7th Edition/R4.06

Introduction	Deleted descriptions of conformity standards.
Entire manual	Added modules for SCSs that support SIL 2.

Dec. 2019/6th Edition/R4.05

Entire manual	Updated descriptions based on a notice of alterations.
Introduction	Updated descriptions of conformity standards. Updated descriptions of registered trademarks.
B1	Added descriptions of S2SC70.
B4.2	Added descriptions of S2CP471.
E3	Added descriptions of life-limited parts.
E3.1	Added descriptions of battery replacement procedure.
E4.3	Added descriptions of S2CP471 replacement procedure.

Aug. 2018/5th Edition/R4.04

Introduction	Updated the description of registered trademarks of YOKOGAWA.
D2.1	Changed the caution for connecting inductive load.

Oct. 2017/4th Edition/R4.03.10

Introduction	Added some standards to the table of standards that the Product conforms to.
B4.7.3, D1.4.4	Added descriptions of the fire and gas communication module.
E2	Added descriptions of inspection by checking status lamps.
E3	Added relays for replacement to the table of parts with defined life spans.
E3.5	Added procedures for replacing relays of relay boards.

May 2017/3rd Edition/R4.03

Entire manual	Added S2MDV843. Changed "Analog digital I/O module" to "N-IO I/O module."
B4.7.1	Added descriptions to the status lamps of analog I/O modules.
B5	Added descriptions of system models.
E2	Added descriptions to inspection by checking status lamps.

Oct. 2016/2nd Edition/R4.02

Entire manual	Changed the symbols that indicate warning and caution.
Introduction	Updated descriptions of requirements for installation.
C1.3	Added descriptions of how to mount/remove the node interface unit on/from a DIN rail.
C1.4.1	Added descriptions of how to mount/remove the base plate with disconnecting terminals on/from a DIN rail.

Dec. 2015/1st Edition/R4.01

Newly published

■ For Questions and More Information Online Query: A query form is available on the following URL for online query. http://www.yokogawa.com/iss
■ Written by Yokogawa Electric Corporation
■ Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Attachment 9.12 Safety Instrumented System ProSafe-RS System Overview TI 32P01A10-01EN

Technical Information

Safety Instrumented System
ProSafe-RS
System Overview

TI 32P01A10-01EN

[Release 4]

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

TI 32P01A10-01EN
©Copyright Dec. 2015 (YK)
3rd Edition Dec. 2018 (YK)

Blank Page

Introduction

ProSafe-RS is a safety instrumented system conforming to IEC 61508. This technical information (TI) document introduces various features and functions of the ProSafe-RS.

Document Structure

An overview of the ProSafe-RS system is described in this TI. After reading this TI, go over to read other documents such as General Specifications (GS) or Instruction Manuals (IM) for more details.

This TI consists of five chapters. Chapter 1 discuss about the importance of safety instrumented system, while the remaining chapters will explain the features of ProSafe-RS, system configuration, safety control station, engineering, operation and maintenance.

Reference Documents

Refer to the following document for a system integrated with CENTUM VP.

- Integrated Production Control System CENTUM VP System Overview (General Overview) (TI 33J01A10-01EN)

Target Readership

- Managers who are considering introduction of a new safety instrumented system.
- Instrumentation, power and computer engineers who evaluate for purchasing or installation of ProSafe-RS.

Representation of Drawings

- Drawings in this TI may be emphasized, simplified, or omitted some features for convenience of explanations.
- The screen captures may be slightly modified for the convenience of the better understanding without disturbing the functional understanding or operation and monitoring.

Trademarks

- ProSafe, CENTUM, PRM, STARDOM, FAST/TOOLS, Exaopc, FieldMate, and Vnet/IP are either registered trademarks or trademarks of Yokogawa Electric Corporation.
- Other company and product names appearing in this document are registered trademarks or trademarks of their respective holders.
- TM or ® mark are not used to indicate trademarks or registered trademarks in this document.
- Logos and logo marks are not used in this document.

All Rights Reserved Copyright © 2015, Yokogawa Electric Corporation

Blank Page

Safety Instrumented System
ProSafe-RS
System Overview

TI 32P01A10-01EN 3rd Edition

CONTENTS

1. Necessity of Safety Instrumented System 1-1
2. Features of the ProSafe-RS 2-1
3. System Configuration of the ProSafe-RS 3-1
   - 3.1 Typical configuration 3-1
   - 3.2 Integration with the CENTUM VP 3-3
   - 3.3 Communications among stations 3-5
4. Safety Control Station (SCS) 4-1
   - 4.1 Hardware configuration of the SCS 4-1
   - 4.2 Safety control unit (SCU) 4-2
   - 4.3 N-IO node, N-IO field enclosure, and safety node unit (SNU) 4-3
5. Engineering and Operation & Maintenance 5-1
   - 5.1 Engineering 5-1
   - 5.2 Operation and maintenance of SCS 5-6
   - 5.3 Sequence of events recorder (SOER) 5-9

Blank Page

1. Necessity of Safety Instrumented System

In this chapter, a plant owner's responsibility, the international standards, positioning of a safety instrumented system and safety evaluation scales are explained.

Plant owner's responsibility

During 1970s and 1980s, serious incidents that occurred at petroleum and chemical plants initiated several countries to legislate that "owners of industrial plants where dangerous materials are handled must evaluate possible risks that may occur in the plants."

These legal regulations stipulate that the plant owners are socially responsible in the entire lifecycle, from planning to disposal, to minimize the risks of causing hazards over "human beings, physical assets and environments." In order to fulfill these social responsibilities, the plant owners are expected to identify risk factors of hazardous elements that cause incidents; to analyze and evaluate them; then to reduce the risks to a socially acceptable level.

The international standards of IEC 61508 and IEC 61511 defined procedures of how to identify, analyze and evaluate risks, then implement the risk reduction measures based on legal regulations of several countries.

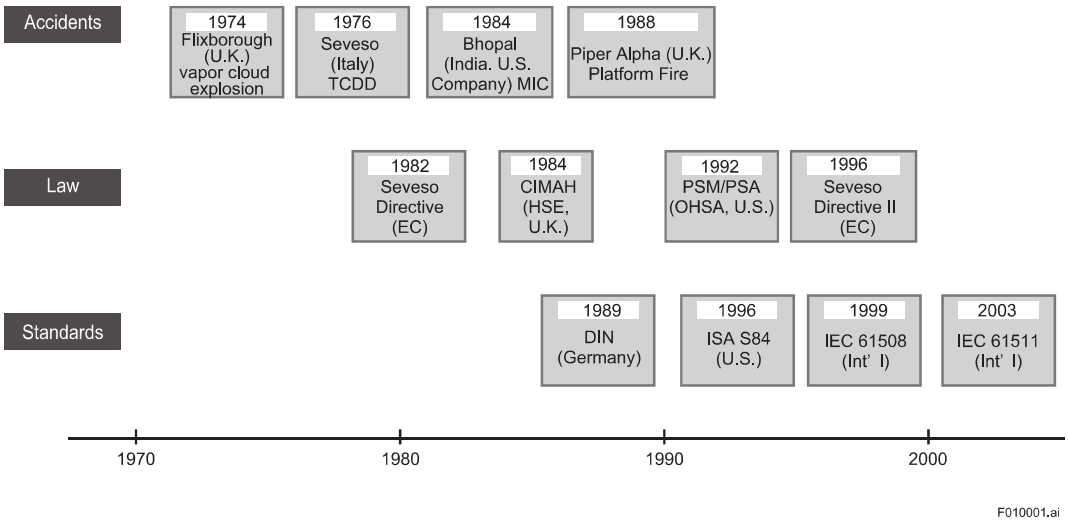


Figure Flow from incidents to standardization

IEC 61508 / IEC 61511 international standards

The IEC 61508 defines the basic safety standard for functional safety for all industries. The IEC 61511 is dedicated for the process industry, in reference to the IEC 61508. These safety standards for functional safety are not established on the premise of “100% accident free,” but with some risks always remain. By converting the risks into numerical value by the globally standardized scale, the necessity and effectiveness of safety measures can be verified.

Positioning of the safety instrumented system in the viewpoint of layer of protection

A “layer of protection” approach is adopted as the basis of securing the plant safety that is to reduce risks by combining independent protection layers with the international standards of the IEC 61511, as shown below. Each protection layer has to be independent from each other, sets quantitative target for reducing risks, and establishes means of achieving these goals.
A safety instrumented system is positioned in the prevention layer for reducing the risk of hazardous event occurrence and the mitigation layer for mitigating the influence of a hazardous incident that has occurred.

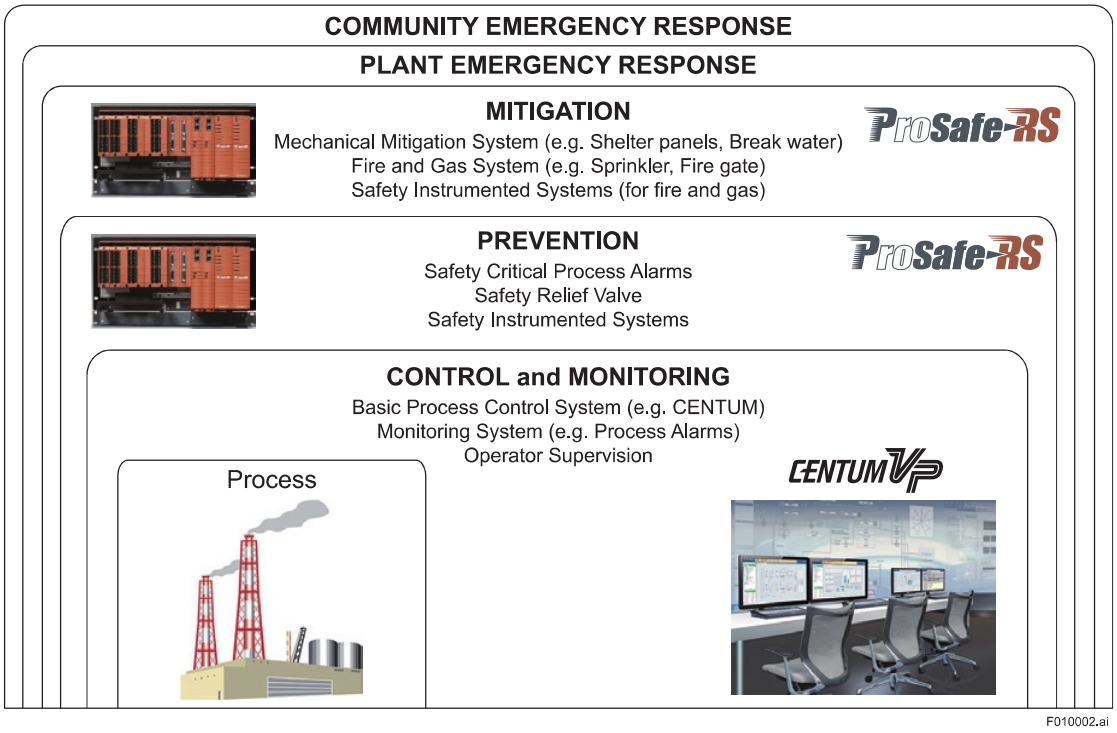


Figure The layer of protection

In order to work out countermeasures for risks based on the layer of protection, risk assessments to the plant must be implemented and essential risk levels inherent in the process must be calculated. (1) In order to reduce the risks to a socially permissible risk level, multiple layers of protection have to be assigned. (2) The figure below shows reducing the risks to the tolerable level by combining external mitigation facilities (e.g. shelter panels, breakwaters, etc.); a process control system (e.g. CENTUM); and a safety instrumented system for emergency shutdown (ESD).

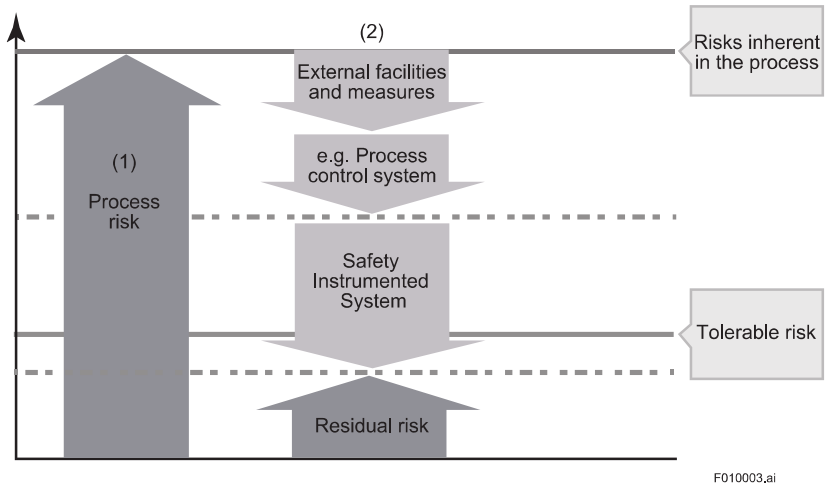


Figure The risk reduction level of the plant

Safety evaluation scales

The IEC 61508 introduces the Safety Integrity Level (SIL) as a method of describing the safety integrity requirements required at each layers of protection. The SIL is classified into four levels according to the value of average Probability of a dangerous Failure on Demand (PFDavg). The PFDavg of manual operation is 1/10 or so, which means a failure may occur out of 10 operation requests and unable to perform its safety operation.

On the other hand, a safety instrumented system reduces the probability of failures as low as possible by enhancing its self-diagnosis function and failure analysis. This means a safety instrumented system with the SIL3 guarantees to perform the operation compared with manual operations.

Table Safety integrity level (SIL)

SIL	PFDavg	Description
4	$\geq 10^{-5}$ to $<10^{-4}$	Frequency of risk occurrence is reduced to the ranges in between 1/10000 and 1/100000 under the current conditions.
3	$\geq 10^{-4}$ to $<10^{-3}$	Frequency of risk occurrence is reduced to the ranges in between 1/1000 and 1/10000 under the current conditions.
2	$\geq 10^{-3}$ to $<10^{-2}$	Frequency of risk occurrence is reduced to the ranges in between 1/100 and 1/1000 under the current conditions.
1	$\geq 10^{-2}$ to $<10^{-1}$	Frequency of risk occurrence is reduced to the ranges in between 1/10 and 1/100 under the current conditions.

2. Features of the ProSafe-RS

This chapter describes about the features of the ProSafe-RS safety instrumented system which conforms to the Safety Integrity Level 3 (SIL3) defined by the IEC 61508.

Achieving SIL3 in single configuration

ProSafe-RS is a safety instrumented system which achieves the SIL3 in a single configuration and its performance is certified by TÜV Rheinland, an external certification organization.

Each of the processor and input/output modules of the ProSafe-RS contain built-in computation matching function and self-diagnostic function, which keeps the modules failure rates to extremely low. The ProSafe-RS flexibly complies with customers' requirements with its single configuration and the SIL3 certification.



Certificate

TÜVRheinland CERTIFIED

Product Safety
Functional Safety

www.tuv.com
ID 0000000000

No.: 968/EZ 196.39/16

Product tested	Safety Control System ProSafe-RS	**Certificate holder**	Yokogawa Electric Corporation 2-9-32 Nakacho Musashino-shi Tokyo 180-8750 Japan

Type designation
ProSafe-RS, R4.01,
The actual revision and official list of the product documentation, hardware components and software modules have to be considered. Please refer to the "Revision Release List" published on http://www.fs-products.com/

Codes and standards
IEC 61508 Parts 1-7:2010
EN 50156-1:2015
EN 298:2012
IEC 62061:2015
IEC 61131-6:2012
IEC 61511 Parts 1-3:2004
NFPA 72:2016
NFPA 85:2015
NFPA 86:2015
EN 54-2:1997 + AC:1999 + A1:2006
IEC 61131-2:2007
IEC 61326-3-1:2008
EN 61000-6-2:2005

Intended application
Safety related and high availability applications such as:

Emergency Shutdown System (ESD), Process Shutdown System (PSD), Burner Management System (BMS), where the safe state is the de-energized state. Fire and Gas System (F&G)applications, where the demand state is the de-energized or the energized state.
The safety control system complies with the requirements of the relevant standards (SIL 3 acc. to IEC 61508 and SILCL 3 acc. to IEC 62061) and can be used in applications up to SIL 3.

Specific requirements
The instructions of the associated Installation and Operating Manual shall be considered.

Valid until 2021-02-04
The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/EZ 196.39/16 dated 2016-02-04.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2016-02-04
Certification Body Safety & Security for Automation & Grid
Dipl.-Ing. Heinz Gall

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

F020001.ai

Redundancy achieves higher reliability

ProSafe-RS allows selecting dual-redundant module configurations in order to achieve higher reliability. Since the system already achieves SIL3 with a single configuration, the SIL3 is maintained even when one of the modules fails.

System integration with CENTUM VP

By integrating with the CENTUM VP system, the operation status of the ProSafe-RS are monitored on the CENTUM VP's operation and monitoring screen. ProSafe-RS and CENTUM VP synchronize time, share data, and notify event & alarm in a single step.

Segregating functions of CENTUM VP from ProSafe-RS

International safety standards require that control and safety functions are independent of each other. Even when the ProSafe-RS and the CENTUM VP systems are integrated, the control and the safety functions are securely segregated. The operation of the CENTUM VP has no influence over safety functions of the ProSafe-RS.

Connecting with other systems

The operating status and data of the ProSafe-RS can be referred to by a supervisory computer or Modbus master via an OPC interface (*1), or a Modbus slave communication. Furthermore, the subsystem data such as sequencers can be set or referred by the ProSafe-RS via a Modbus communication.

*1: The OPC is a way of communication among standard applications of Windows OS applied to process control. The OPC enables to send/receive process data among multiple Windows applications.

Security measures

The ProSafe-RS is accredited with the ISASecure Embedded Device Security Assurance (EDSA) of the ISASecurity Compliance Institute (ISCI), an international accreditation organization. The exida, an American accreditation organization certified by the ISASecure EDSA performed the Communication Robustness Test (CRT), the Fabricated Security Assessment (FSA) and the Software Development Security Assessment (SDSA). Then the ISCI evaluated and verified the conformity to the standard. The ISASecure EDSA certification certifies that the ProSafe-RS's controllers have adequate security measures against threats of cyberattacks.



F020002.ai

Figure ISASecure EDSA certification

3. System Configuration of the ProSafe-RS

In this chapter the system configuration of the ProSafe-RS is explained. The ProSafe-RS consists of Safety Control Station (SCS), Safety Engineering Station (SENG), Automation Design Server (AD Server) and others. AD Server is a Database Server which preserve the project data in a system. A minimum configuration system consists of an SCS and a SENG (including an AD Server).

3.1 Typical configuration

The figure below shows an example of the ProSafe-RS system configuration.

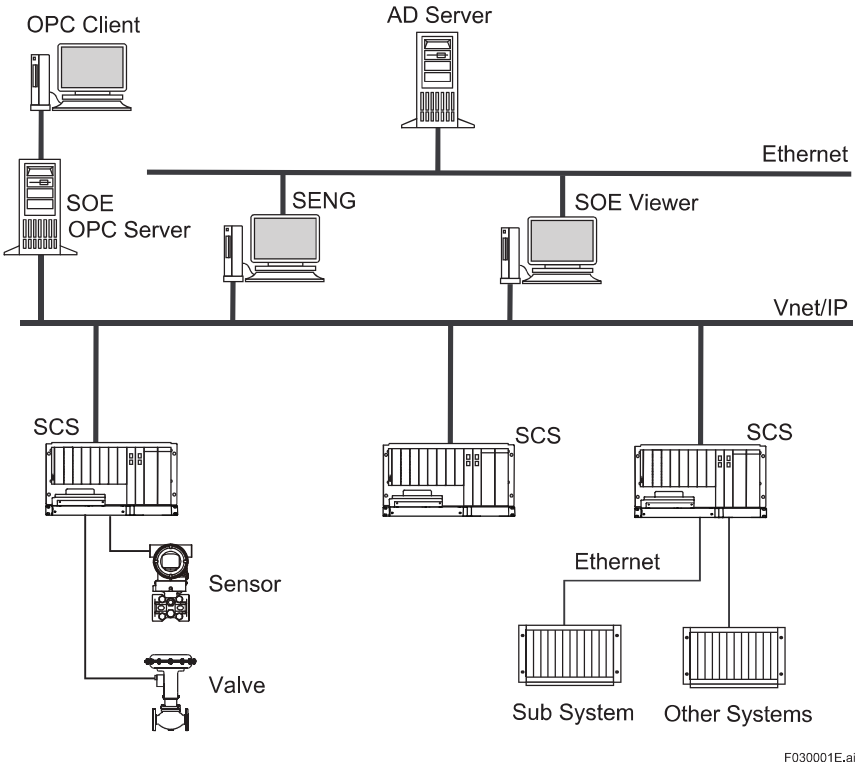


Figure Example of ProSafe-RS system configuration

Safety control station (SCS)

An SCS is a controller to perform safety control of the ProSafe-RS.

Main features

- Executes safety control function
- Receives input datas from field devices
  (e.g. temperature, pressure, flow, ON/OFF status of a switch)
- Transmits output instructions to field devices
  (e.g. open/close of valves, instruction of equipments' ON/OFF)
- Performs inter-station communications
  (e.g. inter-SCS safety communication, SCS link transmission safety communication)
- Communicates with field devices (HART communication)
- Communicates with other systems
  (e.g. Modbus communication)

Safety engineering station (SENG)

The SENG is a computer for performing SCS's engineering and maintenance tasks.

Main features

- Creates and verifies safety control functions (application programs)
- Downloads the created application programs to SCSs
- Monitorings SCSs status
- Receives and displays alarm messages from SCSs

3.2 Integration with the CENTUM VP

The ProSafe-RS and the CENTUM VP systems can be integrated. The figure below shows an example of a system configuration that the ProSafe-RS and the CENTUM VP are integrated.

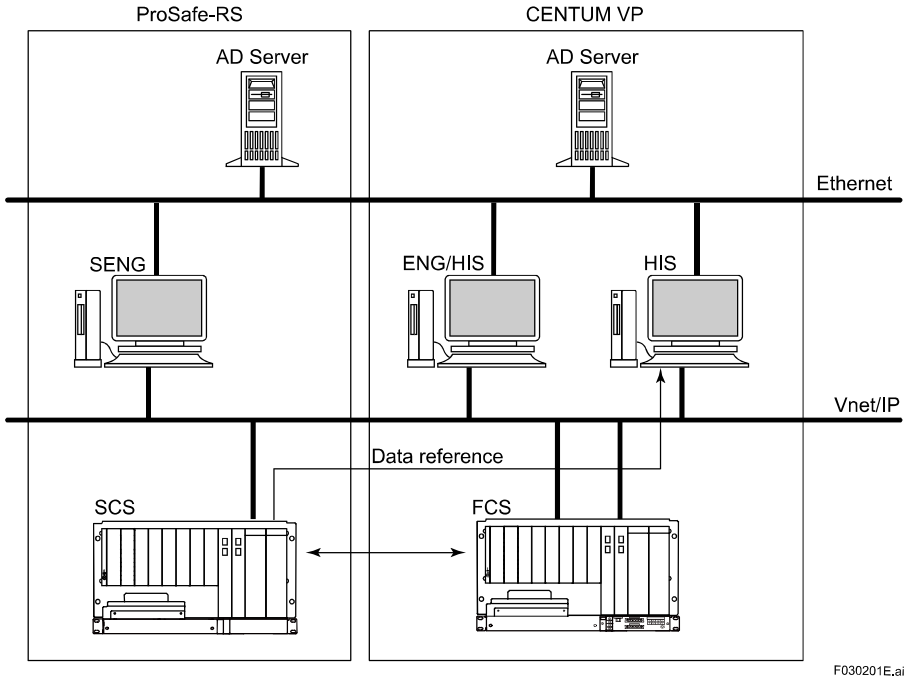


Figure System configuration example of ProSafe-RS integration with CENTUM VP

HIS
An operation and monitoring station of CENTUM VP for operating a plant.

ENG
An engineering station to perform system configuration and maintenance management of the CENTUM VP.

FCS
A controller that controls a process.

- An HIS operates and monitors both FCSs and SCSs.
- The SCS's data can be referred from HISs or FCSs.
- The SENG performs engineering of SCSs and the ENG performs engineering of FCSs and HISs. The engineering of the CENTUM VP integration systems are performed by both the SENG and the ENG. The SENG, ENG and HIS functions can be resided on a single computer or independently installed on different computers.
- The SCS's data setting can be performed from HISs or FCSs; however, the data setting for the SCS is managed with the special security scheme.

System scale

In a ProSafe-RS and CENTUM VP integrated system, the maximum number of station that can be configured is as follows:

- Number of connectable domains: 16
- Number of connectable stations (*1) per domain: 64
- Number of connectable stations: 256

Note: For a Vnet/IP system configuration, refer to General Specifications of “ProSafe-RS Safety Instrumented System Overview (for Vnet/IP)” (GS 32P01B10-01EN).
*1: A station is a generic name for SENG, SCS, ENG, HIS and FCS.

3.3 Communications among stations

"Inter-SCS safety communication," "SCS link transmission safety communication," and "SCS global switch communication" are used for communications among control stations.

Inter-SCS safety communication

The Inter-SCS Safety Communication can be established between an SCS and another SCS (in the same or in the different domain). (*1) Transmission of essential data at the SIL3 level can be performed while maintaining the communication quality.

*1: In order to perform the Inter-SCS safety communication while inter-domain, the integration with CENTUM VP system is needed.

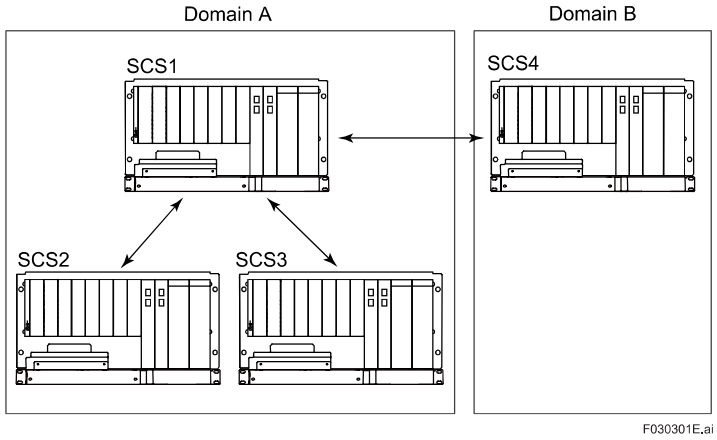


Figure Inter-SCS safety communication

SCS link transmission safety communication

The SCS Link Transmission Safety Communication is a safety communication to concurrently broadcast Boolean data from an SCS to multiple SCSs (in the same domain). By this communication, broadcasting of essential data at the SIL3 level can be performed.

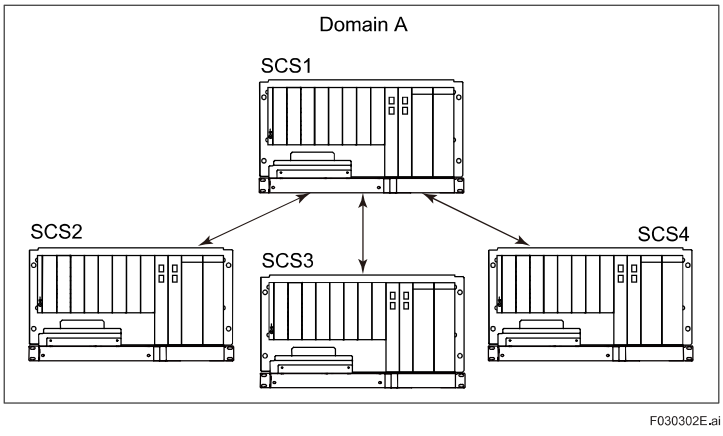


Figure SCS link transmission safety communication

SCS global switch communication

The SCS Global Switch Communication concurrently broadcasts data from an SCS to multiple FCSs, which is an interference-free communication that has no influence over safety control.

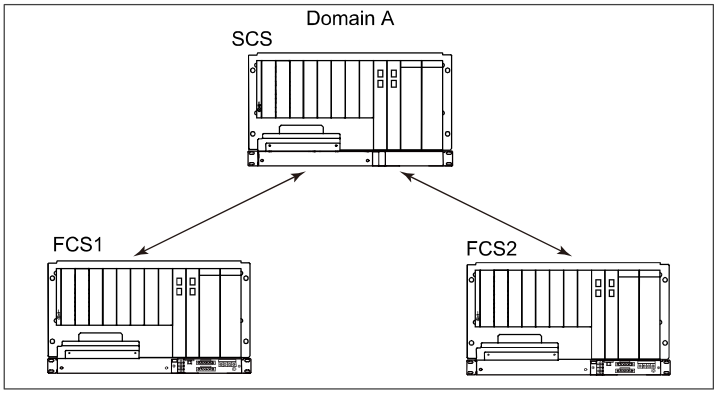


Figure SCS global switch communication

4. Safety Control Station (SCS)

This chapter explains the hardware configuration of a safety control station (SCS) that provides SIL3 in single configuration.

4.1 Hardware configuration of the SCS

The SCS is a safety controller of the ProSafe-RS. The SCS is composed of Safety Control Units (SCU), Safety Node Units (SNU) and N-IO Nodes. (including N-IO field enclosure) N-IO field enclosure is a standardized remote I/O enclosure for outdoor use, in which N-IO nodes are equiped.

The figure below shows an example of a system configuration.

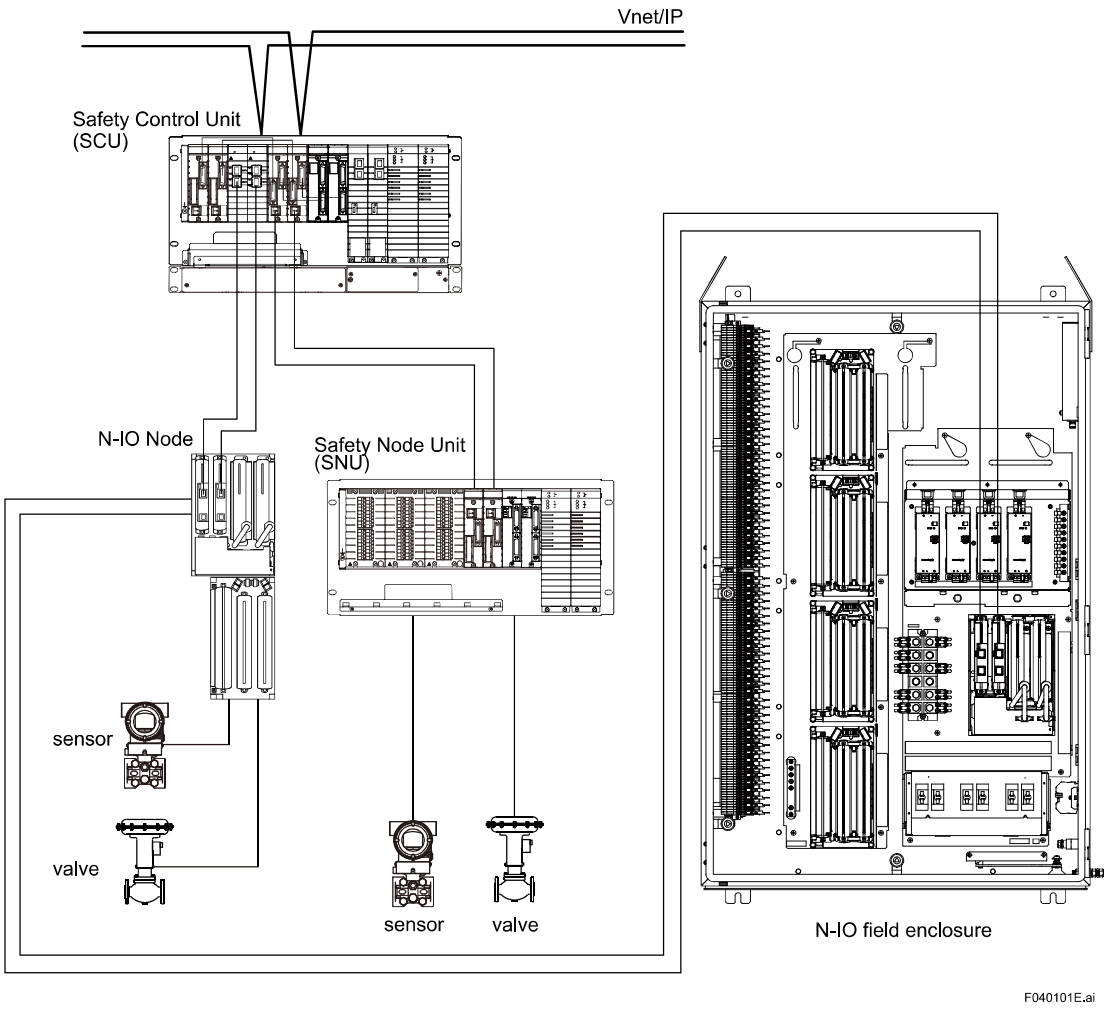


Figure System configuration example of SCS

4.2 Safety control unit (SCU)

Overview

The SCU implements safety control function by executing the application programs downloaded from the SENG. By using the Vnet/IP communication function, inter-station communications can be performed. Input/output modules mounted on SCU perform for input/output of field devices' data.

The input/output modules can be increased by adding safety node units and N-IO nodes.

The following types of the SCU are available.

S2SC70S/D: For large-scale systems or small to medium-scale systems, applicable to N-IO node

SSC60S/D: For large-scale systems or small to medium-scale systems

SSC57S/D: For wide-area systems such as oil and gas production facilities (wellheads) or small to medium-scale systems

SSC50S/D: For small to medium-scale systems

The following figure shows an example of the SCU configuration.

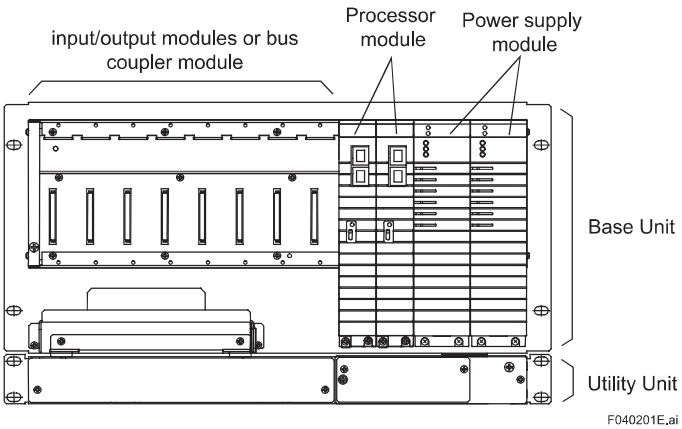


Figure Configuration of safety control unit (S2SC70D)

4.3 N-IO node, N-IO field enclosure, and safety node unit (SNU)

N-IO node

An N-IO node consists of an N-IO node interface units and N-IO Input/Output units. The N-IO node interface unit transmits field device signals received by the N-IO I/O unit to the SCU and the SCU data to field devices via an N-IO I/O unit. Input/output modules can be mounted on the N-IO I/O unit.

The figure below shows an example of N-IO node unit configuration.

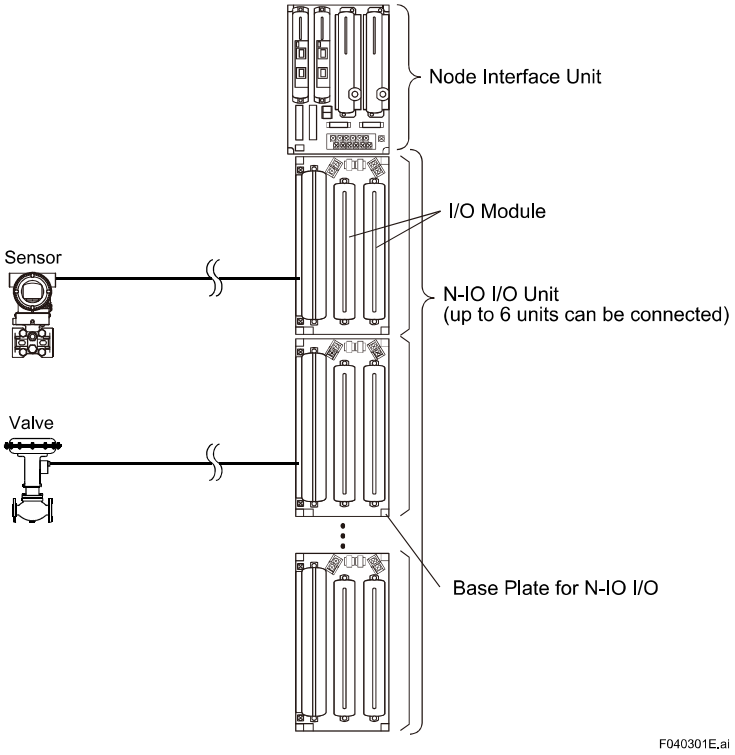


Figure System configuration N-IO node unit

Input/Output modules

AI, AO, DI, or DO signal can be assigned to the input/output modules by the channel by software.

Model	Function	Remarks
Analog Digital Input/Output Module		
S2MMM843	(AI) Analog Input	4-20 mA , HART Communication function, Module isolation
	(AO) Analog Output	4-20 mA , HART Communication function, Module isolation
	(DI) Digital Input	no-voltage contact, Module isolation
	(DO) Digital Output	24 V DC/0.66 A (*1), Module isolation
S2MDV843	(DI) Digital Input	no-voltage contact, Module isolation
	(DO) Digital Output	24 V DC/0.66 A (*1), Module isolation

*1: The maximum load current up to 2 A device can be connected to DO by multiple channels parallel use.

Field wiring

The terminal(s) provided with the N-IO input/output unit is used for wiring directly to field devices.

N-IO field enclosure

N-IO field enclosure is a standardized remote I/O enclosure for outdoor use, which provides the accessories including field power supply units with optimized design. The N-IO field enclosure consists of two components, one is a dedicated enclosure with terminal blocks and the other is a base unit with an N-IO node including field power supply units. It is possible to order the enclosure and the base unit individually.

Safety node unit (SNU)

The input/output modules can be mounted on the SNU, and the SNU transmits analog input signals and contact signals of field devices to the SCU.

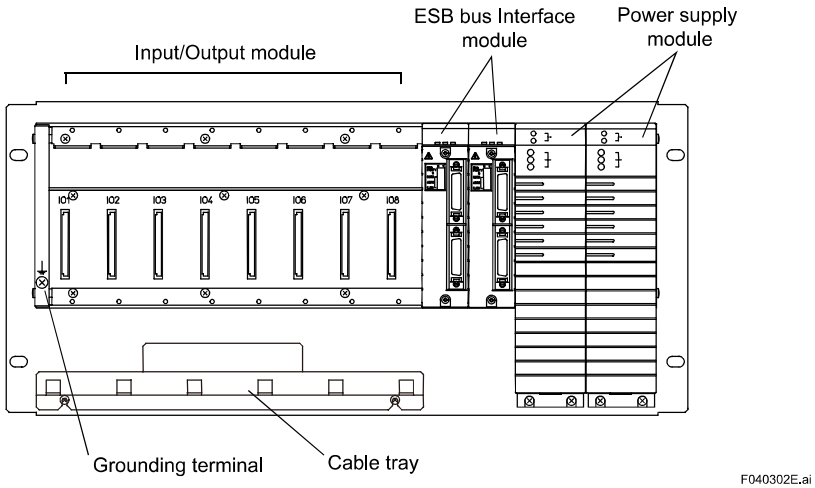


figure Configuration of safety node unit

Input/Output modules

The following table shows the input/output modules available for the ProSafe-RS. The input/output modules can take a dual-redundant configuration in order to improve the availability.

Table

Model	Name	Remarks
Analog Input/Output Modules		
SAI143	Analog input module	4-20mA, Module isolation, HART Communication function
SAV144	Analog input module	1 to 5 V/1 to 10 V, Module isolation
SAT145	TC/mV Input module	Isolated Channels
SAR145	RTD Input Module	Isolated Channels
SAI533	Analog output module	4-20mA, Module isolation, HART Communication function
Digital Input/Output Module		
SDV144	Digital input module	no-voltage contact, Module isolation
SDV521	Digital output module	24 V DC/2 A, Module isolation
SDV526	Digital output module	100-120 V AC, Module isolation
SDV531/SDV541	Digital output module	24 V DC, Module isolation
SDV53A	Digital output module	48 V DC, Module isolation
Communications Module		
ALR111/ALR121	Serial communication module	RS-232C, RS-422/RS-485
ALE111	Ethernet communication module	
S2LP131	Fire and Gas communication module	

Field wiring

For connecting a field device and an input/output module can be done by directly wiring using a pressure clamp terminal block or wiring via a terminal board using a cable-interface. Or, connecting a user-provided MIL cable with an MIL connector terminal block is available.

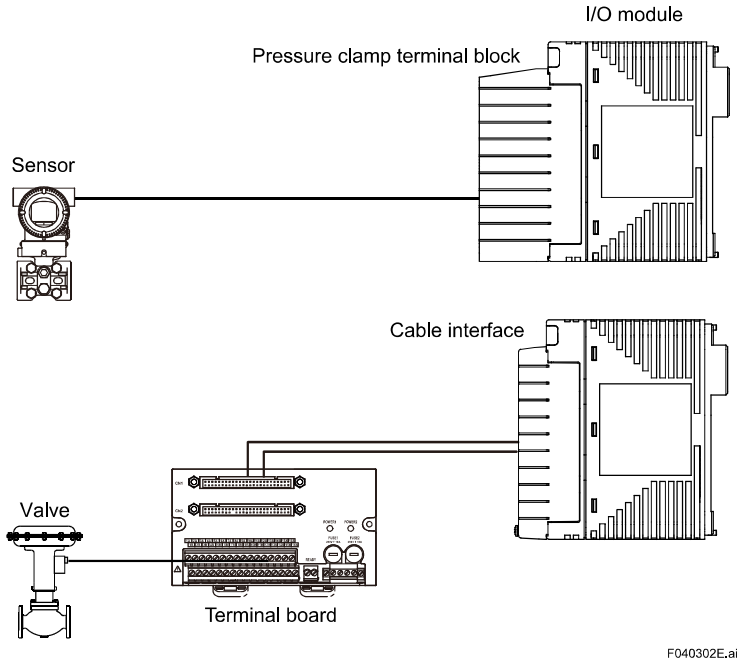


Figure Example of field wiring

5. Engineering and Operation & Maintenance

The engineering and operation & maintenance of the SCS are described in this chapter.

5.1 Engineering

Application logics need to be generated to activate ESD or fire and gas (FAG) protection systems.

Engineering procedure

The procedures of how to create applications to activate ESD or FAG systems as well as how to perform operational tests are as shown in the following figure.

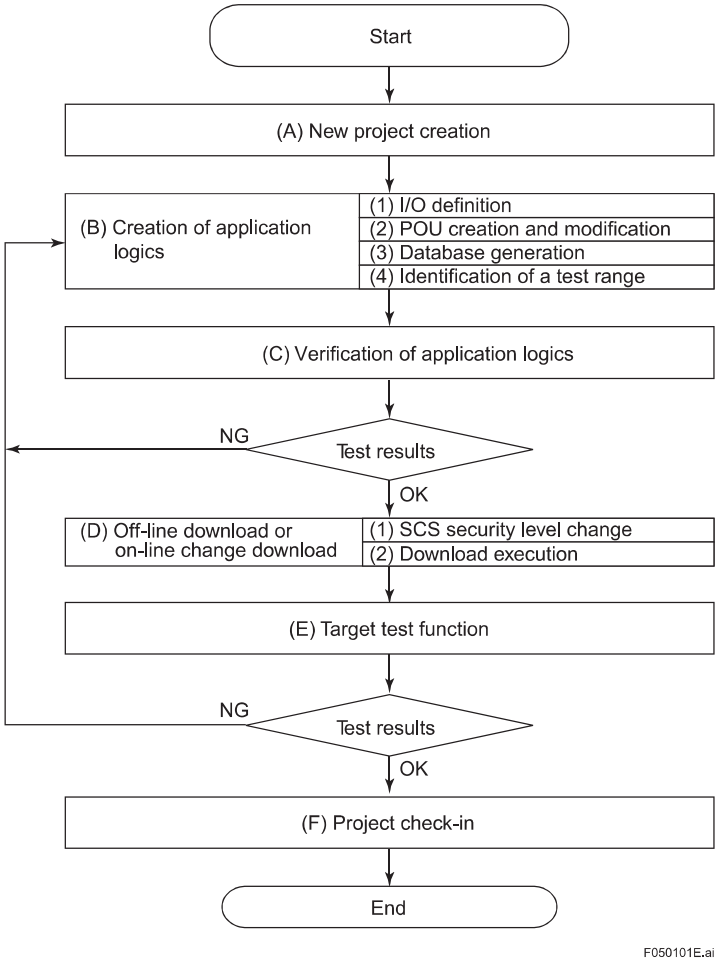


Figure Procedures for creating a ProSafe-RS standard application

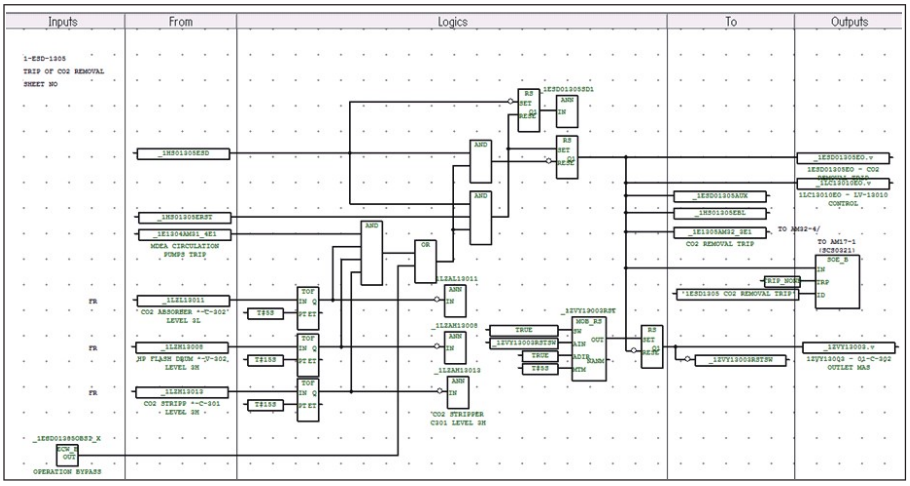
(A) New project creation

Create a new project to manage application logics. Creation of the application logic is enabled only after a creation of a new project.

(B) Creation of application logics

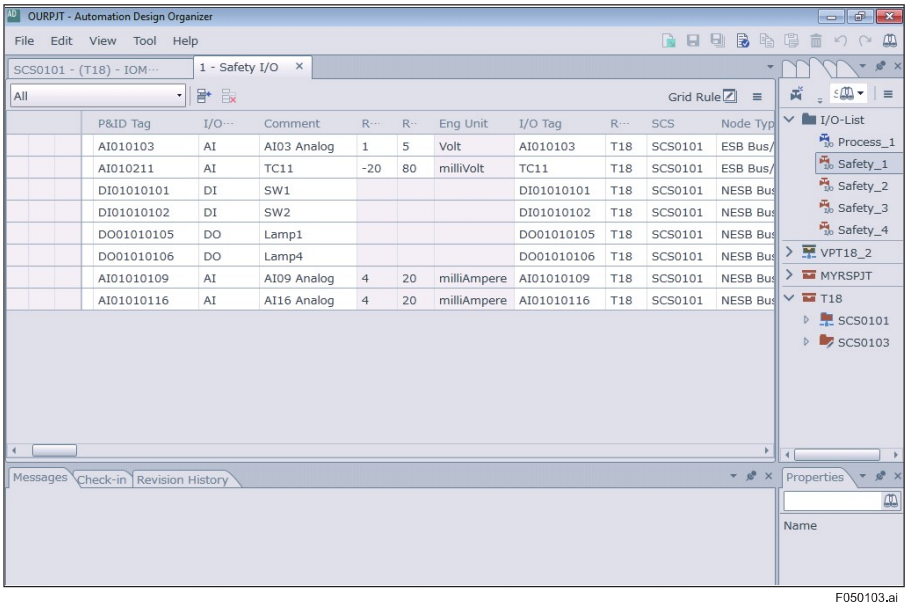
Create an application logic to materialize the designed SCS operation, by using function block diagram (FBD) or ladder diagram (LD) which conform to the IEC 61131-3 international standard.

Use the multi-language editor to create FBD. By connecting boxes of functional units called function blocks (FB) with lines, application logics from input to output can easily be created.



F050102.ai

Figure Example of creation of application logics by using multi-language editor



F050103.ai

Figure Define of I/O

(C) Verification of application logics

The application logic made in step (B) can be verified by using the virtual test function. The virtual test function performs the verification of the application logics on a computer without having an actual SCS. With the virtual test function displays the computation results of the application logics intuitively as TRUE (blue) and FALSE (red) on a screen. The logic simulation test and the SCS simulation test are available for the virtual test.

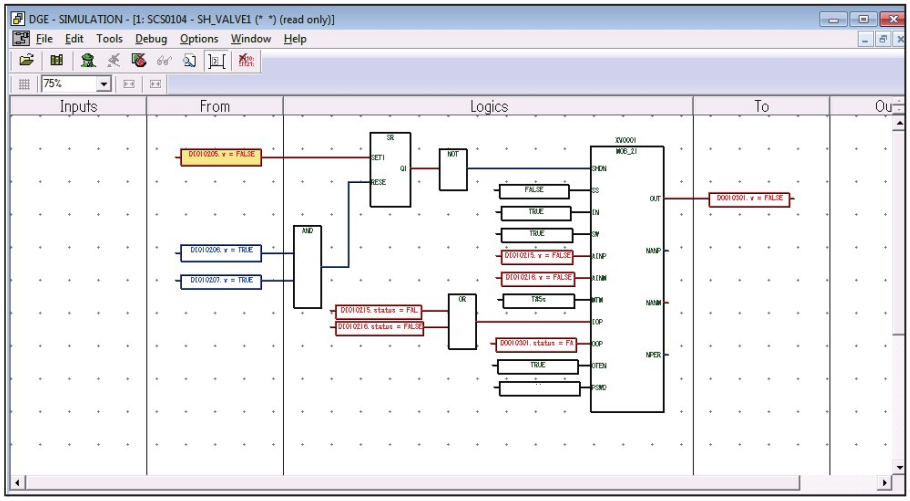


Figure Example of a test window

During the logic simulation test, the SENG executes the application logic using the logic simulator. The SCS security level is disregarded when verifying the application logic of each SCS.

When the SCS simulator on the ENG or the SENG executes application logic during the SCS simulation test, can also be conducted in accordance with the SCS's security level, integrated operation environment with CENTUM VP is required. Alarm confirmation on the HIS window enabled by temporarily overwritng application logic variables using override function of the HIS simulator. And if two or more of the SCS simulators are used, the inter-SCS safety communication test can be performed as well.

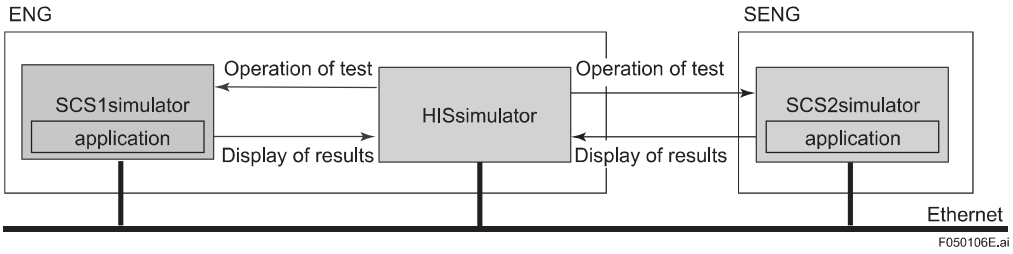


Figure SCS simulation test

(D) Off-line download or on-line change download

Download the application program verified in Step (C) from SENG to SCSs. An engineer is to compare the application program on the SENG and the data base in the SCS and confirm if the downloading has been correctly executed.

(E) Target test function

The application logic can be verified on the actual SCS using the target test function. The test can also be performed without mounting input/output modules by using the forcing function (see chapter 5.2 Maintenance Functions) and manually simulate input/output signal status. The target test function can be performed in reference to the security level of the SCS.

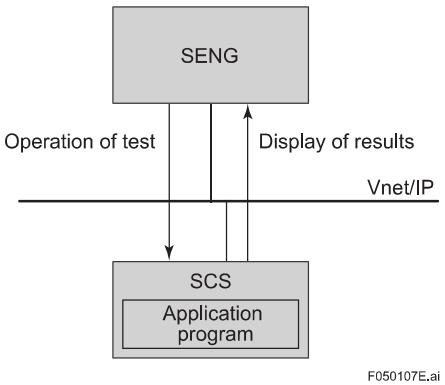


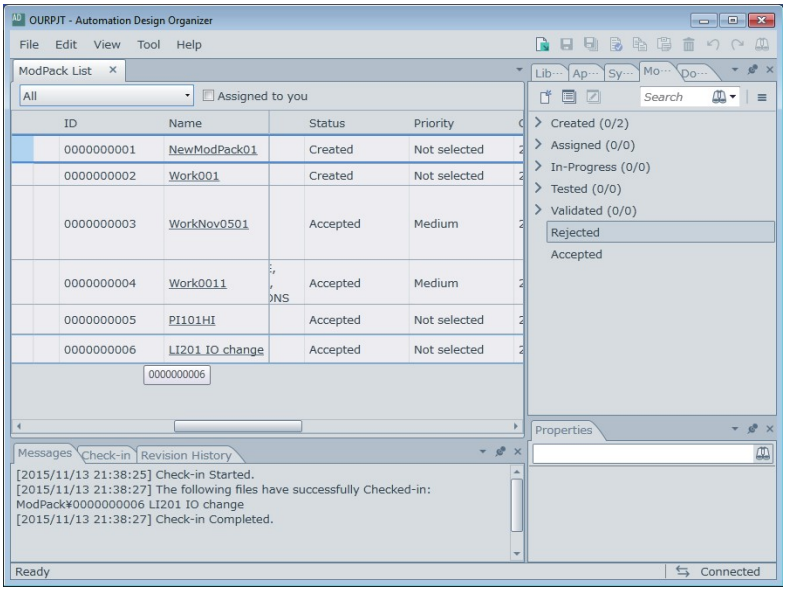
Figure Target test function

(F) Project check-in

Save the projects including the application logics created to the version management database for change management.

Change management function

The change management function an engineering support tool to manage change requirements generated during engineering work. By recording the changes in planning, execution, and testing, overlooking of the changes in the application programs can be prevented.



F050108.ai

Figure Change management function window

5.2 Operation and maintenance of SCS

Status of SCS and its operations in response to the plant's operating conditions and maintenance of the safety system are described in this section.

SCS status and operation

A safety system is expected to run properly and safely to prevent operators without authorities from making erroneous operations. The ProSafe-RS manages the SCS's operation and operational authorities by the operating mode and the SCS security level. The override and alarm window functions permits operation and monitoring of the SCS from CENTUM VP's HIS.

Operating modes

The operating modes indicate the operating statuses of the SCS. Depending on the kinds of operating mode determines how the SCS system program performs.

Table Operating modes

Operating Modes	
Name	**Status**
Stop Mode	The initial state of the SCS
Loading Mode	Downloading a program or database information from the SENG to the SCS.
Initial Mode	Executing diagnosis, database initialization, I/O module booting and others that are needed for starting initialization of the SCS.
Waiting Mode	Waiting for all the output modules to activate.
Running Mode	The SCS is operating normally.

SCS security levels

The SCS security level limits changes made by the operations to the SCS from outside.

Enable or disable of the user operation is controlled by the application logics depending on the defined security level.

Two categories of the security levels are available; one is the On-line level to be used during normal operation of SCS and the other is the Off-line level to be used when offline download is required. The security levels are password protected and only the authorized user with specific privileges can change.

On-line level:

Level 2
The highest security level with which the normal operation of the SCS is executed.

Level 1
The security level is temporarily used by an engineer or a specially authorized user for maintenance of the system and changing applications online.

Off-line level:

Level 0
The security level to be used when off-line download is required.

Operation and monitoring of SCS by HIS (Override and alarm windows)

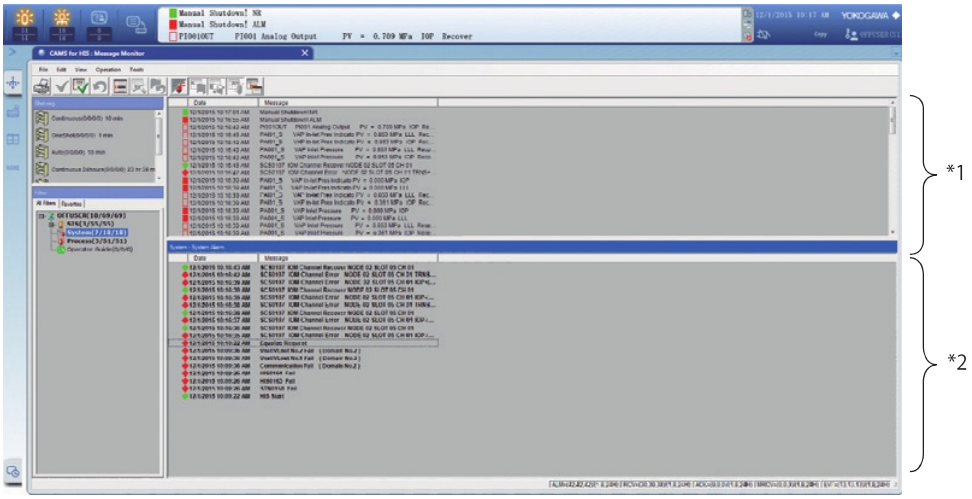
ProSafe-RS allows CENTUM VP's HIS to control and monitor the SCSs so that the safety instrumented systems perform its functions by knowing the overall plant operation status.

Override

I/O values can be set to a specified value that is different from the actual I/O value by operation from HIS while the system is controlled normally by the SCS. This operation is called override. This override can be created in the application logic using safety function blocks.

Alarm window

The Alarm window is to notify operators essential alarms to sustain the plant safety. By displaying only the SCS alarms extracted from all alarms, operators are able to recognize the important alarms easily.



*1: Alarms that the SCS extracted.
*2: All alarms.

Figure Integrated alarm window

Maintenance functions

A safety instrumented system is required to have regular maintenance because it has to function without fail when an abnormality occurs. For the maintenance of the ProSafe-RS, maintenance support tools and forcing are provided.

SCS maintenance support tools

The SCS maintenance support tools have been developed for the purpose of simplifying the maintenance of the SCS. Equipped with a user interface to easily spot on a failure section, the function chronologically displays maintenance data necessary for analysis in the form of diagnostic information messages.

The SCS maintenance support tools are as described below:

SCS status display:	Displays the operating status of the SCS
Diagnostic information display:	Displays diagnostic information in the SCS
Online monitoring:	Displays the operating status of the application logic on the SCS
Message cache tool:	Acknowledges the diagnostic information message and accumulation of SOE events
SOE Viewer:	Displays event information stored on the SCS
Setup Tool:	Customizes how to display and use the SCS maintenance support tools.

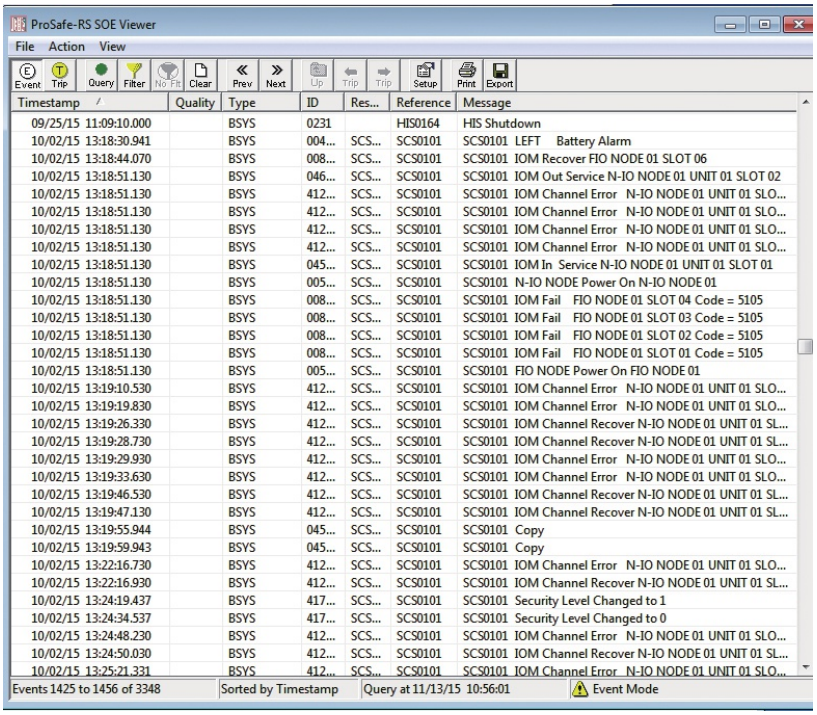
Forcing

The forcing is a function to fix or forcibly change values of input/output modules and application logic for the purpose of maintenance of the SCS or verification of application logics. Different from the override function, a dedicated user interface is used and creation of an application logic is not required.

5.3 Sequence of events recorder (SOER)

The sequence of events recorder (SOER) is a function to record the events (*1) that the SCS detects. Especially when the safety instrumented system is triggered, the SOER can be utilized for analyzing the causes of the plant's emergency shutdown. The SOER function consists of the event collection, the event storage and the time synchronization functions.

*1: The term an "event" refers to a change to the predefined application logic.



F050301E.ai

Figure SOE Viewer

Event collection

Not only digital inputs (DI) but also changes in digital outputs (DO) and analog inputs (AI) are collected as event information. By using the SOER function blocks with the application logic, changes in application logics can be acquired as event information, which enables to record changes in communication data with other SCSs.

Event storage

A certain volume of event information is stored in the SCS, and a computer for the data storage is not required to be activated all the time. On the other hand, the essential event information before and after the ESD are stored separately.

Revision Information

- Title : Safety Instrumented System ProSafe-RS System Overview
- Manual No. : TI 32P01A10-01EN

Dec. 2018/3rd Edition

Front page	ProSafe-RS Logo change
4.1	Added the description of N-IO field enclosure.
	Added the figure of N-IO field enclosure in the Figure “System configuration example of SCS”.
4.3	Added the description of S2MDV843, S2LP131, and N-IO field enclosure.

July 2016/2nd Edition

All pages, Clerical error correction.

Dec. 2015/1st Edition

Newly published.

Written by Yokogawa Electric Corporation

Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Subject to change without notice.

Attachment 9.13 ProSafe-RS Installation Guidance

TI 32P01J10-01EN

Technical Information

ProSafe-RS
Installation Guidance

TI 32P01J10-01EN

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

TI 32P01J10-01EN
©Copyright Nov. 2015 (YK)
15th Edition Nov. 2020 (YK)

Introduction

ProSafe-RS is a safety control system aimed at protecting people, environment, and equipment from unexpected accidents or problems at a plant.

This manual describes the requirements for installation (control room size and power supply requirements), storage and transportation, and wiring.

Chapter 1 System Installation Requirements

This chapter describes the engineering specifications that cover the control room design/ environment, power supply system, grounding, noise prevention, corrosive-gas environment compatibility and compliance with marine standards for the ProSafe-RS system.

Chapter 2 Transportation, Storage and Installation

This chapter describes precautions for the transport, unpacking and storage of the ProSafe-RS system. This chapter also describes temperature and humidity changes when temporarily storing the ProSafe-RS system, and how to install cabinets and rack mounted devices.

Chapter 3 Cabling

This chapter describes how to connect power, ground, signal and bus cables to the installed devices, and how to connect optical fiber cables.

Chapter 4 Installation Specifications

This chapter covers the power consumption, power dissipation, in-rush current, and fuse and breaker ratings as well as the parts that need replacement within 10 years. Read this section when deciding the power supply capacity.

Chapter 5 Post-installation Inspection and Environmental Preservation

This chapter describes items that must be checked before turning on power and the precautions to be taken to safeguard the environment after installing the system.

All Rights Reserved Copyright © 2015, Yokogawa Electric Corporation

Safety Precautions

Safety, Protection, and Modification of the Product

- In order to protect the system controlled by the product and the product itself and ensure safe operation, observe the safety precautions described in this Technical Information and the User's Manuals. We assume no liability for safety if users fail to observe these instructions when operating the product.
- If this product is used in a manner not specified in this Technical Information, the protection provided by this product may be impaired.
- If any protection or safety circuit is required for the system controlled by the product or for the product itself, prepare it separately.
- Be sure to use the spare parts approved by Yokogawa Electric Corporation (hereafter simply referred to as YOKOGAWA) when replacing parts or consumables.
- Do not use the accessories (Power supply cord set, etc.) that came with the product for any other products.
- Modification of the product is strictly prohibited.
- The following symbols are used in the product and this Technical Information to indicate that there are precautions for safety:

	Indicates that caution is required. This symbol for the Product indicates the possibility of dangers such as electric shock on personnel and equipment, and also indicates that the user must refer to the User's Manuals for necessary actions. In the User's Manuals, this symbol is used together with a word "CAUTION" or "WARNING" at the locations where precautions for avoiding dangers are described
	Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.
	Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock
	Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.
	Indicates an AC supply.
	Indicates a DC supply.
	Indicates that a component such as a power supply switch is turned ON.
	Indicates that a component such as a power supply switch is turned OFF.

Symbol Marks of this Technical Information

Throughout this Technical Information, you will find several different types of symbols are used to identify different sections of text. This section describes these icons.



WARNING

Indicates precautions to avoid a danger that may lead to death or severe injury.



CAUTION

Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.

IMPORTANT

Identifies important information required to understand operations or functions.

TIP

Identifies additional information.

SEE ALSO

Identifies a source to be referred to.

Cautions for Safely Applying the Device

Wiring Power Cable

WARNING

Connect the power cables according to the procedure in this document.

Power cables must conform to the safety standards of the country where the device is installed.

SEE ALSO For Wiring Power Cable, refer to 3.2, “Connecting Power.”

Earth Wiring

WARNING

This equipment requires a protective grounding defined by the safety standard.
Ground the device following the procedure in this document to prevent from electric shock and to minimize the noise.

SEE ALSO For Earth Wiring, refer to 3.3, “Connecting Ground Cable.”

Tightening Torque of Screws

IMPORTANT

The tightening torque that the Product recommends is showed in the following table. However, if the tightening torque of the screw is specified in the User’s Manuals, follow the instructions described in the User’s Manuals.

Table Table of Recommended Tightening Torque

Nominal diameter of a screw	M2.6	M3	M3.5	M4	M5	M6	M8	M10
Recommended tightening torque (N•m)	0.35	0.6	0.8	1.2	2.8	3.0	12.0	24.0

Battery

CAUTION

- Must use Yokogawa designated batteries.
- Mounting and changing batteries must follow the procedure in the hardware instruction manual for each device.
- When changing batteries while the power supply is not shutdown, do not put hands inside of the device since it is danger of electric shock.

Fan Unit

CAUTION

• When changing fan unit while the power supply is not shutdown, be careful not to touch other parts so as to avoid electric shock.

SEE ALSO For Fan Unit, refer to 4, “Installation Specifications, Durability of Parts.”

Wiring I/O Cables

CAUTION

Wiring I/O cables must follow the procedure in this document.

SEE ALSO For Wiring I/O Cables, refer to 3.5, “Connecting Signal Cable.”

Connected Devices

IMPORTANT

To ensure this system’s compliance with the CSA safety standards, all devices connected to this system shall be CSA certified devices.

Fuse Replacement

WARNING

- Be sure to use the specified fuses.
- Switch off the power supply before exchanging the fuses.

Maintenance

CAUTION

- The maintenance work for the devices described in this manual should be performed only by qualified personnel.
- When the device becomes dusty, use a vacuum cleaner or a soft cloth to clean it.
- During maintenance, put up wrist strap, and take other ESD (Electrostatic Discharge) measures.
- If the existing caution label is dirty and illegible, prepare a new label (part number: T9029BX) to replace it.

SEE ALSO For Maintenance, refer to 1.5.2, “Countermeasures against Static Electricity.”

Drawing Conventions

Some drawings may be partially emphasized, simplified, or omitted, for the convenience of description.

Trademark

Trademark Acknowledgment

The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

ProSafe-RS
Installation Guidance

TI 32P01J10-01EN 15th Edition

CONTENTS

1. System Installation Requirements 1-1
   - 1.1 Control Room Design 1-2
   - 1.2 Control Room Environment 1-5
   - 1.3 Power Supply System 1-13
   - 1.4 Grounding 1-19
   - 1.5 Noise Countermeasures 1-22
     - 1.5.1 Noise Sources and Noise Countermeasures 1-22
     - 1.5.2 Countermeasures against Static Electricity 1-26
   - 1.6 Cabling Requirements 1-27
   - 1.7 Corrosive-gas Environment Compatibility 1-29
   - 1.8 Compliance with Marine Standards 1-32
2. Transportation, Storage and Installation 2-1
   - 2.1 Precautions for Transportation 2-2
   - 2.2 Unpacking 2-3
   - 2.3 Storage 2-4
   - 2.4 Servicing Area 2-5
   - 2.5 Installation 2-6
     - 2.5.1 Installation on Floor 2-7
     - 2.5.2 Rack Mounting 2-11
     - 2.5.3 DIN Rail Mountable Devices 2-15
     - 2.5.4 Wall Mountable Devices 2-20
     - 2.5.5 Installation Guideline for Cabinet (FIO) 2-23
     - 2.5.6 Installation Guideline for Cabinet (N-IO) 2-29
     - 2.5.7 Desktop Equipment 2-49
     - 2.5.8 Installing Control Network Interface Card 2-49
3. Cabling 3-1
   - 3.1 Cables and Terminals 3-2
   - 3.2 Connecting Power 3-5
   - 3.3 Connecting Ground Cable 3-12
   - 3.4 Power and Ground Cabling 3-13
   - 3.5 Connecting Signal Cable 3-31

3.6 Connecting Signal Cables to I/O Modules (for FIO) 3-45
3.6.1 Combination of I/O Modules and Terminal Blocks 3-45
3.6.2 Signal Cable Connections 3-46
3.6.3 Connecting Signal Cables to I/O Modules 3-48
3.7 Signal Connections of N-IO I/O Unit 3-66
3.7.1 N-IO I/O Unit Types 3-66
3.7.2 Base Plate 3-66
3.7.3 Base Plate for Barrier 3-71
3.8 Connecting Bus Cable 3-74
3.8.1 Vnet/IP network 3-74
3.8.2 ESB Bus 3-78
3.8.3 N-ESB Bus 3-80
3.8.4 Optical ESB Bus 3-81
3.8.5 F-SB Bus (for N-IO Node) 3-87
4. Installation Specifications 4-1
5. Post-installation Inspection and Environmental Preservation 5-1

1. System Installation Requirements

This section describes installation requirements such as environmental conditions, required space and layout considerations, power consumption, cabling and grounding.

1.1 Control Room Design

Control rooms, in which the system control equipment is to be installed, should be designed in accordance with the following conditions:

General

In designing a control room, ensure adequate floor strength and air conditioning including dust- and moisture-proofing.

SEE ALSO

- 1.1 Control Room Design — Air Conditioner
- 1.2 Control Room Environment — Air Purity
- Applied Standards (Table Installation Environment Specifications)

Floor Strength and Space

The floor should have adequate strength, and you should design the layout in accordance with the weight and size of equipment to be installed.

SEE ALSO

- For the maintenance space required, refer to 2.4, “Servicing Area.”
- For the weight and dimensions of standard equipment, refer to applicable general specifications.

Floor Structure

To prevent damage to cables by operators and maintenance equipment, do not lay cables on the floor.

Lay cables under the floor as follows:

- Provide an “accessible” floor which also facilitates maintenance work.
- Make cable pits under the floor if it is concrete.

Flooding- & Dust-proof Floor

To protect equipment and cables, design a flooding-proof floor.

After the cabling is completed, seal all cable conduits using putty to prevent intrusion of dust, moisture, rats, and insects into the equipment.

Clearance From The Wall and The Floor Surface

There are ventilation holes on the front and rear doors of the cabinets. To ensure good air ventilation and easy maintenance, provide a clearance of at least 1000 mm (including the service areas) from the wall to the front and rear doors of the cabinets. Also make sure the height of the ceiling is at least 2400 mm from the floor.

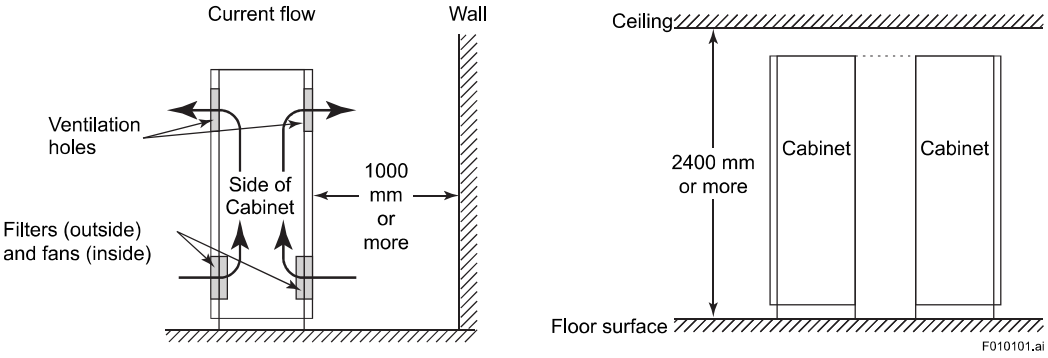


Figure Wall Clearance and Ceiling Height

Illumination

The illumination level around a display unit should be 700 to 1500 lx (target illumination level: 1000 lx). The illumination level inside the control room should be reasonably uniform.

Select proper light fixtures and install them in positions where they don't cause glare on the CRT displays and LCDs.

TIP

REFERENCE (Illumination standards):

For ultra-precision work:	1500 to 3000 lx (illumination level: 2000)
For precision work:	700 to 1500 lx (illumination level: 1000)
For ordinary work:	300 to 700 lx (illumination level: 500)
For non-detail work:	150 to 300 lx (illumination level: 200)
Passages, warehouses:	30 to 150 lx (illumination level: 50 to 100)

(Source: JIS Z9110)

Outlets for Maintenance

Outlets (approx. 1.5 kVA) for measurement devices should be provided near the installed equipment for maintenance.

Telephone

Telephones should be installed for communications with related stations.

Air Conditioner

The air conditioner should be operated according to the conditions below to prevent moisture condensation on the installed equipment.

- Keep changes in temperatures within ±10°C/h.
- Install the air conditioner away from the equipment.
- Install substitute air conditioners to prevent moisture condensation as a result of the temperature rising or falling if an air conditioner fails.
- Set the air conditioner so that its air outlet is not above the equipment (to avoid water dropping on the equipment).

Windows

Close the windows of the control room. If a draft comes in around the windows, seal around the windows.

Opening the window while air conditioning is running may result in condensation forming, or let in dust or corrosive gas, adversely affecting the installed equipment. Windows on the sea side must be closed to keep out salt air.

Install blinds, if necessary, to prevent sunlight reflecting from CRT displays and LCDs.

1.2 Control Room Environment

This section describes environmental conditions of the control room to operate the system safely, and stably over a long period of time.

It is recommended that user have the control room environment assessment. For the assessment, contact Yokogawa if necessary.

Temperature and Humidity Limits

SEE ALSO See "Table of Equipment Installation Specifications" in this section, for the temperatures and humidity limits for operating and storing this equipment.

When bringing the equipment into a location where allowable operating temperature is set from another location where the temperature exceeds the allowable operating range, following precautions are necessary:

- The equipment should reach the ambient temperature according to the requirements for the temperature change rate, keeping it unpacked from its case. At that time, be careful not to let condensation form on the equipment.
- Once the equipment reaches the allowable operating temperature range, leave it for about three hours before operation.

Under normal operation, the rate of change of ambient temperatures should be within 10°C/h. All the equipment should be kept out of direct sunlight.

Condensation

Prevent condensation. If condensation occurs, or its trace is found on the control room, contact Yokogawa.

SEE ALSO See "Section 2.3 Storage" for more information.

Vibration

Vibration in the control room should be limited as follows:

- For vibration frequency up to 8.4 Hz: Limit displacement amplitude to 1.75 mm or less.
- For vibration frequency over 8.4 Hz: Limit acceleration to 4.9 m/s^2 or less.

The following is the relationship of the vibration frequency, displacement amplitude, and acceleration:

Acceleration $(m/s^2) = 4\pi^2 \cdot A \cdot F^2 \cdot 10^{-3}$

A: Displacement amplitude (mm)
F: Frequency (Hz)

F010201.ai

Consult Yokogawa if complex vibrations are involved.

Air Purity

The dust in the control room should be kept below 0.3 mg/m^3. Minimize corrosive gas such as hydrogen sulfide (H_2S), sulfur dioxide (SO_2), chlorine, and conductive dust such as iron powder and carbon.

The allowable content of H_2S, SO_2, or any other corrosive gas varies with temperatures, humidity, or existence of other corrosive gas. Consult Yokogawa if corrosive gas exists.

Magnetic Field

Do not install the CRT near cables with heavy current flowing or in the magnetic field of a power supply. If installed in such locations, the display may be distorted or its colors may be affected by the magnetic fields.

Electric Field Strength (Electric Wave Condition)

For the proper and stable operation of this system, the field electric strength of the location for the equipment should be controlled as following:

10 V/m or less (26 MHz to 1.0 GHz)

10 V/m or less (1.4 to 2.0 GHz)

1 V/m or less (2.0 to 2.7 GHz)

In case of the usage of wireless equipment such as transceiver nearby this system, note as following:

- The door of this system should be closed.
- In case of the usage of transceiver with 10 W or less, the distance from this system should be kept 1 m or more.
- As for the usage of wireless equipment with 1 W or less such as mobile-telephone, PHS, wireless telephone or LAN equipment, the distance should be kept 1 m or more. Attention should be paid to the micro wave radiated from mobile-telephone or PHS even out of usage.

Following formula represents the electric field strength. However, the calculated value requests ideal environment. Worse conditioned environment should be taken into consideration. In case some wireless equipment is used nearby this system, this formula would be useless. The value calculated through this formula should be considered noting other than reference.

$$E=\frac{k\sqrt{P}}{d}$$

E : Electric field strength (V/m)
k : Coefficient (0.45 to 3.35; average 3.0)
P : Radiation power (W)
d : Distance (m)

F010202.ai

Installation Specification

Installation Altitude

N-IO node (*1) (*2) : 3000 m or less
Other than N-IO node : 2000 m or less

Installation category based on IEC 61010-1 (*3)

Category I

- For YOKOGAWA products, category I applies to the devices that receive the electric power not more than 33 V AC, 70 V DC.

Category II

- For YOKOGAWA products, category II applies to the devices that receive the electric power exceeding 33 V AC or 70 V DC.

Pollution degree based on IEC 61010-1: 2 (*4)

*1: For more information about the device, refer to General Specification (GS).
*2: For S2BN4D and S2BN5D, the installation altitude is 2000 m or less.
*3: The installation category, also referred to as an overvoltage category, defines the standard for impulse voltage. The category number from I to IV applies the devices to determine the clearance required by this standard.
Category I applies to the device intended to be connected to a power supply with impulse voltage reduced to the safe level.
Category II applies to the device intended to be supplied from the building wiring.
*4: Pollution degree indicates the adhesion level of foreign matter in a solid, liquid, or gaseous state that can reduce dielectric strength. Degree 2 refers to a pollution level equivalent to the general indoor environment.

SEE ALSO See “Installation Environment Specifications” at the end of this chapter.

Measurement Categories

Regarding the measurement inputs, the following requirements must be satisfied to meet the specifications for the device:

The category of the equipment applies to O (Other) in the following table.

The rated transient overvoltage is 1500 V.

Note: Do not use the equipment for measurements within measurement categories II, III and IV.

Table Measurement category

Applicable Standard IEC/EN 61010-2-030 CAN/CSA-C22.2 No.61010-2-030	Description
O (Other) (*1)	For measurements performed on circuits not directly connected to MAINS.
Measurement category II	For measurements performed on circuits directly connected to the low voltage installation.
Measurement category III	For measurements performed in the building installation.
Measurement category IV	For measurements performed at the source of the low-voltage installation.

*1: Measurement category I defined in IEC/EN 61010-1:2001 and CAN/CSA-C22.2 No.61010-1-04 has been changed to “O (Other)” in IEC/EN 61010-2-030 and CAN/CSA-C22.2 No.61010-2-030.

Conformity Standards

The ProSafe-RS complies with the standards shown below.

IMPORTANT

Different standards are applied according to the types of equipment.

For details, refer to GS 32P01B60-01EN “ProSafe-RS Standards Compliant Models”.

Functional Safety Standards

IEC 61508, IEC 61511-1 and IEC 62061

Programmable Controllers Standards (*1), (*2), (*3)

IEC 61131-2

Application Standards (*1)

EN 54-2 (*2), EN 298 (*3), (*4), EN 50156-1, NFPA 72, NFPA 85, and NFPA86

Safety Standards (*5), (*6), (*7), (*8)

[CSA]
CAN/CSA-C22.2 No.61010-1, CAN/CSA-IEC 61010-2-201, CAN/CSA-C22.2 No.61010-2-030

[CE Marking] Low Voltage Directive
EN 61010-1, EN 61010-2-201, EN 61010-2-030, EN 60825-1

[EAC Marking]
CU TR 004

[Morocco Compliance Marking(C_e Marking)] Low Voltage Directive
NM EN 61010 1
NM EN 61010 2 201
NM EN 61010 2 030
NM EN 60825 1

*1: Except for the case of using S2BN1D, S2BN4D, and S2BN5D in combination with S2MMM843 or S2MDV843 of style S2 or later, a lightning arrester or the like is required to meet this surge immunity standard.
*2: 24 V DC and 48 V DC field power to DI and DO shall not be provided directly from a DC distribution network. The field power supply cable length must be 30 m or less.
*3: Where the system power uses 24 V DC (SPW484), use an external uninterruptible power supply (UPS).
*4: 24 V DC and 48 V DC field power to DI and DO shall not be provided directly from a DC distribution network. The field power supply cable length must be 10 m or less.
*5: For the rack mountable devices, DIN rail mountable devices, and wall mountable devices to meet the Safety Standards and EMC Standards, the devices must be installed in a lockable metal cabinet. The cabinet must conform to IEC/EN/CSA 61010-2-201 or provide degrees of protection IP3X or above and IK09 or above.
*6: ProSafe-RS measurement input corresponds to the measurement category O (Other) based on IEC/EN 61010-2-030 and CAN/CSA-C 22.2 No. 61010-2-030. The measurement category I defined in IEC/EN 61010-1: 2001 and CAN/CSA-C 22.2 No. 61010-1-04 has been changed to O (Other).
*7: For ensuring all the hardware devices to satisfy the safety standards, the dedicated breakers in the power supply distribution board must conform to the following specifications.
[CSA] CSA C22.2 No.5 or UL 489
[CE Marking] EN 60947-1 and EN 60947-3
[EAC Marking, C_e Marking] EN 60947-1 and EN 60947-3
*8: The ground suitable for the power distribution system in the country or region has to be used for protective grounding system.

EMC Conformity Standards (*1), (*2), (*3)

[CE Marking] EMC Directive
EN 55011 Class A Group1 (*4)
EN 61000-6-2
EN 61000-3-2 (*5)
EN 61000-3-3
EN 61326-1 (*6)

[RCM]
EN 55011 Class A Group1 (*4)

[KC Marking]
Korea Electromagnetic Conformity Standard

[EAC Marking]
CU TR 020

[Functional Safety]
IEC 61326-3-1 (*6) (*7)

[Morocco Compliance Marking(C$_e$ Marking)] EMC Directive
NM EN 55011 Class A Group 1 (*4)
NM EN 61000 6 2
NM EN 61000 3 2 (*5)
NM EN 61000 3 3

*1: Except for the case of using S2BN1D, S2BN4D, S2BN5D, S2NN70D, and S2NN60D in combination with S2MMM843 or S2MDV843 of style S2 or later, a lightning arrester or the like is required to meet this surge immunity standard.
*2: 24 V DC and 48 V DC field power to DI and DO shall not be provided directly from a DC distribution network. The field power supply cable length must be 30 m or less.
*3: For the rack mountable devices, DIN rail mountable devices, and wall mountable devices to meet the Safety Standards and EMC Standards, the devices must be installed in a lockable metal cabinet. The cabinet must conform to IEC/EN/CSA 61010-2-201 or provide degrees of protection IP3X or above and IK09 or above.
*4: A Class A hardware device is designed for use in the industrial environment. Please use this device in the industrial environment only.
*5: An external device such as a power unit with harmonic current neutralizer and an active harmonics conditioner must be connected to meet this harmonic current emission standard. See Section 1.3 “Power Supply System”.
*6: The base plate for barrier S2BN4D and S2BN5D conforms to the EMC standards with conditions. For details, refer to GS 32P06P10-01EN “Base Plates for Barrier (for N-IO)”.
*7: Where the system power uses 24 V DC (S2PW504), use an external uninterruptible power supply (UPS).

Standard for Hazardous (Classified) Locations

[ATEX Type “n”]

[IECEx Type “n”]

[Canada (FM) Non-Incendive]

[US (FM) Non-Incendive]

[ECAS-Ex Type “n”]

SEE ALSO For more information about Standard for Hazardous Locations, refer to TI 32S01J30-01E “Explosion Protection (for ProSafe-RS).”

Marine Standards

ABS (American Bureau of Shipping)
BV (Bureau Veritas)
LR (Lloyd's Register)
DNV GL

SEE ALSO For more information about the components which comply with the marine standards and how to install those components, refer to 1.8, "Compliance with Marine Standards."

In relation to the CE Marking, the manufacturer and the authorised representative for ProSafe-RS in the EEA are indicated below:

Manufacturer: YOKOGAWA Electric Corporation
(2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, Japan.)

Authorised representative in the EEA: Yokogawa Europe B.V.
(Euroweg 2, 3825 HD Amersfoort, The Netherlands.)

Installation Environment Specifications

The following table lists environmental requirements for the installation of the ProSafe-RS System.

SEE ALSO For details on each equipment, refer to the ProSafe-RS general specifications (GS).

Table Installation Environment Specifications (1/2)

Item		Specifications			Remarks
		Safety Control Unit (SCU)	Safety Node Unit, Unit for Optical Bus Repeater Module	N-IO Node (*1)	
Temperature	Normal operation	-20 to 40ºC (*2) (standard type SCU for Vnet/IP)	-20 to 70ºC (*3)	-40 to 70ºC (*4) (*5)	
		-20 to 70ºC (*3) (wide range temperature type SCU for Vnet/IP)			
	Transportation/storage	–40 to 85°C			
Humidity	Normal operation	5 to 95% RH (non-condensing)			5 to 85% RH when the SRM53D/ SRM54D/SBM54D is mounted.
	Transportation/storage	5 to 95% RH (non-condensing)			
Temperature change	During operation	Within ± 10ºC/h			
	Transportation/storage	Within ± 20ºC/h			
Power supply	Voltage range	100 to 120 V AC –15%, +10%			
		220 to 240 V AC –15%, +10%			
		24 V DC: –10% to +20%		24 V DC: –15% to +20%	
	Frequency	50/60 Hz ± 3Hz			
	Distortion factor	10% or less			
	Crest factor	100 V system: 118 V or larger 220 V system : 258 V or larger			
	Momentary failure	20 ms or less (when receiving the rated AC voltage)			
	DC power supply ripple rate	1% p-p maximum			
Withstanding voltage		1500 V AC for 1 minute (for 100-120/220-240 V AC) 500 V AC for 1 minute (for 24 V DC)			Between power & grounding terminals
Insulation resistance		20 M ohms at 500 V DC			Between power & grounding terminals
Grounding		Apply the grounding system which is defined by the rules and standards of the country or the region.			
Dust		Maximum of 0.3 mg/m^3			
Corrosive gas		ANSI/ISA S71.04 G3 (standard)			Excluding SRM53D/ SRM54D/SBM54D

*1: An N-IO node consists of S2NN30D, S2BN1D, S2BN4D, S2BN5D, S2MMM843, S2MDV843, S2KPB10, and S2KLF10.
*2: 0 to 40°C when ALR111-S□1, ALR121-S□1, or ALE111-S□1 is mounted.
*3: 0 to 60°C when ALR111-S□1, ALR121-S□1, or ALE111-S□1 is mounted.
*4: For S2BN4D and S2BN5D, the ambient temperature must be from -20 to 60°C.
*5: When the S2NN30D Node Interface Unit is used with an optical ESB bus with the following specifications at an altitude of 2000 m or higher, the ambient temperature range is -40 to 60°C.

S2NN30D-□□□□□01□□ S2NN30D-□□□□□02□□ S2NN30D-□□□□□10□□
S2NN30D-□□□□□11□□ S2NN30D-□□□□□12□□ S2NN30D-□□□□□20□□
S2NN30D-□□□□□21□□ S2NN30D-□□□□□22□□

For cable connector of Base plate with disconnecting terminal (S2BN1D-□9), the normal operation temperature is -20 to 70°C as the temperature specification of the dedicated cable is applied.

Table Installation Environment Specifications (2/2)

Item		Specifications			Remarks
		Safety Control Unit (SCU)	Safety Node Unit, Unit for Optical Bus Repeater Module	N-IO Node (*1)	
Noise	Electric field	10 V/m maximum (80 MHz to 1 GHz)			
	Static electricity	4 kV or less (direct discharge) 8 kV or less (aerial discharge)			
Vibration	Continuous vibration	Amplitude: 1.75 mm (5 Hz to 9 Hz)		Amplitude: 17.5 mm 5 Hz ≤ f < 8.4 Hz	
		Acceleration: 4.9 m/s^2 (9 Hz to 150 Hz)		Acceleration: 4.9 m/s^2 (8.4 Hz ≤ f < 150 Hz)	
	Non-continuous vibration	Amplitude: 3.5 mm (5 Hz to 9 Hz)		Amplitude: 3.5 mm 5 Hz ≤ f < 8.4 Hz	
		Acceleration: 9.8 m/s^2 (9 Hz to 150 Hz)		Acceleration: 9.8 m/s^2 (8.4 Hz ≤ f < 150 Hz)	
	Seismic	Acceleration: 4.9 m/s^2 or less			
	Transportation	Horizontal: 4.9 m/s^2 or less vertical: 9.8 m/s^2 or less			When packaged
Impact		147 m/s^2, 11 ms			
Altitude (above sea level)		2000 m or less		3000 m or less (*5)	

*1: An N-IO node consists of S2NN30D, S2BN1D, S2BN4D, S2BN5D, S2MMM843, S2MDV843, S2KPB10, and S2KLF10.
*5: When the S2NN30D Node Interface Unit is used with an optical ESB bus with the following specifications at an altitude of 2000 m or higher, the ambient temperature range is -40 to 60°C.
S2NN30D-□□□□□01□□ S2NN30D-□□□□□02□□ S2NN30D-□□□□□10□□
S2NN30D-□□□□□11□□ S2NN30D-□□□□□12□□ S2NN30D-□□□□□20□□
S2NN30D-□□□□□21□□ S2NN30D-□□□□□22□□

SEE ALSO For the level of corrosive gases permitted in an ordinary office, refer to TI 33Q01J20-01E “Guidelines for Installation Environment.”

1.3 Power Supply System

The following conditions should be met:

- **Voltage and frequency fluctuations are within the limits specified for each system component.**
- **Waveform distortion is within limits.**
- **High-frequency noise is not at a level that affects system operation.**
- **Use an UPS (uninterruptible power supply) if necessary.**

AC Power Specification

AC power used for the system must be within the specified rated voltage and the peak value must be greater than the minimum specified (see below). DC power must be within 24 V DC -10%/+20% at the power supply terminals.

IMPORTANT

If the power unit has high output impedance or high wiring impedance, the resulting voltage drop flattens the input voltage wave, forming a distorted waveform with a low peak value (“B” in the chart below).

Even if the effective value of the distorted input voltage wave is the same as that specified for a non-distorted input voltage wave, the voltage across the terminals of the smoothing capacitor in the power circuit may be so low that the system detects power failure. Even if input voltage waves A and B shown below have the same effective value of 100 V AC, wave B will have a lower smoothing capacitor terminal voltage.

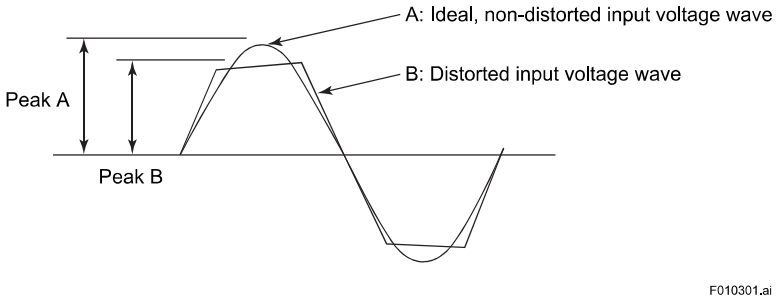


Figure Distorted Input Voltage Waveform

The system operating voltage range is shown below based on the relationship between effective and peak values at the power input terminal of each system. Apply AC power within these ranges to operate the system.

TIP

Average-value rectifying measuring instruments such as general type digital voltmeters and testers cannot measure effective values accurately. Use Yokogawa's digital oscilloscope DL series, power analyzer WT series or equivalent device, which can measure effective values, peak values, and waveform distortion.

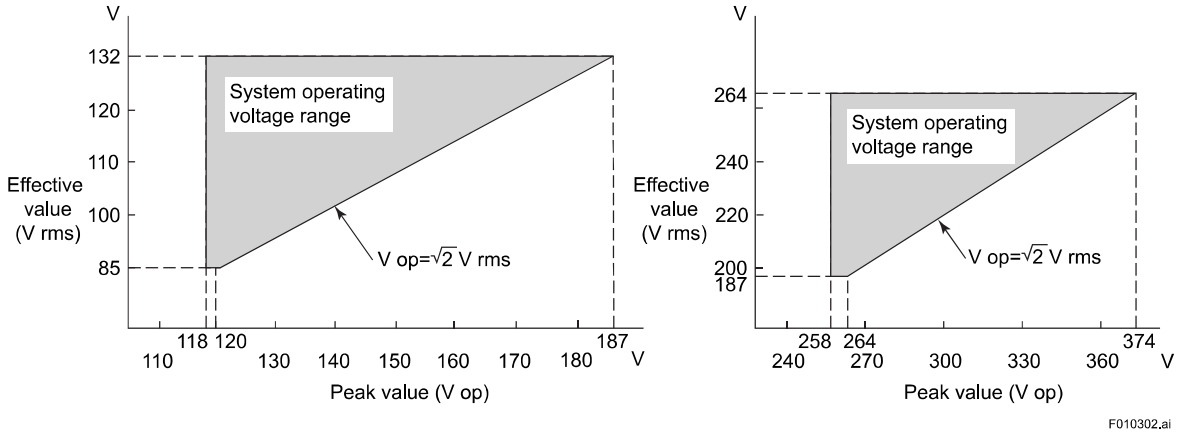


Figure System Operating Voltage Range

The DC stabilized power supply for the ProSafe-RS (except PCs) uses a compact and efficient switching regulator circuit. In this circuit, output voltage cannot be maintained if the energy (terminal potential) of the smoothing capacitor falls below a predetermined value. The circuit monitors the capacitor terminal voltage and regards it as power failure if the voltage falls in the danger zone, causing the system to enter power fail mode (non-detected momentary power failure: up to 20 ms).

Current flows to the capacitor in this circuit when AC input voltage is higher than the capacitor terminal voltage. Since the capacitor is charged by the peak value of the input waveform, it is required that both the effective voltage value and the peak value conform to the specification requirements.

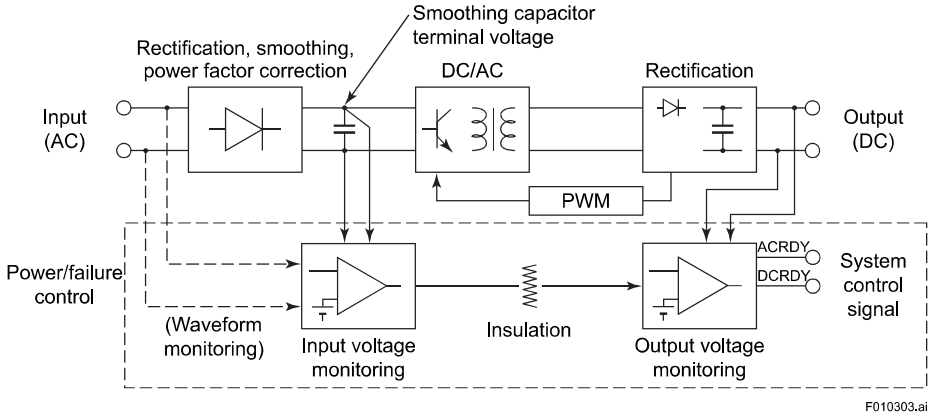


Figure Power Circuit Diagram of Safety Control Unit

Selecting a Power System

The ProSafe-RS system requires a power supply that satisfies power requirements in accordance with EMC regulations. It is recommended that an external power supply unit be used in order to prevent disruptions due to momentary or extended power failure, line noise, or lightening surges, as well as to suppress harmonic current from various devices.

For selection of the power supply unit, consult with a power unit manufacturer taking the following points into consideration.

Source Output Capacity

Take the following items into consideration when consulting with a power unit manufacturer to determine the output capacity.

Power consumption:	Both volt-ampere and watt data should be studied.
Device crest factor:	Ratio of the peak value to the effective value of the device input current.
Device in-rush current:	The method of turning on the power should also be studied.
Backup ready time after failure:	Time period required to backup the devices when power fails.
Reserve capacity:	An extra power capacity should be determined as reserve to meet any device additions.

SEE ALSO

- Electrical Specifications Table for power consumption in Chapter 4
- In-rush Current of Each Component in Chapter 4

Crest factor

The crest factor is the ratio of the peak value to the effective value of the device input current.

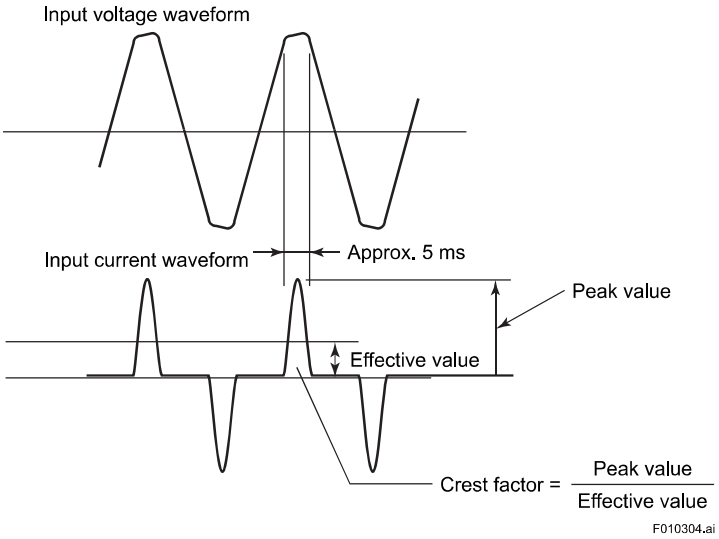


Figure Input Voltage and Input Current Waveforms

Crest factor = Peak value of device input current / Effective value of device input current

The crest factor must be considered for the input current supplied to every device connected to the system when estimating the power output capacity in selecting the power unit.

Approximate device crest factors should be as follows:

100-120 V supply voltage: Crest factor About 3.

220-240 V supply voltage: Crest factor About 6.

Common Method to Determine Power Unit Capacity

The following shows the commonly used method used to determine the power unit capacity taking the crest factor into consideration - the final determination should be made in consultation with a power unit manufacturer:

- If the specification of power unit crest factor (the peak current value allowable for the effective current value) is larger than the above device crest factor, the power unit can be used for up to full rated capacity. However, in-rush current, backup time, reserve capacity, etc., must be separately taken into consideration.
- If the power unit crest factor is smaller than the device crest factor, the power unit capacity needs to be calculated in the expression shown below. In-rush current, backup time, reserve capacity, etc., must be separately taken into consideration.

Power unit output capacity = Total device power consumption x Capacity coefficient

Capacity coefficient = Device crest factor / Power unit crest factor specification

In-Rush Current

When the equipment is turned on, a large in-rush current flows as the capacitor is instantaneously charged and the transformer is excited. When any equipment is turned on, this should not cause any voltage fluctuation that could adversely affect other equipment. Do not turn on all equipment at the same time. Start equipment one by one.

Power may be switched to backup or AC line power if in-rush current activates the overload protection circuit on power-up. After such an overload, select an uninterruptible power unit, with automatic-recovery.

Suppressing Harmonic Current

In order to suppress harmonic current supplied to a low-voltage distribution system, it is necessary to install a power unit or an active harmonic suppressor, such as indicated below, between a device and the distribution system:

- Power unit equipped with the harmonic suppression function (a high power-factor inverter-type uninterruptible power unit, etc.)
- Active harmonic suppressor

In Europe, a power unit should be selected so that harmonic current emissions are within the limits specified by EMC regulations.

The capacity of the harmonic suppression unit should be determined in consultation with a power unit manufacturer in the same manner as the selection of power unit's output capacity previously discussed.

Notes for the field power supply unit of N-IO

As described in GS 32P06K20-01EN "Base Plate (for N-IO)", field power supply (24 V DC) is required when Digital output function of the base plate with disconnecting terminal (Model S2BN1D) is utilized.

When using the node interface unit S2NN30D-□4□□□□□□□ (24 V DC power input type) in combination with S2BN1D and the power supply unit as shown on the left side of the figure below, it is recommended to separate the power supply as shown in right.

This is because the rapid change of the field output load of S2BN1D may causes an influence on 24 V power line, it is worried that the input voltage rating of S2NN30D will not be satisfied.

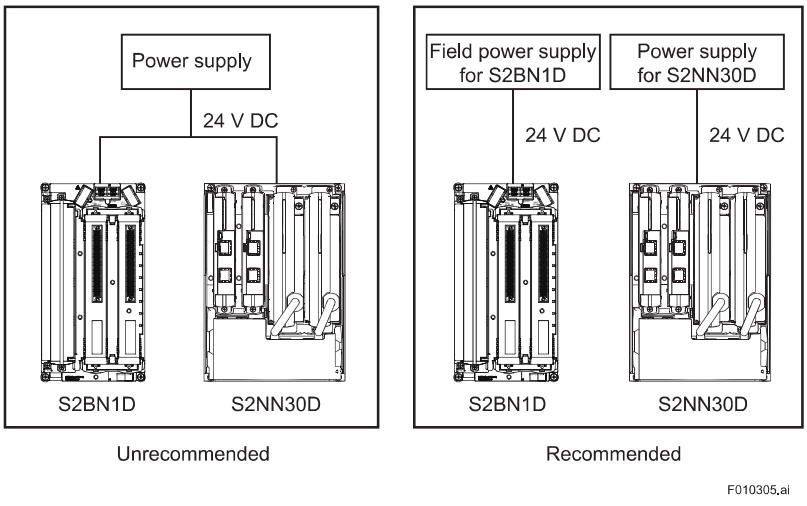


Figure Connection of the field power supply of S2BN1D

Cabling

Observe the following when cabling the power unit to the ProSafe-RS system equipment:

- Protect signal cables from induced noise.
- Protect signal cables from induction from high-voltage power lines.
- Separate the ProSafe-RS system power supply from other equipment power supplies. Use a separate power distribution board.
- Provide a dedicated breaker for each power supply.
- Install breakers and devices in the same room.
- Label the breakers with the name of the connected equipment.
- Install the breakers where they can be easily operated.
- The breaker, must not interrupt connection by wiring to protective grounding system.
- As far as possible install power supply cables and high-voltage power lines in metallic conduits.
- Use shielded cables if metallic conduits cannot be provided.

1.4 Grounding

To avoid electric shocks and minimize the influences of external noise, the installed devices must be grounded to the protective grounding system which complies with the safety standards, the electrical installations standard, and the power distribution system of the country or the region.

As for the protective grounding systems, the meshed grounding systems described in IEC 60364, IEC 62305 and IEC 61000-5-2 can be applied.

A protective device is to be installed in compliance with the rules and regulations, in order to prevent electric shocks caused by a ground fault.

A plug type power cable has to be connected to the receptacle connected to the protective grounding system.

Grounding Circuit

Grounding examples are given below.

If ProSafe-RS systems are housed in a cabinet, the cabinet must be grounded according to the grounding network topology of the building or plant for installation.

In order to connect a cabinet with a protective grounding system, the grounding topology shown in the figures “Grounding connected to a single grounding bus inlet” or “Grounding connected to each grounding bus inlet” can be used.

When providing lightning arresters on power and signal lines, those arresters need to be grounded to the same bus. For details, see Section 1.5, “Noise Countermeasures.”

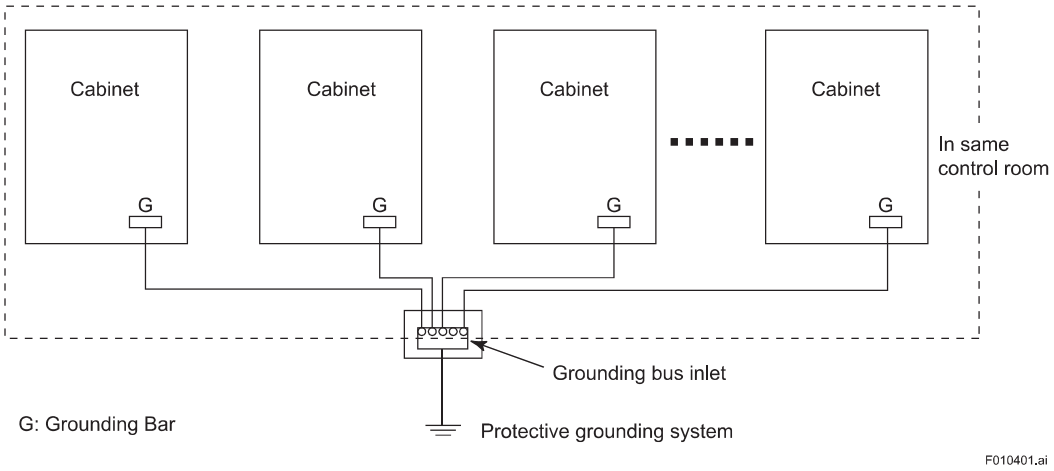


Figure Grounding connected to a single grounding bus inlet

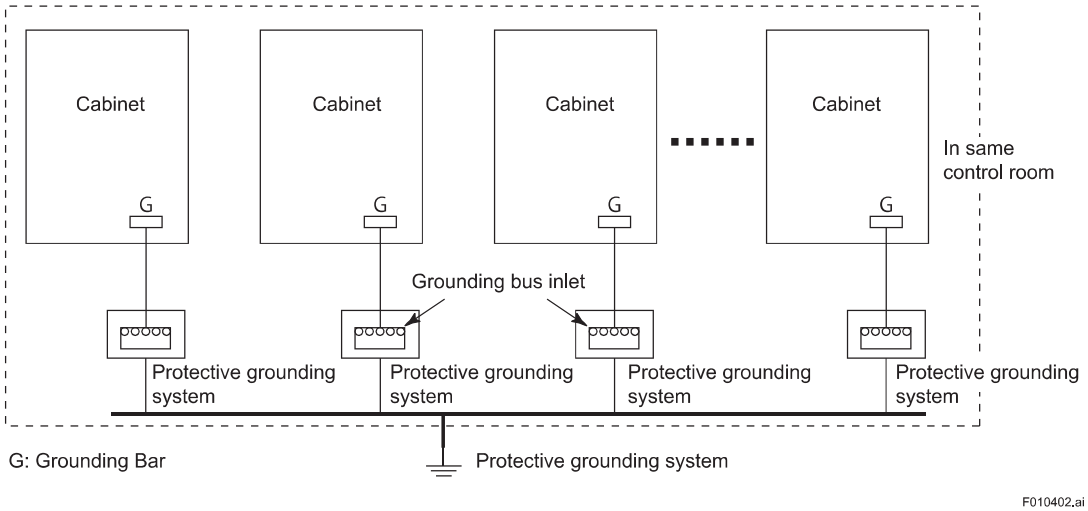


Figure Grounding connected to each grounding bus inlet

Grounding with Other System

Do not connect ProSafe-RS's cabinet with other system cabinets or consoles electrically using bolts or other connection mechanism in order to avoid unexpected electrical connection or interference.

When ProSafe-RS is joining side by side with other system cabinets or consoles, ensure to insert insulating sheets.

The cabinets or consoles other than ProSafe-RS must be insulated from a floor and connect it to a protective grounding system using a different grounding cable.

CENTUM VP can be treated as the ProSafe-RS system in this page.

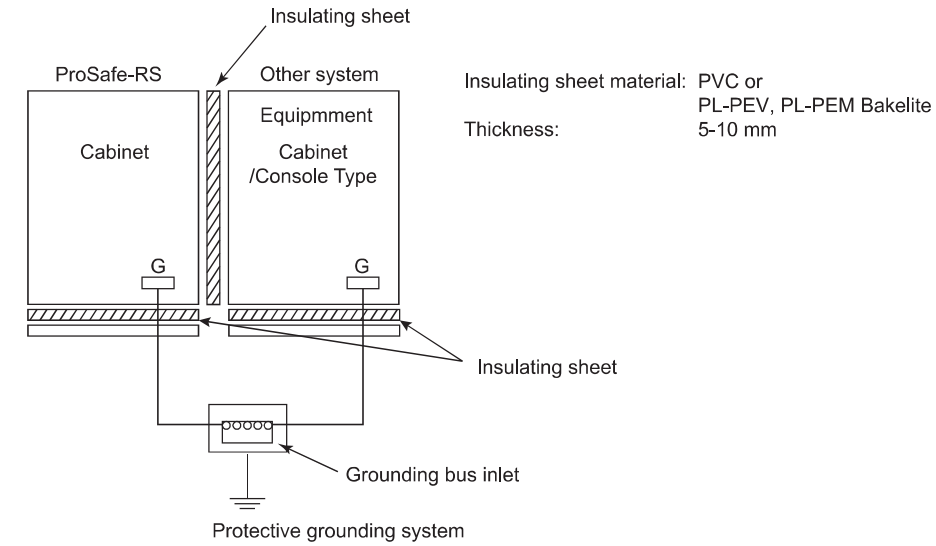


Figure Grounding Using Insulating Sheets

IMPORTANT

Do not install the following systems side-by-side with ProSafe-RS:

- Systems using power supply voltages over 300 V AC.
- Systems with current consumption over 50 A.
- System containing high frequency sources.

1.5 Noise Countermeasures

Noise may be induced by electromagnetic induction, electrostatic induction, or come from radio waves, lightning, inductive loads, static electricity and ground potential differences.

It can be picked up by power, signal and ground cables, and devices. With computerized control systems, noise-induced errors in A/D conversion or in an instruction word may lead to malfunction. Therefore, it is necessary to prevent the noise from being generated or coming too much from the outside.

To prevent noise and electrostatic buildup, take the measures described in this section when deciding cable type, cable routing, and grounding.

1.5.1 Noise Sources and Noise Countermeasures

It is not easy to identify the cause of any noise-triggered errors or failures due to their lack of reproducibility.

To prevent noise generation, it is necessary to consider the installation environments such as the external cable routing, cable types, and grounding.

The following table lists typical noise sources, symptoms of noise problems, and preventive countermeasures:

Table Noise Sources & Countermeasures

Noise sources	Effects	Countermeasures
Electromagnetic induction (magnetic field)	• CRT display instability, distortion, color shift, color fringing. • Destroys magnetic/flexible disk data.	• Maintain separation from magnetic-field source. • Shield power cables with metallic conduits. • Shield magnetic field using ferromagnetic substance (e.g. Permalloy). Or use LCD. • Use twisted-pair cables.
Electrostatic induction	• Equipment maloperation. • Interference with signals.	• Use shielded signal cables. • Electrically separate power and signal cables using metallic conduits and separators. • Lay power and signal cables which intersect at right angles.
Lightning	• Interference with signals. • Equipment maloperation. • Component damage.	• Lay cables underground. • Use optical fiber cables. • Lay cables as close to ground as possible if the cables cannot be laid underground. • Install and ground arresters on field and system.
Electrostatic discharge	• Equipment maloperation. • Electronic component deterioration, damage. • Paper jam.	• Discharge static electricity from operators. • Provide proper humidity. • Ground equipment properly. • Use antistatic floor material and clothing.
Inductive load open/close	• Spike noise interference to power andsignal lines.	• Add protection circuit for noise caused by inductive load. • Separate laying of cables.
Radio (electric field)	• CRT display disruption. • Equipment maloperation. • Interference with signals.	• Keep at least 1 m away from devices to use a transceiver or a PHS or a cellular phone (max. output is 1W).
Ground potential difference	• Equipment Maloperation (noise imposed on signal lines)	• Avoid multipoint grounding of signal cable.

Grounding with Lightning Arresters

Connect the protective conductor terminals of arresters and ProSare-RS equipment to the grounding pole as shown in the diagram below.

The grounding method must comply with the grounding system defined by rules and standards of the country or the region.

Concatenation grounding a lightning arrester and other equipment may cause high-tension in each equipment by the product of lightning current from arrester and grounding resistance. To prevent from electrification, overall connection should be equipotential including the floor and the case of other equipment.

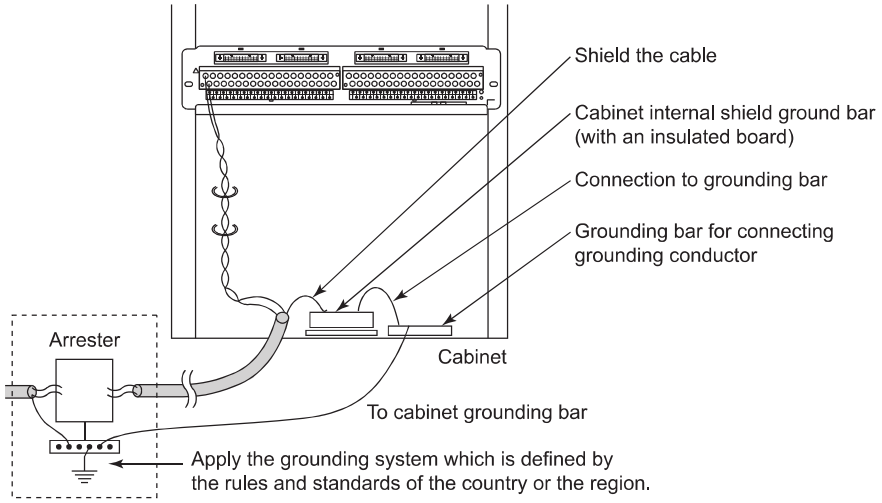
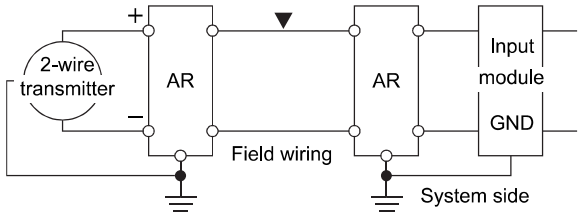


Figure Grounding with Lightning Arresters

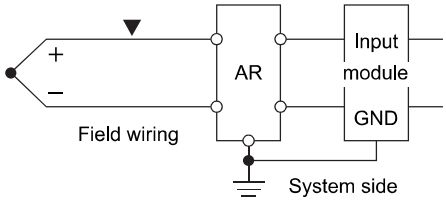
Examples of Arrester

The following shows how to install an arrester as a countermeasure against lightning-Induced noise.

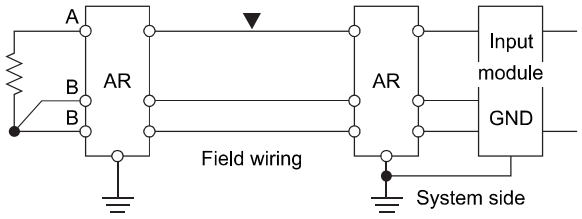
● 2-wire transmitter



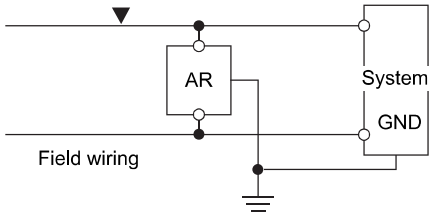
● Thermocouple



● Resistance temperature detector



● Power supply



▼: Induced lightning strike point
AR: Arrester

F010502E.ai

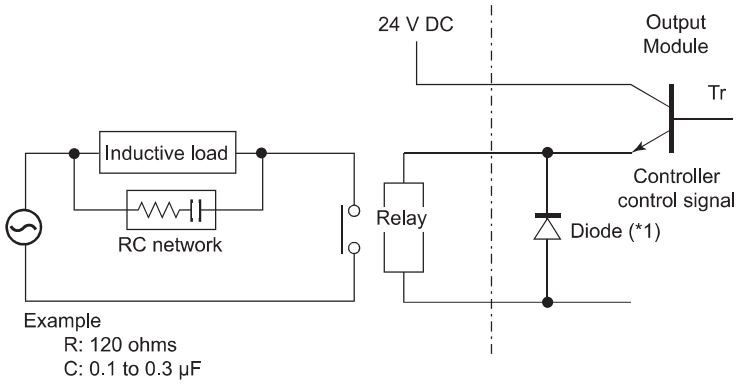
Figure Examples of Arrester Installation

Examples of installing protection circuit for noise caused by inductive load

The following shows how to install RC network and a diode as a countermeasure against noise caused by inductive load :

● Relay contact for FIO

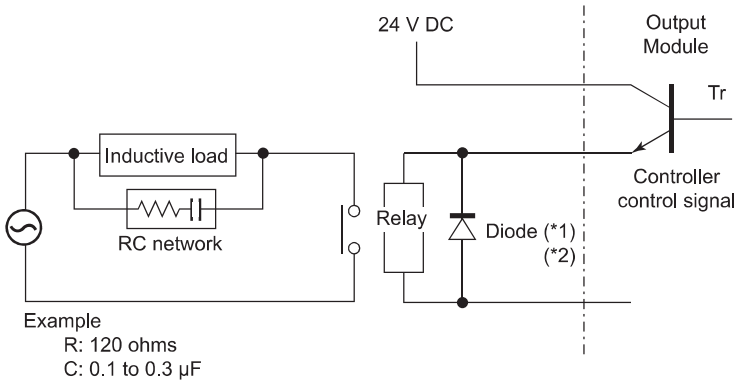
The RC network protects relay contacts from noise occurring when inductive loads working under AC operation are turned off.



*1: The diode, which protects the output transistor from noise occurring during on-to-off transition of the relay, is incorporated in the output module except SDV526.

● Relay contact for N-IO

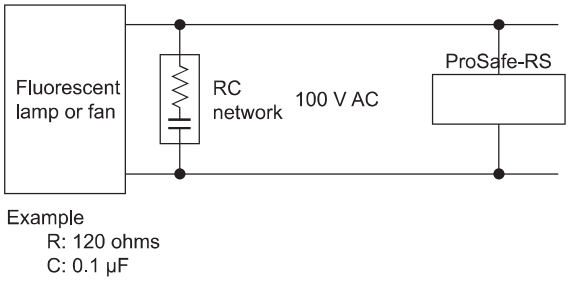
The RC network protects relay contacts from noise occurring when inductive loads working under AC operation are turned off.



*1: The diode protects the output transistor from noise occurring during on-to-off transition of the relay.
*2: S2MMM843 or S2MDV843 of style S2 or later has a built-in diode, so this diode is not required.

● Power supply

The RC network prevents noise-caused equipment failure when a fluorescent lamp or fan is turned on or off.



F010503.ai

Figure Examples of installing protection circuit for noise caused by inductive load

1.5.2 Countermeasures against Static Electricity

Take countermeasures against electrostatic damage when handling cards with semi-conductor IC components, for maintenance or to change settings.

Observe the following to prevent electrostatic damage:

- When storing or carrying maintenance parts, keep them in a conductive bag (when delivered from the factory, they are packed in such bags with labels warning about static electricity).
- When doing maintenance work, wear a wrist strap connected to a ground wire with a grounding resistance of 1 M ohm. Be sure to ground the wrist strap.

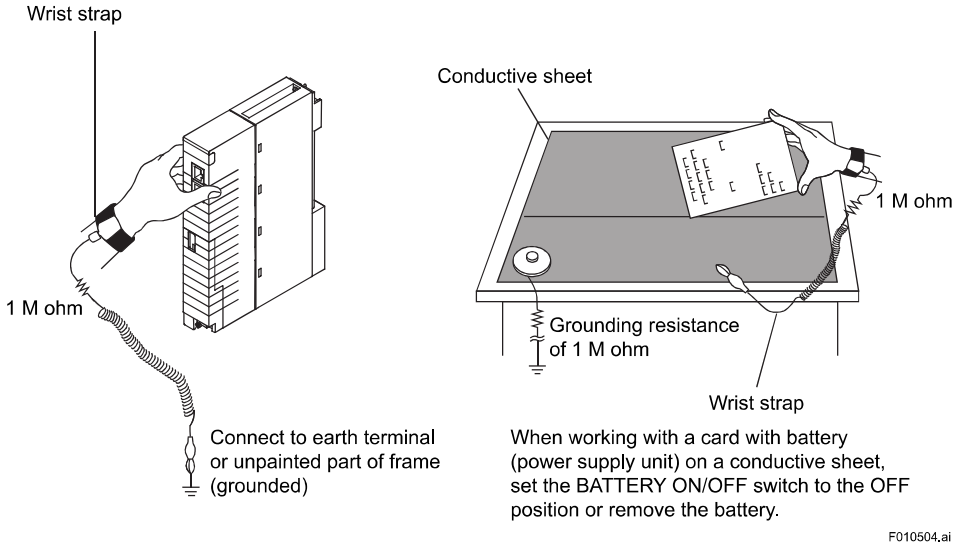


Figure Example of Use of A Wrist Strap and Conductive Sheet

- When working on cards: keep conductive sheets, grounded via a resistance of 1 M ohm, on the work bench. Wear a grounded wrist strap. Remove electrostatic plastics from the work bench.
- Be sure to wear a wrist strap and use a conductive sheet when handling maintenance parts.

1.6 Cabling Requirements

The following requirements must be fulfilled to prevent an equipment malfunction when laying power and signal cables (these are shielded cables unless specified).

Signal cables used for high-voltage, high-frequency signals (inductive load ON/OFF) must be separated from other signal cables.

Separator

To prevent an equipment malfunction, provide a separator between power and signal cables as illustrated below:

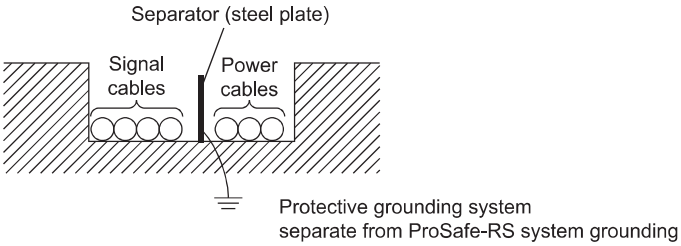


Figure Separator Used in Duct/Pit

Distance between Cables

If a separator cannot be used, keep a distance between signal cables and power cables.

The distances between cables due to operating voltages and currents are shown below.

Table Required Distance between Power & Shielded Signal Cables

Operating	voltage Operating	current Distance
240 V AC max	10 A max	150 mm min
	10 A min	600 mm min
240 V AC min	10 A max	600 mm min
	10 A min	Cannot be laid together

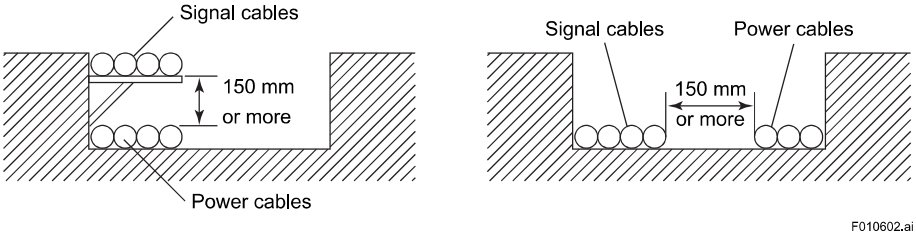


Figure Distance between Cables under Pit/Free-access Floor

Intersecting Cables

With unshielded power cables, place a grounded steel plate with a thickness of at least 1.6 mm over the cables where they intersect with signal cables.

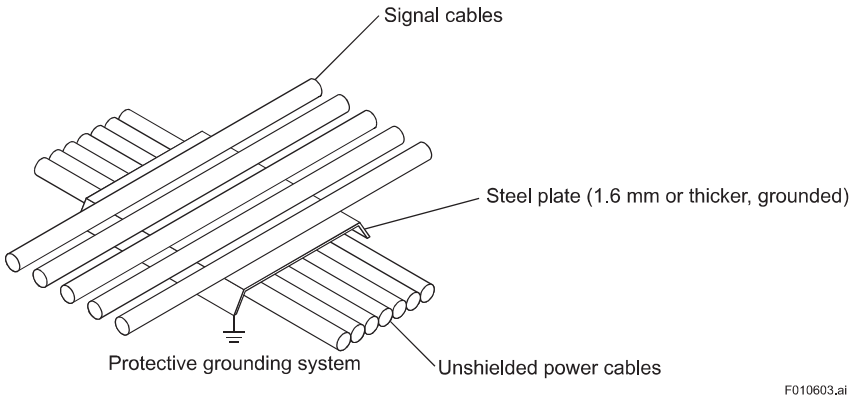


Figure Intersecting Cables under Pit/Free-access Floor

Ambient Temperature

The ambient temperature where signal and bus cables are laid must be within the limits specified for each cable.

Measures against EMI

As a rule, avoid laying the cables on the floor. However, lay them on the floor only if there are no duct and no pit. In that case, it is required to cover them with shield plates or take other measures to suit the EMC Directive.

1.7 Corrosive-gas Environment Compatibility

The ProSafe-RS system complies with the ANSI/ISA G3 environment requirements, allowing use in a corrosive gas-susceptible environment.

G3 Environment-compatible Products

Table G3 Environment-compatible Products (1/2)

No.	Product	Model	Description
1	Node unit	SSC60☐	Safety control unit (rack mountable type, for Vnet/IP)
		SSC50☐	Safety control unit (rack mountable type, for Vnet/IP)
		SSC57☐	Safety control unit (rack mountable type, for Vnet/IP-Upstream)
		S2SC70☐	Safety control unit (rack mountable type)
		SNB10D	Safety node unit (rack mountable type)
2	Input/output module	SAI143-S	Analog input module (4 to 20 mA, 16 channels, Module isolation)
		SAI143-H	Analog input module (4 to 20 mA, 16 channels, Module isolation, HART Communication)
		SAV144	Analog input module (1 to 5 V/1 to 10 V, 16 channels, Module isolation)
		SAI533	Analog output module (4 to 20 mA, 8 channels, Module isolation, HART Communication)
		SAT145	TC/mV Input Module (16 channels, Isolated Channels)
		SAR145	RTD Input Module (16 channels, Isolated Channels)
		SDV144	Digital input module (no-voltage contact, 16 channels, Module isolation)
		SDV521	Digital output module (24 V DC/2 A, 4 channels, Module isolation)
		SDV526	Digital output module (100-120 V AC, 4 channels, Module isolation)
		SDV531	Digital output module (24 V DC, 8 channels, Module isolation)
		SDV53A	Digital output module (48 V DC, 8 channels, Module isolation)
		SDV541	Digital output module (24 V DC, 16 channels, Module isolation)
3	ESB Bus Interface Module	SEC402	ESB Bus Coupler Module (2-port)
		SEC401	ESB Bus Coupler Module
	N-ESB Coupler Module	S2EN402	N-ESB Bus Coupler Module (2-port)
		S2EN404	N-ESB Bus Coupler Module (4-port)
4	Unit for Optical Bus Repeater Module	SNT10D	Unit for Optical Bus Repeater Module
5	Optical ESB Bus Repeater Module	SNT401	Optical ESB Bus Repeater Master Module
		SNT501	Optical ESB Bus Repeater Slave Module
		SNT411	Optical ESB Bus Repeater Master Module 5 km - 50 km
		SNT511	Optical ESB Bus Repeater Slave Module 5 km - 50 km
6	Communication module	ALR111-☐☐1	Serial communication module (RS-232C, 2-port)
		ALR121-☐☐1 ALR121-☐☐B ALR121-☐☐3	Serial communication module (RS-422/RS-485, 2-port)
		ALE111-☐☐1 ALE111-☐☐3	Ethernet communication module
		S2LP131	Fire and gas communication module
7	Wiring check adapter	SCB1☐0	Wiring check adapter for digital input module
8	Power supply bus unit	AEPV7D-☐☐6 AEPV7D-☐☐F	Power Supply Bus Unit, Vertical Type
		AEP7D-☐6 AEP7D-☐F	Primary power supply bus unit

Table G3 Environment-compatible Products (2/2)

No.	Product	Model	Description
9	Terminal Board	A2BM4	Terminal board for analog digital I/O (for N-IO)
		SEA4D	Analog terminal board (Single and Dual-redundant, 16 channels x 2)
		SBA4D	Terminal board for Analog: DIN rail mount type (Single and Dual-redundant, 16 channels x 1)
		SBT4D	Terminal board for TC/mV: DIN rail mount type (Single and Dual-redundant, 16 channels x 1)
		SBR4D	Terminal board for RTD input: DIN rail mount type (Single and Dual-redundant, 16 channels x 1)
		SED2D	Digital terminal board (Single and Dual-redundant, 4 channels x 4)
		SED3D	Digital terminal board (Single and Dual-redundant, 8 channels x 4)
		SED4D	Digital terminal board (Single and Dual-redundant, 16 channels x 2)
		SWD2D	Digital terminal board (Single and Dual-redundant, 100 to 120 V AC, 4 channels x 4)
		SBD2D	Terminal board for Digital output: DIN rail mount type (Single and Dual-redundant, 4 channels x 1, for SDV521)
		SBD3D	Terminal board for Digital output: DIN rail mount type (Single and Dual-redundant, 8 channels x 1, for SDV53□)
		SBD4D	Terminal board for Digital: DIN rail mount type (Single and Dual-redundant, 16 channels x 1, for SDV144/SDV541)
		S1BB4D	Terminal Board for Analog Input, 3-wire: DIN rail mount type
10	Router	AVR10D-□□□□□1	Duplexed V net router
		AW810D-□□□□□6	Wide Area Communication Router
11	Node Interface Unit	S2NN30D	Node Interface Unit (for N-IO)
12	Base Plate	S2BN1D	Base Plate with disconnecting terminal (for N-IO, 16 channels)
		S2BN4D	Base Plate for Barrier (for N-IO, MTL Barrier)
		S2BN5D	Base Plate for Barrier (for N-IO, P+F Barrier)
13	I/O Module	S2MMM843	Analog Digital I/O Module (16 channels, module isolation)
		S2MDV843	Digital I/O Module (16 channels, module isolation)

Outline of G3 Environment Compatibility

The classification of the environment in which the process control equipment is installed is determined by the ANSI/ISA S71.04 “Environmental Conditions for Process Control Systems” standard. The environment having an atmosphere which contains steams and mists (liquids, coded L), dusts (solids, coded S), or corrosive gases (gases, coded G) is classified into four categories according the levels of these substances determined.

The four categories of the corrosive gas environment are defined as follows:

G1 (Mild): A well-controlled environment in which corrosive gas is not the major cause adversely affecting the reliability of plant equipment. The corrosion level on the copper test piece is below 0.03 µm (see note below).

G2 (Moderate): An environment in which corrosive gas can be detected and it could be determined that the gas is the major cause adversely affecting the reliability of plant equipment. The corrosion level on the copper test piece is below 0.1 µm (see note below).

G3 (Harsh): An environment in which corrosive gas is frequently generated to cause corrosion and that it is necessary to provide special measures or employ specially designed or packaged plant equipment. The corrosion level on the copper test piece is below 0.2 µm (see note below).

GX (Severe): A corrosive gas-polluted environment that demands special protective chassis for the plant equipment, specifications of which should be seriously determined by the user and a power unit manufacturer. The corrosion level on the copper test piece is 0.2 µm or more (see note below).

Note: Copper test pieces are used to determine the level of corrosion for the classification of the plant environment.
The test piece is an oxygen-free copper sheet, which is 15 cm^2 in area, 0.635 mm in thickness, 1/2 to 3/4H in hardness. The test piece is placed in the plant site for one month and checked for any change before and after the test to determine the degree of corrosion (see table below). If the test period is shorter than one month, the result is calculated to obtain equivalent data using a expression defined by the standard.

Table Classification of Corrosive-gas Corrosion Levels

Environment category		G1 (Mild)	G2 (Moderate)	G3 (Harsh)	GX (Severe)	
Copper corrosion level		< 300 (< 0.03)	< 1000 (< 0.1)	< 2000 (< 0.2)	≥ 2000 (≥ 0.2)	[Å] ([µm])
Group A	H_2S	< 3	< 10	< 50	≥ 50	[mm^3/m^3]
	SO_2, SO_3	< 10	< 100	< 300	≥ 300	
	Cl_2	< 1	< 2	< 10	≥ 10	
	NOx	< 50	< 125	< 1250	≥ 1250	
Group B	HF	< 1	< 2	< 10	≥ 10	
	NH_3	< 500	< 10000	< 25000	≥ 25000	
	O_3	< 2	< 25	< 100	≥ 100	

Note: The gas density data indicated in the table are for reference only, with the relative humidity of 50% RH or less.
The category goes up one rank higher every time the humidity increases 10% exceeding the 50% RH or over 6% per hour.

The Group-A gases shown in the table may coexist and cause inter-reaction. Inter-reaction factors are not known for the Group-B gases.

1.8 Compliance with Marine Standards

The ProSafe-RS offers compliance with the following marine standards:

- **ABS (American Bureau of Shipping)**
- **BV (Bureau Veritas)**
- **LR (Lloyd's Register), ENV3**
- **DNV GL**

This Section introduces the components of systems which comply with the marine standards, and precautions for installing those components.

Marine Standard-compliant ProSafe-RS Components

The table below shows the ProSafe-RS components which comply with the marine standards.

Table Marine Standard-compliant ProSafe-RS Components (1/3)

Product	Model	Module Type	Description
Node Unit	S2SC70S-F	Safety control Unit (19-inch rack mountable)	Including SCP461, S2CP471, SPW481, SPW482, and SPW484. S2SC70S-S and S2SC70D-S do not comply.
	S2SC70D-F		
	SSC60S-F	Safety control unit (19-inch rack mountable)	Including SCP461, S2CP471, SPW481, SPW482 and SPW484. SSC60S-S and SSC60D-S do not comply.
	SSC60D-F		
	SSC50S	Safety control unit (19-inch rack mountable)	Including SCP451, SPW481, SPW482 and SPW484. (*2) Suffix code "-F" is certified for category ENV3, and "-S" is certified for category ENV2.
	SSC50D		
	SSC57S		
	SSC57D		
	SNB10D	Node unit for dual-redundant ESB bus (19-inch rack mountable)	Including SSB401, SPW481, SPW482 and SPW484.
Node Interface Unit	S2NN30D	Node Interface Unit (for N-IO)	Exclude DIN rail type. Including S2EN501, S2PW503 and S2PW504. S2PW503 and S2PW504 are applicable only when attached to S2NN30D.
Base Plate	S2BN1D	Base plate with disconnecting terminal (for N-IO)	Exclude DIN rail type.
	S2BN4D	Base plate for Barrier (for MTL Barrier)	
	S2BN5D	Base plate for Barrier (for P+F Barrier)	
I/O Module	S2MMM843	Analog digital I/O module	
	S2MDV843	Digital I/O module	
Input/Output Module	SAI143	Analog input module (4 to 20 mA, 16 channels, and module isolation)	(*1) SAI143-H□C does not comply.
	SAV144	Analog input module (1 to 5 V/1 to 10 V and module isolation)	Including SCCC01, STB4D, STB4S and STK4A.
	SAT145	TC/mV input module (16 channels, Isolated Channels)	
	SAR145	RTD input module (16 channels, Isolated Channels)	
	SAI533	Analog output module (4 to 20 mA, 8 channels and module isolation)	(*1)

*1: Including SCCC01, STA4D, STA4S and STK4A.
*2: Except for SSC50□-□□□□1, SSC50□-□□□□2, SSC57□-□□□□1, SSC57□-□□□□2 and SCP451-□1.

Table Marine Standard-compliant ProSafe-RS Components (2/3)

Product	Model	Module Type	Description
Input/Output Module	SDV144	Digital input module (16 channels, contact input and module isolation)	(*2) SDV144-S□C does not comply.
	SDV521	Digital output module (4 channels, 24 V DC/2A, and module isolation)	SDV521-S3C does not comply.
	SDV531	Digital output module (8 channels, 24 V DC, and module isolation)	(*2) SDV531-L complies with Marine Standards from style code S3. SDV531-L□C does not comply.
	SDV53A	Digital output module (8 channels, 48 V DC, and module isolation)	
	SDV541	Digital output module (16 channels, 24 V DC, and module isolation)	(*2) SDV541-S□C does not comply.
	SDCV01	Dummy cover (for I/O modules)	
Wiring Check Adapter	SCB100	Wiring check adapter for digital input	
	SCB110		
Unit for Optical Bus Repeater Module	SNT10D	Unit for optical bus repeater module	Including SPW481, SPW482 and SPW484.
Optical ESB bus repeater module	SNT401	Optical ESB bus repeater master module	
	SNT411	Optical ESB bus repeater master module 5 km to 50 km	
	SNT501	Optical ESB bus repeater slave module	
	SNT511	Optical ESB bus repeater slave module 5 km to 50 km	
ESB Bus Interface Module	SEC402	ESB bus coupler module	
	SEC401		
N-ESB Bus Coupler Module	S2EN402	N-ESB Bus coupler Module (for 2-port)	
	S2EN404	N-ESB Bus coupler Module (for 4-port)	
Cover	S2DCV02	Dummy cover (for N-IO I/O module)	
Communication Module	ALR111	Serial communications module (RS-232C, 2-port)	
	ALR121	Serial communications module (RS-422/RS-485, 2-port)	
	ALE111	Ethernet communication module	
	S2LP131	Fire and Gas Communication Module	
Terminal Board	SEA4D	Analog terminal board (single and dual-redundant, 16 channels x 2)	
	SED2D	Digital terminal board (single and dual-redundant, 4 channels x 4)	
	SED3D	Digital terminal board (single and dual-redundant, 8 channels x 4)	
	SED4D	Digital terminal board (single and dual-redundant, 16 channels x 2)	
	SBT4D	Terminal board for TC/mV: DIN rail mount type (Single and Dual-redundant, 16 channels x 1)	
	A2BM4	Terminal board for analog digital I/O (for N-IO)	

*1: Including SCCC01, STA4D, STA4S and STK4A.
*2: Including SCCC01,SCCC02, STB4D, STB4S and STD4A.

Table Marine Standard-compliant ProSafe-RS Components (3/3)

Product	Model	Module Type	Description
Terminal Board	SBR4D	Terminal board for RTD input: DIN rail mount type (Single and Dual-redundant, 16 channels x 1)	
	SBA4D	Terminal board for Analog: DIN rail mount type (Single and Dual-redundant, 16 channels x 1)	
	SBD2D	Terminal board for Digital output: DIN rail mount type (Single and Dual-redundant, 4 channels x 1, for SDV521)	
	SBD3D	Terminal board for Digital output: DIN rail mount type (Single and Dual-redundant, 8 channels x 1, for SDV53□)	
	SBD4D	Terminal board for Digital: DIN rail mount type (Single and Dual-redundant, 16 channels x 1, for SDV144/SDV541)	
	S1BB4D	Terminal Board for Analog Input, 3-wire: DIN rail mount type	
Relay Board	SRM53D	Relay Board (8 × 2 dry contact output)	
	SRM54D	Relay Board (16 × 1 dry contact output)	
	SBM54D	Relay board for Digital output: DIN rail mount type (Single and Dual-redundant, 16 channels x 1, for SDV541)	
Control Bus Interface	VI702	Control bus interface card	(*3)
V net Router	AVR10D -□□□□□1	Duplexed V net router	AVR10D-□□□□□0 does not comply.
Cable, etc.	YCB301	ESB bus cable	
	AKB651	Signal cable (50 - 50 pins) (for connections between SDV521 and Terminal Board)	When AKB651 is connected to SDV531-L, SDV53A or SDV541, it does not comply.
	AKB331	Signal cable (50 - 50 pins)	
	AKB136	RS-232C null modem cable (9 - 25 pins)	
	AKB161	RS-422/RS-485 cable	
	AKB611	Signal cable (for connections between SAR145 and Terminal Board)	
	KS1	Signal cable (40 - 40 pins)	
	S2KLF10	F-SB bus cable	
	S2KPB10	Power supply cable for Base plate	

*3: Noisecut transformer shall be attached in the power-line cable of SENG.

Precaution on Selecting System Components

When building a system, use components which have already obtained type approval for marine standards. For the SENG and HISs too, use generic computers (including monitors, keyboards, mice, and other peripheral devices) which are accredited by the required marine standards.

Precaution on Installing Components

Each component shall be installed in accordance with its installation guidance. In addition, all components related with S2SC70☐-F, SSC60☐-F, SSC50☐, SSC57☐, SNB10D, SNT10D and SENG shall be installed in a metal cabinet.
Furthermore, the following conditions are indispensable to conform to a marine standard.

- The cabinets including their doors and side panels must be made of a metal.
- Securely connect the cabinet frames and ground bosses on doors and side panels to each other to ensure electric contacts.
- Attach noise suppression devices, such as noise filters and ferrite cores, to the cables connecting each component.

Installation of Power-line Noise Filter

Attach a noise filter on the power line for the following components:

- Safety Control Unit (S2SC70☐-F, SSC60☐-F, SSC50☐,SSC57☐)
- Safety Node Unit (SNB10D)
- Unit for Optical Bus Repeater Module (SNT10D)
- Safety Control PC (SENG) installed control bus interface (VI702)

Power-line for S2SC70☐-F, SSC60☐-F, SSC50☐, SSC57☐, SNB10D, SNT10D and S2NN30D

Attach a noise filter in each power line of SPW48☐, S2PW50☐, FAN and external power supply unit. Alternatively, other devices such as noisecut transformer and insulating transformer can be used if its characteristic of noise-reducing effects is same as the following equipment.

Noise filter and external power supply unit shall be installed in the same cabinet of the connecting terminal board for them.

If digital Input/output modules such as SDV144, SDV521, SDV531, SDV53A and SDV541 are used, use a power supply whose output-ground is insulated for external power supply.

Wiring examples of power cables (a) to (d) are shown below according to the mounting position of the noise filter and the tap.

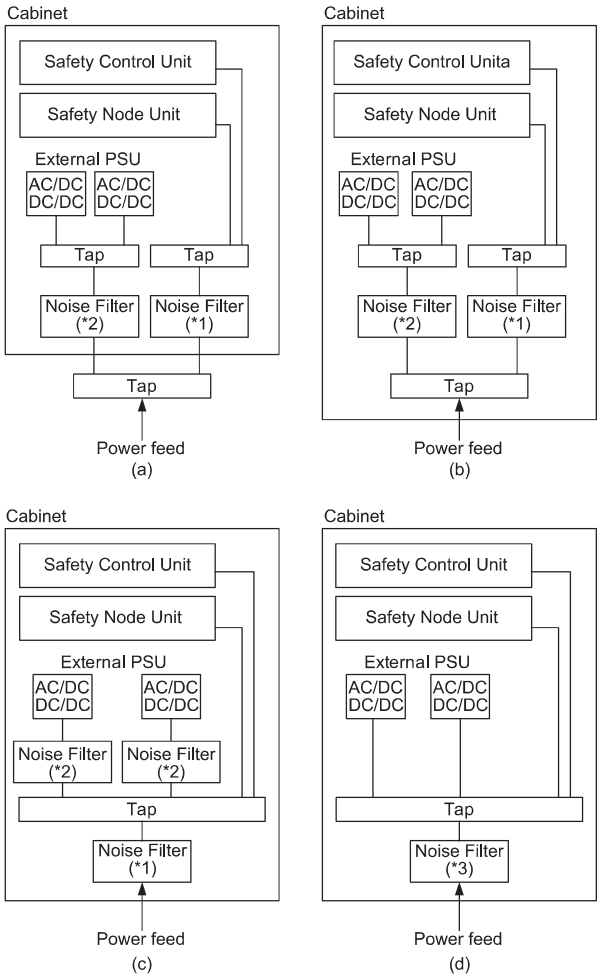


Figure Wiring for power cables

*1: This noise filter is for the power line of SPW48☐, S2PW50☐, and FAN. Refer to "Table Example of a noise filter for the power line of SPW48☐, S2PW50☐, and FAN.".
*2: This noise filter is for the external power supply unit. Regarding necessity of the noise filter, please follow directions on instructions for marine standards of this external power supply unit.
*3: If the noise filter for the external power supply unit is equivalent to the ones of "Table Example of a noise filter for the power line of SPW48☐, S2PW50☐, and FAN.", both noise filters can be shared.

The following table shows example of a noise filter.
Table Example of a noise filter for the power line of SPW48☐, S2PW50☐, and FAN.

Category	Manufacturer	Model no.	Power Source
Noise filter	OKAYA Electric Industries Co., LTD	SUP-P30H-EPR-4	100 - 120 V AC, 220 - 240 V AC (*1)
		SUPH-EX10-ER-6	100 - 120 V AC, 220 - 240 V AC
	COSEL Co., LTD	NBH-20-432	24 V DC (*2)

*1: For S2PW50☐, SUPH-EX10-ER-6 can be used.
*2: For expansion or modification of unit, the existing TDK Lambda PSHN-2020 can also be used.

IMPORTANT

Lay the incoming wires to a noise filter separately from its outgoing wires.
Minimize the wiring to the ground terminals of the noise filters to minimize the impedance.

Power-line for SENG

Noisecut transformer shall be installed in the cabinet and attached in the power-line cable of SENG in case of using VI702.
The following table shows applicable noisecut transformer.

Table Applicable noisecut transformer

Description	Manufacturer	Model
Noisecut Transformer	DENKENSEIKI Research Institute CO., Ltd	NCT-I1 (*1)
	TAMURA Corporation	NRPT-TB0.5 (*2)

*1: Purchase it through distributer.
*2: Sales was terminated. Use NCT-I1 when purchase noisecut transformer newly.

IMPORTANT

Lay the incoming wires to a noisecut transformer separately from its outgoing wires.

Minimize the wiring to the ground terminal of the noisecut transformer to minimize the impedance.

Installation of Ferrite Cores for Vnet/IP

Attach ferrite cores on the power cables, the communication cables and the signal cables. The following table shows the cables to which ferrite cores are to be attached, the models and quantities of the ferrite cores to be attached, and the locations at which they are to be attached. Ferrite core is not required if the component is not listed below. See also the figure following the table for the locations of installation.

Table Cables that Need Ferrite Cores to be Attached to, and Ferrite Core Models and Quantities for Vnet/IP (1/3)

Component		Description	Ferrite Core Model (*1)	Quantity	Location (See the Figures)
Power supply	S2SC70☐-F Power module	AC/DC power cable	ZCAT3035-1330	3	(1)
	SSC60☐-F Power module	AC/DC power cable	ZCAT3035-1330	3	(1)
	SSC50☐ Power module	AC/DC power cable	ZCAT3035-1330	2	—
	SSC57☐ Power module	AC/DC power cable	ZCAT3035-1330	2	—
	SNB10D Power module	AC/DC power cable	ZCAT3035-1330	4	(2)
	SNT10D Power module	AC/DC power cable	ZCAT3035-1330	2	(3)
	AVR10D Power module	AC/DC power cable	ZCAT3035-1330	4	(4)
Fan	S2SC70☐-F Fan unit	AC/DC power cable	ZCAT3035-1330	3	(5)
	SSC60☐-F Fan unit	AC/DC power cable	ZCAT3035-1330	3	(5)
	SSC50☐-F Fan unit	AC/DC power cable	ZCAT3035-1330	2	—
	SSC57☐-F Fan unit	AC/DC power cable	ZCAT3035-1330	2	—
External power supply (Input side)	Power Supply (SDV531, SDV541)	AC power cable (Input side)	ZCAT3035-1330	1	(6)
			ZCAT2032-0930	1	

*1: The part number of ZCAT3035-1330 is A1179MN, and ZCAT2032-0930 is A1193MN.
Models ZCAT3035-1330 and ZCAT2032-0930 are from TDK Corporation.

Table Cables that Need Ferrite Cores to be Attached to, and Ferrite Core Models and Quantities for Vnet/IP (2/3)

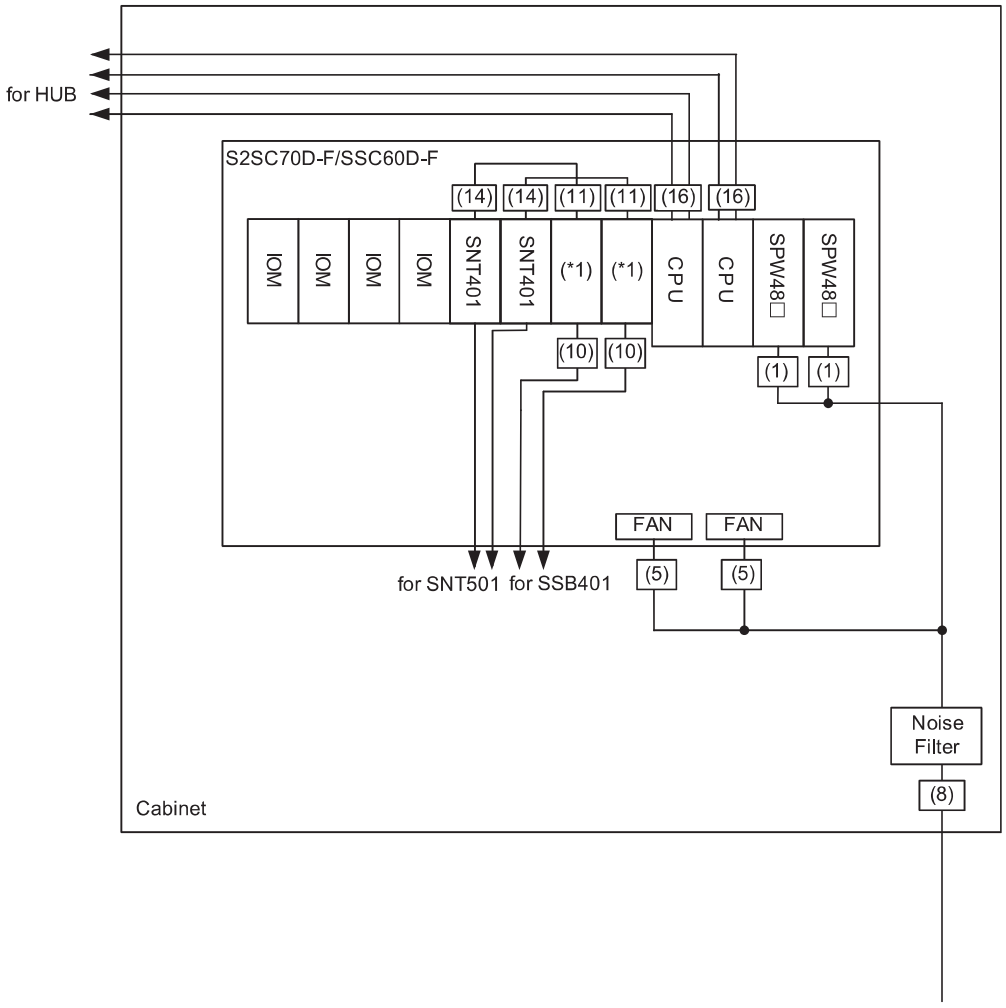
Component		Description	Ferrite Core Model (*1)	Quantity	Location (See the Figures)
External power supply (output side)	Power Supply (SDV531, SDV541)	DC power cable (Output side)	ZCAT3035-1330	3	(7)
			ZCAT2032-0930	1	
	Power Supply (SDV521, SDV53A)	DC power cable (Output side)	ZCAT3035-1330	1	
Noise filter (Input side)	AC power-line filter	AC power cable	ZCAT3035-1330	1	(8)
			ZCAT2032-0930	3	
			ZCAT3035-1330	1	(9)
ESB bus coupler module	SEC402	ESB bus cable	ZCAT3035-1330	5	(10)
	SEC401	ESB bus cable	ZCAT3035-1330	5	(10)
			ZCAT3035-1330	1	(11)
ESB bus interface module	SSB401	ESB bus cable	ZCAT3035-1330	4	(12)
			ZCAT3035-1330	1	(13)
Optical ESB bus repeater module	SNT401	ESB bus cable	ZCAT3035-1330	1	(14)
	SNT501	ESB bus cable	ZCAT3035-1330	1	(15)
CPU	SCP461 S2CP471	Vnet/IP cable	ZCAT3035-1330	1	(16)
	SCP451	Vnet/IP cable	ZCAT3035-1330	3	—
Fan unit	SSC60□-F Fan unit	Flat cable	ZCAT3035-1330	1	— (*3)
	SSC50□-F Fan unit	Flat cable	ZCAT3035-1330	1	— (*3)
	SSC57□-F Fan unit	Flat cable	ZCAT3035-1330	1	— (*3)
Analog module	SAI143	KS1 cable	ZCAT3035-1330	4	(17)
	SAV144				
	SAI533				
Digital module	SDV144	AKB331 cable	ZCAT3035-1330	3	(18)
	SDV521	AKB651 cable	ZCAT3035-1330	4	
	SDV531	AKB331 cable	ZCAT3035-1330	3	
	SDV53A	AKB331 cable	ZCAT3035-1330	3	
	SDV541	AKB331 cable	ZCAT3035-1330	3	
Terminal board	SEA4D	KS1 cable	ZCAT3035-1330	1	(19)
	SED4D	AKB331 cable	ZCAT3035-1330	1	(20)
Relay board	SRM53D	AKB331 cable	ZCAT3035-1330	3	—
	SRM54D				
Bus converter	VC401	V net cable	ZCAT3035-1330	4	(21)
	VI451	Vnet/IP cable	ZCAT3035-1330	4	(22)
N-ESB bus coupler modules	S2EN402	N-ESB Bus cable	—	—	—
	S2EN404	N-ESB Bus cable	—	—	—

*1: Quantity "—": Ferrite core is not necessary.
*2: The part number of ZCAT3035-1330 is A1179MN, and ZCAT2032-0930 is A1193MN.
Models ZCAT3035-1330 and ZCAT2032-0930 are from TDK Corporation.
*3: The component is mounted on the standard model.

Table Cables that Need Ferrite Cores to be Attached to, and Ferrite Core Models and Quantities for Vnet/IP (3/3)

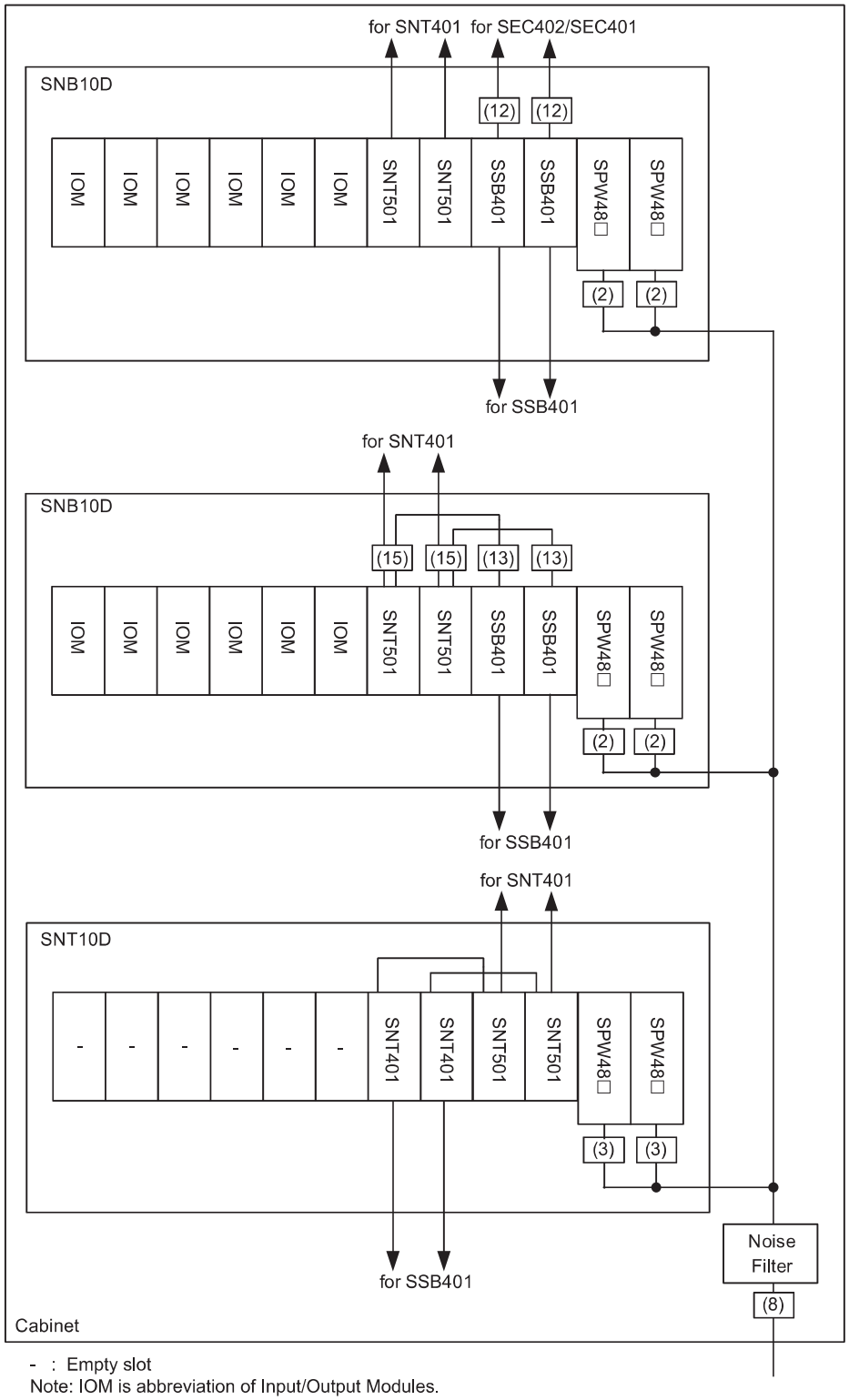
Component		Description	Ferrite Core Model (*1)	Quantity	Location (See the Figures)
Node Interface Unit	S2NN30D	N-ESB Bus/Optical ESB Bus cable	—	—	—
		Power supply input cable	—	—	—
		System power supply cable (S2KLF10)	—	—	—
		System power supply output cable (S2KPB10)	—	—	—
		External alarm input cable	—	—	—
Base Plate	S2BN1D	F-SB bus cable (S2KLF10)	—	—	—
		System power supply cable (S2KPB10)	—	—	—
		Field power supply cable	—	—	—
	S2BN4D	F-SB bus cable (S2KLF10)	—	—	—
		System power supply cable (S2KPB10)	—	—	—
		Field power supply cable	—	—	—
	S2BN5D	F-SB bus cable (S2KLF10)	—	—	—
		System power supply cable (S2KPB10)	—	—	—
		Barrier power cables	—	—	—
Terminal Boards	S1BB4D	Power supply cable	—	—	—
		Ready contact cable	—	—	—

*1: Quantity "—", Ferrite core is not necessary.



*1: SEC401/SEC402 ESB Bus Coupler Module
Note: IOM is abbreviation of Input/Output Modules.
Note: Figures in ( ) show the locations listed in "Table Cables that Need Ferrite Cores to be Attached to, and Ferrite Core Models and Quantities". It is NOT a number of ferrite core.

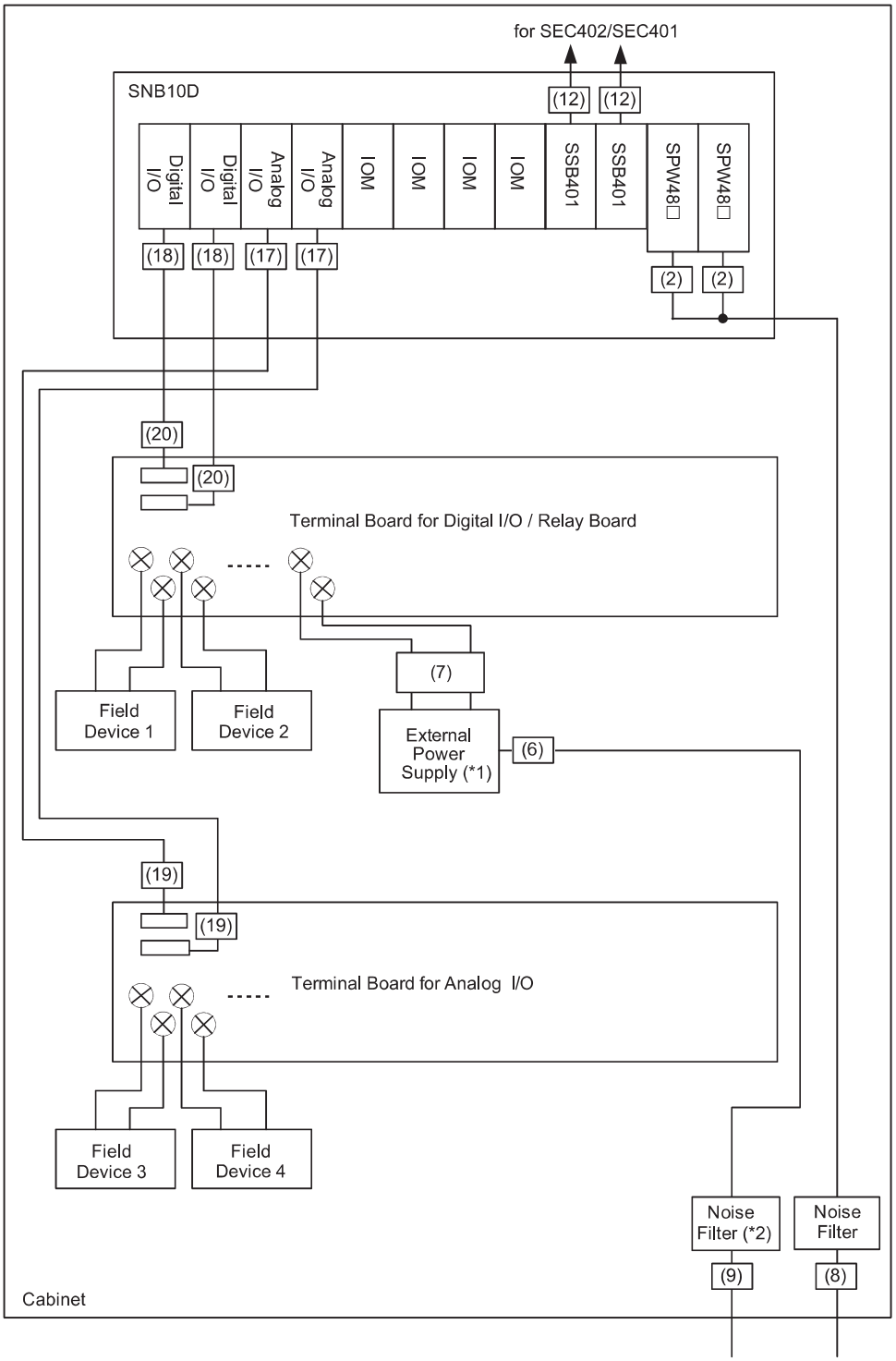
Figure Locations of Ferrite Core Installation for S2SC70D-F/SSC60D-F



- : Empty slot
Note: IOM is abbreviation of Input/Output Modules.
Note: Figures in ( ) show the locations listed in "Table Cables that Need Ferrite Cores to be Attached to, and Ferrite Core Models and Quantities". It is NOT a number of ferrite core.

F010803.ai

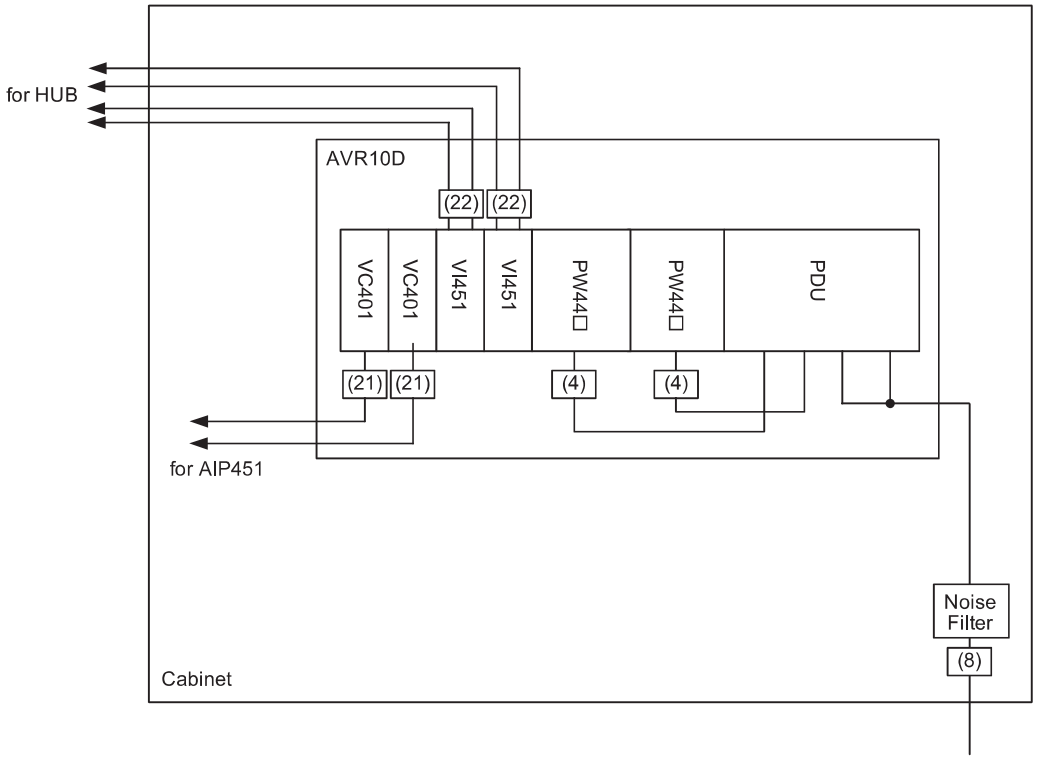
Figure Locations of Ferrite Core Installation for SNB10D and SNT10D



F010804.ai

Note: IOM is abbreviation of Input/Output Modules.
Note: Figures in ( ) show the locations listed in "Table Cables that Need Ferrite Cores to be Attached to, and Ferrite Core Models and Quantities". It is NOT a number of ferrite core.
*1: When supplying 24 V DC from outside of a cabinet, it isn't necessary to install "External Power Supply". But, when not installing this "External Power Supply", it's necessary to install (6) and (7).
*2: This noise filter is for the external power supply unit. Regarding necessity of the noise filter, please follow directions on instructions for marine standards of this external power supply unit.

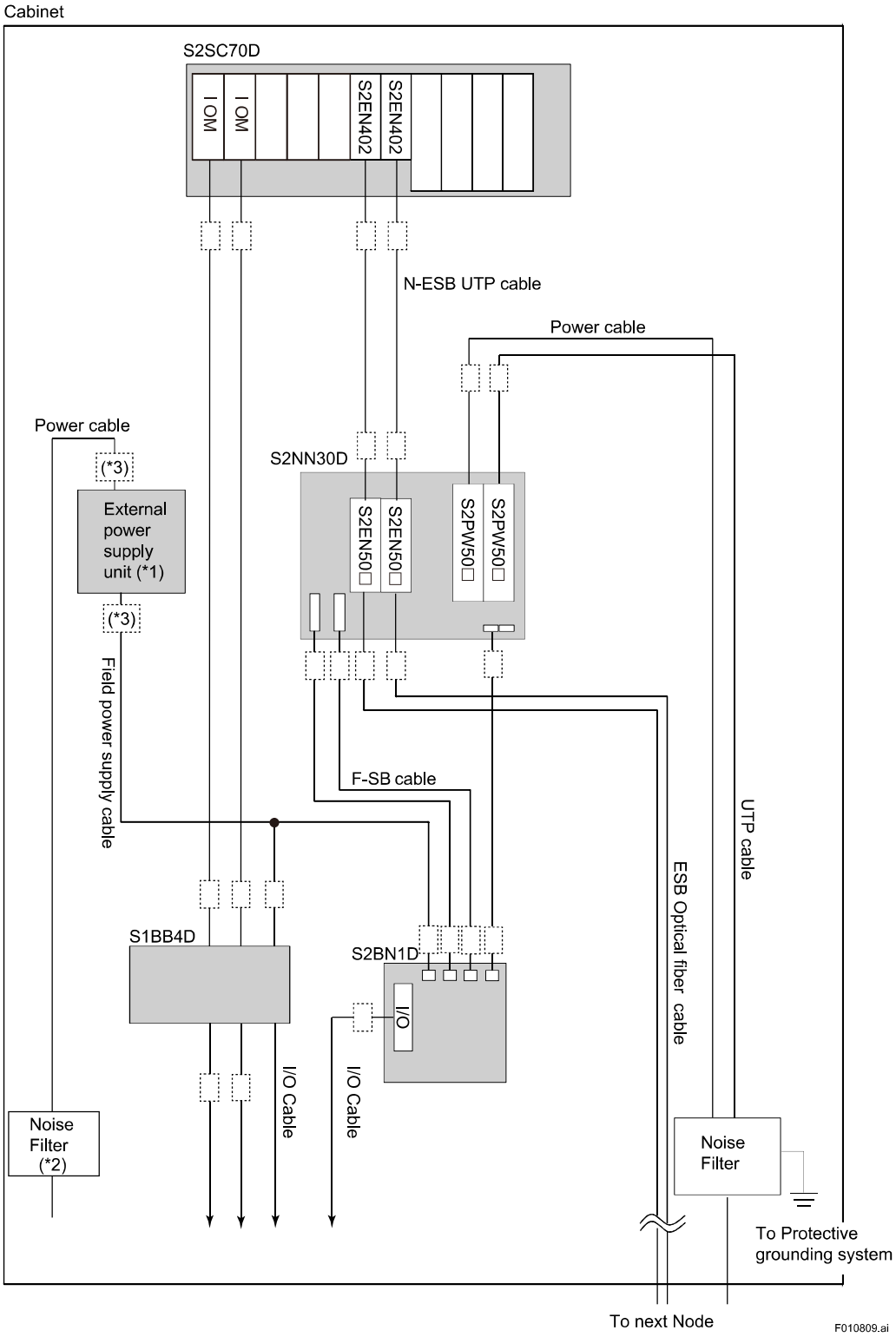
Figure Locations of Ferrite Core Installation for Input/Output Modules, Terminal Boards and Relay Boards



Note: Figures in ( ) show the locations listed in "Table Cables that Need Ferrite Cores to be Attached to, and Ferrite Core Models and Quantities". It is NOT a number of ferrite core.

F010805.ai

Figure Locations of Ferrite Core Installation for AVR10D



*1: The marine standard isn't acquired to use S2PW50□ by alone. Please don't use for field power supplies.
*2: This noise filter is for the external power supply unit. Regarding necessity of the noise filter, please follow directions on instructions for marine standards of this external power supply unit.
*3: This ferrite core is for the external power supply unit. Regarding necessity of the ferrite core, please follow directions on instructions for marine standards of this external power supply unit.
⋮⋮ : Ferrite core is not necessary for the mounting positions shown in the dotted line boxes.

Figure Location of Ferrite Core Installation for N-IO (S2NN30D, S2BN1D, and S1BB4D)

Location of Ferrite Cores for Cables

For the following cables, be careful about the locations at which you install ferrite cores:

Power-line cables:

Install ferrite cores on each cable at the nearest possible place to each connector.
In order to prevent the load at the connectors, secure the power-line cables to the cabinet frame or dummy plate using cable ties at the nearest possible place to each ferrite core.

ESB bus cables:

Install ferrite cores on each cable at the nearest possible place to each connector.
In order to prevent the load at the connectors, secure the ESB bus cables to the cabinet frame or dummy plate using cable ties at the nearest possible place to each ferrite core.

Vnet/IP cables:

Install ferrite cores on each cable at the nearest possible place to each connector.
In order to prevent the load at the connectors, secure the Vnet/IP cables to the cabinet frame or dummy plate using cable ties at the nearest possible place to each ferrite core.

Cables connected to analog input/output modules and digital input/output modules:

- Cables Connecting to terminal boards or relay boards
  Install ferrite cores on each cable at the nearest possible place to each connector.
  In order to prevent the load at the connectors, secure the cables to the cabinet frame or dummy plate using cable ties at the nearest possible place to each ferrite core.
- Vinyl insulated cables used with pressure clamp terminals
  Install ferrite cores for all cables. Refer to “Table Cables that Need Ferrite Cores to be Attached to, and Ferrite Core Models and Quantities” for the number of cores.
  It is possible to consolidate multiple cables as per the cable diameter if same ferrite cores are used for both plus (+) and minus (-) lines.

Signal cables connected to terminal boards or relay boards:

Install ferrite cores on each cable at the nearest possible place to each connector.
In order to prevent the load at the connectors, secure the cables to the cabinet frame or dummy plate using cable ties at the nearest possible place to each ferrite core.

Installing Unit Components in Cabinet

Unit components here indicate the S2SC70☐-F, SSC60☐-F, SSC50☐, SSC57☐ and SNB10D node units and SNT10D unit for optical bus repeater modules. When installing these unit components in a cabinet, dummy plates may have to be installed and a gasket may have to be attached to the dummy plates in the following cases:

- There is a large space between unit components.
- There is no space between unit components.
- Unit components are installed unevenly inside the cabinet.

When Leaving a Large Space between Unit Components

When leaving a large space between unit components, install the following dummy plates to board up the spaces. A UNIT equals 44.45 mm high. Depending on the location of the dummy plate, attach an EMI shielding gasket to the dummy plate.

Table Space Sizes and Part Numbers of Dummy Plates

Space Size (UNITs in Height)	Dummy Plate
1	T9082EX
2	T9933VF
3	T9082EY
6	T9082EZ

1 UNIT = 44.45 mm

Specification of EMI shielding gasket: Width 5 mm, Thickness 1 mm

Location to attach EMI shielding gasket:

Attach an EMI shielding gasket onto the bottom surface of the lower bend of a dummy plate as shown below. Where a unit component is installed immediately above a dummy plate, attach an EMI shielding gasket also onto the top surface of the upper bend of the plate. However, for the dummy plate installed at the bottom of the component mounting area, no EMI shielding gasket needs to be attached onto its lower bend.

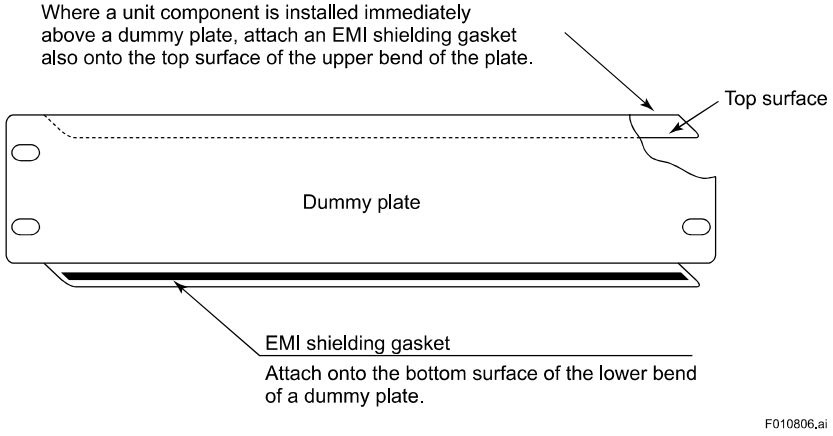


Figure Examples of Installing EMI Shielding Gasket to Dummy Plate

When Installing Unit Components with No Space between Them

When installing two unit components with no space between them, attach an EMI shielding gasket onto the bottom surface of the lower bend of the upper unit. However, for the unit installed at the bottom of the component mounting area, no EMI shielding gasket needs to be attached onto its lower bend.

For the EMI shielding gaskets, use the model introduced in the paragraph under “When Leaving a Large Space between Unit Components.”

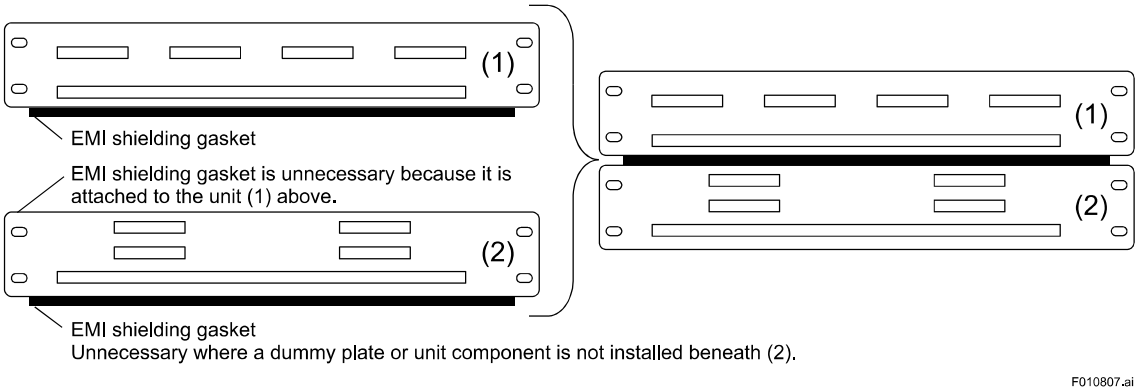


Figure Examples of Installing EMI Shielding Gasket to Unit Component

When Installing Unit Components Unevenly Inside Cabinet

When installing unit components unevenly and gathering them to the upper or lower part of a cabinet, leaving a large space in the cabinet, install dummy plates. Attach an EMI shielding gasket to the dummy plates.

For the EMI shielding gaskets, use the model introduced in the paragraph under “When Leaving a Large Space between Unit Components.”

SEE ALSO For how to attach EMI shielding gaskets, refer to “When Leaving a Large Space between Unit Components.”

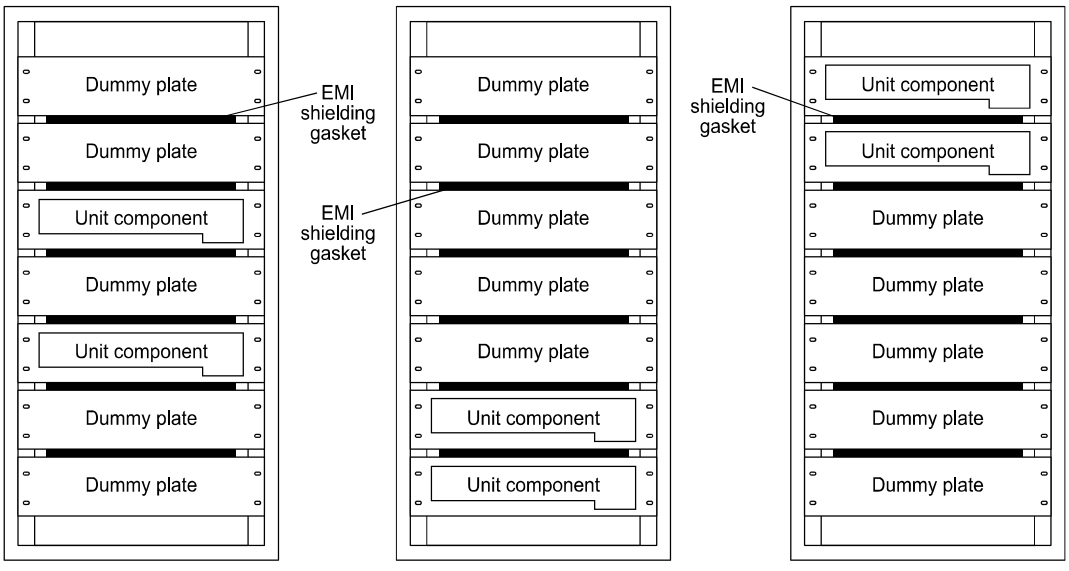


Figure Example of Installing Dummy Plates and EMI Shielding Gaskets in Cabinet

2. Transportation, Storage and Installation

This chapter describes the precautions in transporting, storing, and installing the ProSafe-RS system.

SEE ALSO See Section 1.2, “Control Room Environment” for the environmental requirement for each piece of equipment.

2.1 Precautions for Transportation

This section describes the precautions required to prevent accidents and damage when transporting ProSafe-RS system equipment. These precautions apply when the equipment is contained in our original packing.

Transportation

SEE ALSO For ambient temperature, humidity, vibration and impact, see Section 1.2, “Control Room Environment.”

Loading

- Do not load crates on top of others or turn them on their sides.
- Keep all crates upright.
- Secure loaded crates using ropes, and cover them completely with waterproof coverings.
- Do not load crates outdoors when it is raining.

Don’t Stack Outdoors

Be sure to store cargoes inside a warehouse if they must be stored for some time.

Transportation

Cargoes contain precision instruments. Select a company specializing in the transportation of computers and precision instruments.

Keep all products upright during air transport, freightage, or truck transport. When transporting by track, drive at low speed to avoid vibration and impact. Also, slow down to the limit on a bad road.

Others

Do not transport equipment through areas where there may be corrosive gas, intense electric or magnetic fields.

2.2 Unpacking

In unpacking the received cargoes and equipment, inspect them according to inspection list below. It is recommended to unpack by Yokogawa engineers or in their presence.

Table Inspection List

	Inspection Items	Result		Measures Required
Exterior	• Environment of unpacking location (temperature, humidity, dust)	Suitable	Unsuitable	If unsuitable, select proper location according to specified environmental requirements.
	• Rapid temperature fluctuation (should be within ±10 °C/h)	No	Yes	If yes, do not unpack and wait until the fluctuation remains within ± 10 °C/h.
	• Damage to equipment exterior	No	Yes	If damaged badly, inform Yokogawa.
	• Condensation or its trace on equipment exterior. (*1)	No	Yes	If yes, inform Yokogawa.
Interior	• Loose parts inside equipment.	No	Yes	If yes, remove them and check the surrounding.
	• Damage to equipment interior.	No	Yes	If damaged badly, inform Yokogawa.
	• Condensation or its trace on equipment interior. (*1)	No	Yes	If yes, inform Yokogawa.

*1: Condensation symptoms are as follows:
- Dew patterns on PCBs.
- Printed circuit copper trace is floating off the board.
- Label characters on PCBs are smudged.
- Connectors on PCBs are smudged.
- Dew patterns or traces of droplets are found on cabinet panels.

IMPORTANT

Condensation may cause a fatal system failure in the ProSafe-RS system. Be sure to unpack the equipment indoor under the specified environmental conditions. Strictly observe the allowable temperature fluctuation range of ±10 °C/h. Do not bring the equipment into a heated room straight from the outside in winter. Our warranty does not cover any damage caused by condensation.

2.3 Storage

The delivery date should be determined in accordance with your installation schedule. Avoid storing products more than three months. If long-term storage more than three months cannot be avoided, consult Yokogawa in advance because it is necessary to provide waterproofing, condensation prevention, and dustproofing measures as well as periodical inspections.

Storage Condition

Store products without unpacking. Be sure to confirm that the crate is not damaged. To store them after unpacking, be sure to take the precautions described below.

Location of Storage

Store products in a warehouse or indoor facilities - never in an open-air location.

Storage Environment

- Ambient Temperature for storage: 5 to 40 °C.
- Avoid direct sunlight.
- Prevent condensation.
- Do not store products where corrosive gas or salty air may be present.

SEE ALSO See “Section 1.2 Control Room Environment” for permissible temperature, humidity and temperature fluctuation of storage area.

Storage of Packed Equipment

- Place squared pieces of lumber with a height of 100 mm or higher on the floor. The lumber should be long enough so that more than 100 mm remains outside of the crate on every side.
- Securely place unopened crates on the lumber platform.
- Do not stack crates in piles.
- Make sure to provide good air circulation in the storage area and periodically inspect the crates to keep them under proper conditions.

Storage of Unpacked Equipment

To store unpacked products without power connection, follow the specified environmental requirements. If stored in a non-air-conditioned room, cover them with polyethylene or other sheets for protection against dust and moisture. For moisture-proofing, place a sufficient amount of Silica gel or other desiccating agent inside the covering and inspect its effectiveness from time to time.
When using desiccating agent or corrosion inhibitor etc., please select the appropriate one. Also, please make sure that it does not affect the function and performance of the product before actually using it.

2.4 Servicing Area

Take enough space around equipment for its operation and maintenance service. This servicing area is indicated for each equipment.

The servicing area should be considered in determining the size of installation location. When installing a number of equipment side by side, take the largest service - area between them if different dimensions are indicated for different side of equipment, as indicated below.

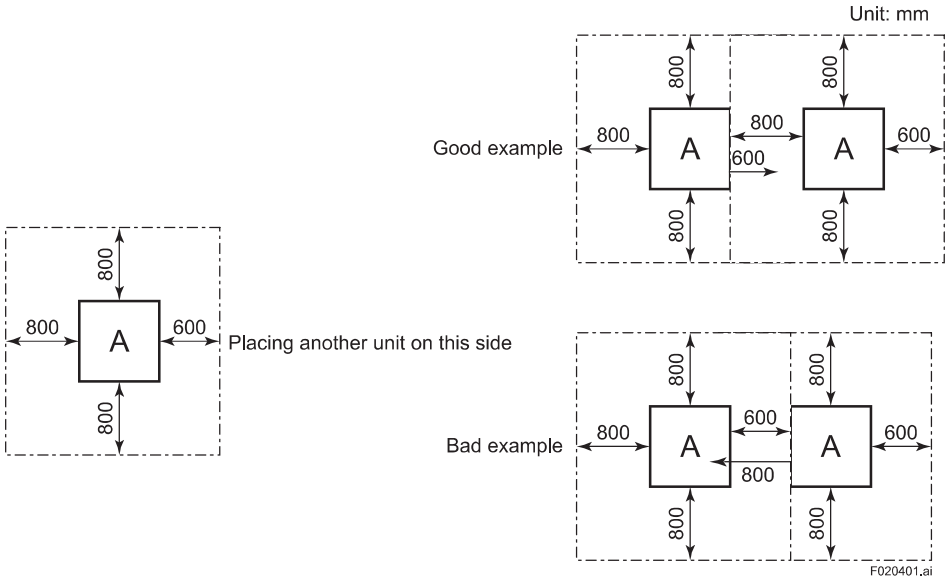


Figure Servicing Area when Installing Units Side-by-side

SEE ALSO For equipment servicing areas, refer to “External Dimensions” (SD).

2.5 Installation

Before installation, be sure that anchor bolts, pedestals, and cable holes are provided according to the customer's system configuration plans. Check that the positions of holes on the floor fit the anchor bolt holes in the channel base of each piece of equipment.

2.5.1 Installation on Floor

The installation method varies with the type of the floor and building.

- After unpacked, be careful not to put any impact until the equipment is fixed to the floor to prevent it from falling to the floor.
- Install devices as specified in the plans. Check the position of front and back panels of the cabinet.
  Avoid physical shock. Never use hammers.
- Fix each equipment to the floor.

The explanation below shows how to fix devices on different types of floors.

Concrete Floor

Clamp the equipment to the floor using anchor bolts. It is recommended to use M12 bolts and 3200 N•cm (320 kgf•cm) tightening torque.

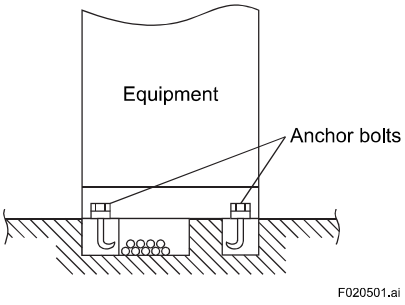


Figure Using Anchor Bolts

Steel Floor

Clamp the equipment to the floor using clamp bolts.

After cabling through the riser duct, fill the duct with rubber sponges and seal the top with putty.

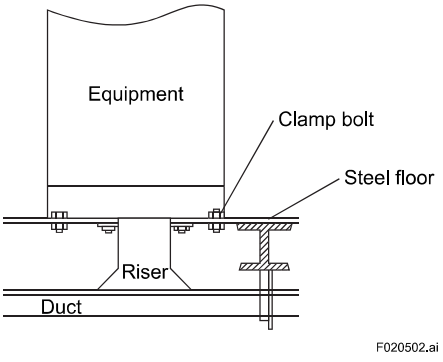


Figure Using Clamp Bolts

"Free-access" Floor

Clamp the equipment to pedestals that are anchored to the base floor.

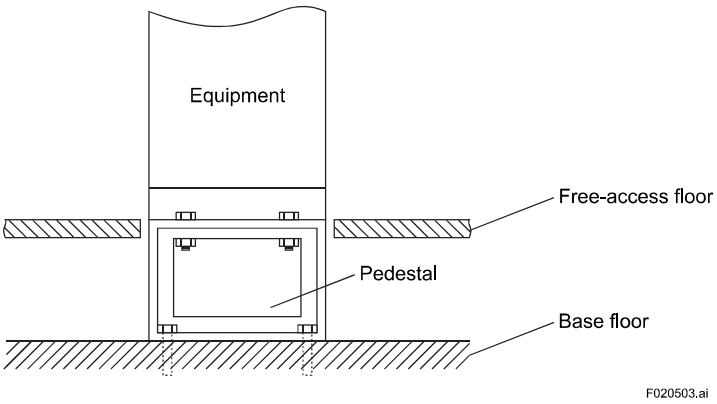


Figure Using Pedestal

In the "free-access" floor, make holes for riser cables to connect to each piece of equipment as follows:

- If one floor tile is removed, be sure to reinforce the opening with an angle frame for floor stability.

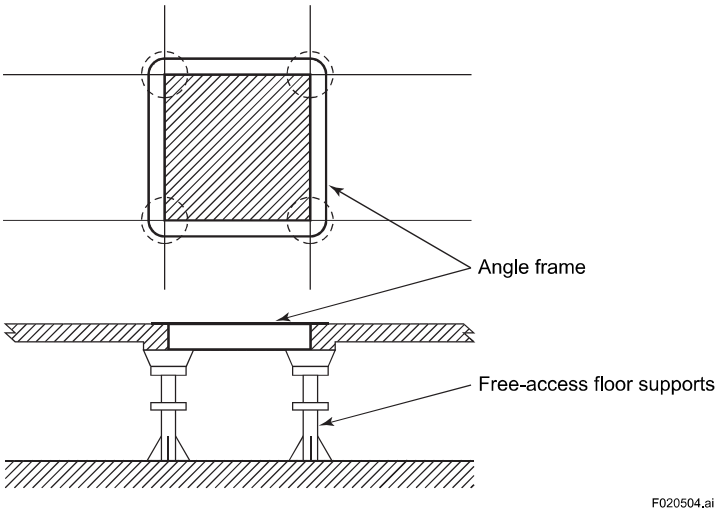


Figure Removing One Floor Tile

- Do not make a holes near the floor supports.
- Do not cut away more than 1/3 of a floor tile.

CAUTION

If a number of neighboring floor tiles are removed, be sure to provide angle frames or pedestals for reinforcement.

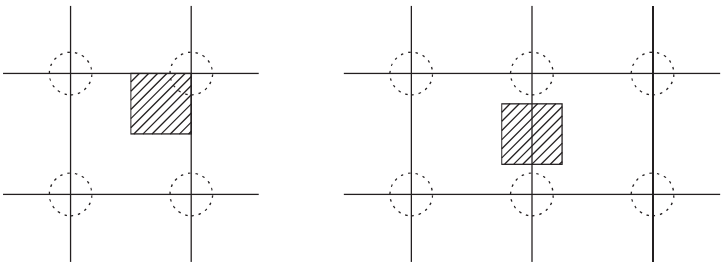


Figure Partially Cutting Floor Tile

Size of Cabling Holes in Floor

For ease of cabling, and for separating power cables from signal cables, it is recommended that you make holes in the floor for cabling that are the maximum size indicated in the floor plans. If the specified maximum size hole cannot be provided due to the floor construction or pit dimensions, the size may be smaller within the range indicated in the plans. If you use the specified minimum size of hole, use flexible cables that can bend inside the channel base.

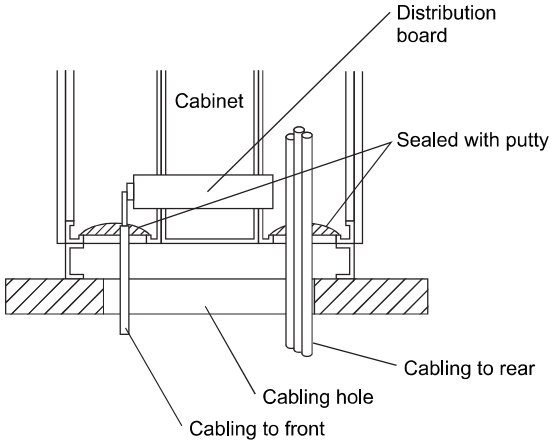


Figure Cabling through Maximum Size Hole

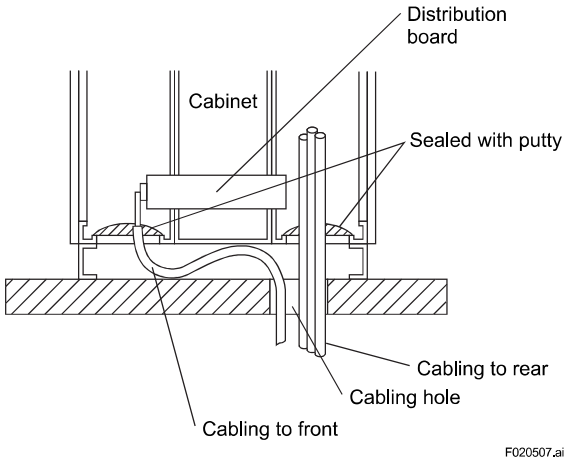


Figure Cabling through Minimum Size Hole

2.5.2 Rack Mounting

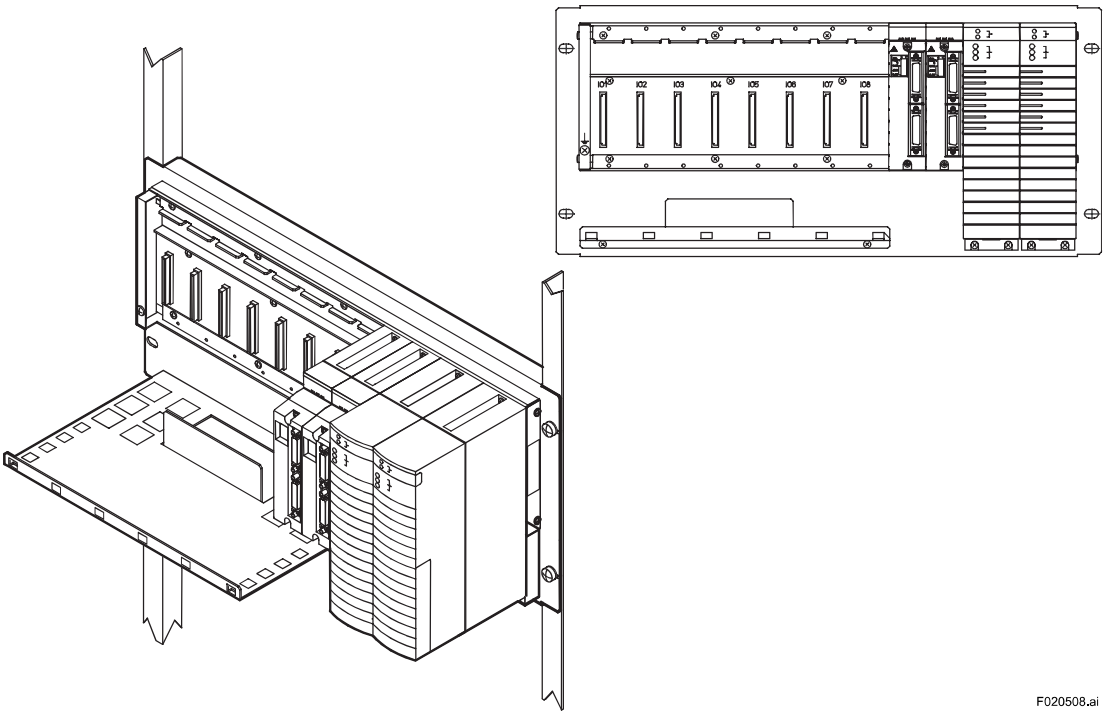
Rack-mount devices include:

SSC60S, SSC60D, SSC50S and SSC50D Safety Control Units (for Vnet/IP);
SSC57S and SSC57D Safety Control Unit (for Vnet/IP-Upstream)
S2SC70S and S2SC70D Safety Control Units;
SNB10D Safety Node Unit;
SNT10D Unit for Optical Bus Repeater Module;
SEA4D, SED2D, SED3D, SED4D and SWD2D Terminal Board;
SBA4D, SBD2D, SBD3D, and SBD4D Terminal Board (*1);
SRM53D and SRM54D Relay Board;
SBM54D Relay Board (*1);
AEPV7D Power Supply Bus Unit Vertical Type (*2)
AEP7D Primary Power Supply Bus Unit; and
AVR10D Duplexed V net router.

*1: DIN Rail Mount Type
*2: AEPV7D can not be installed to 19-inch Rack.

IMPORTANT

- To meet the Safety Standards and EMC Standards, the devices must be installed in a lockable metal cabinet. The cabinet must conform to IEC/EN/CSA 61010-2-201 or provide degrees of protection IP3X or above and IK09 or above.
- When installing rack mount devices on the same rack, keep 3-unit spacing (1 unit: 44.45 mm) under a safety control unit. Other units can be installed next to each other with specified condition.
  For more details, see “Providing Space for Heat Radiation”.



F020508.ai

Figure Mounting SNB10D Safety Node Unit

Notes on Installation

CAUTION

For safety during installation, secure an ample working space and work in a team. Be sure to observe the following when installing on a rack or on an instrumentation panel:

Insulation from Rack

The safety control unit or safety node unit or Unit for Optical Bus Repeater Module must be insulated from the rack using insulating bushing to prevent direct contact. Place the bushing on both sides of the plate, as shown in the figure below. Make sure that the rack-mounted equipment is electrically insulated from the rack. Insulating bushing is supplied as an accessory.

When you mount a device with insulating bushing to a rack, please do not leave it in an unstable condition where it is only hooked with loose screws. It may add unnecessary force to an insulating bushing to cause breakage.

Installation Procedure

1. Fasten a pair of insulating bushings together to each of the screw holes on the plate or the bracket on the device. The tapering end of the insulating bushings must come to the front side where a screw enters.
2. Using eight M5 screws to fix the device onto the rack or the panel.

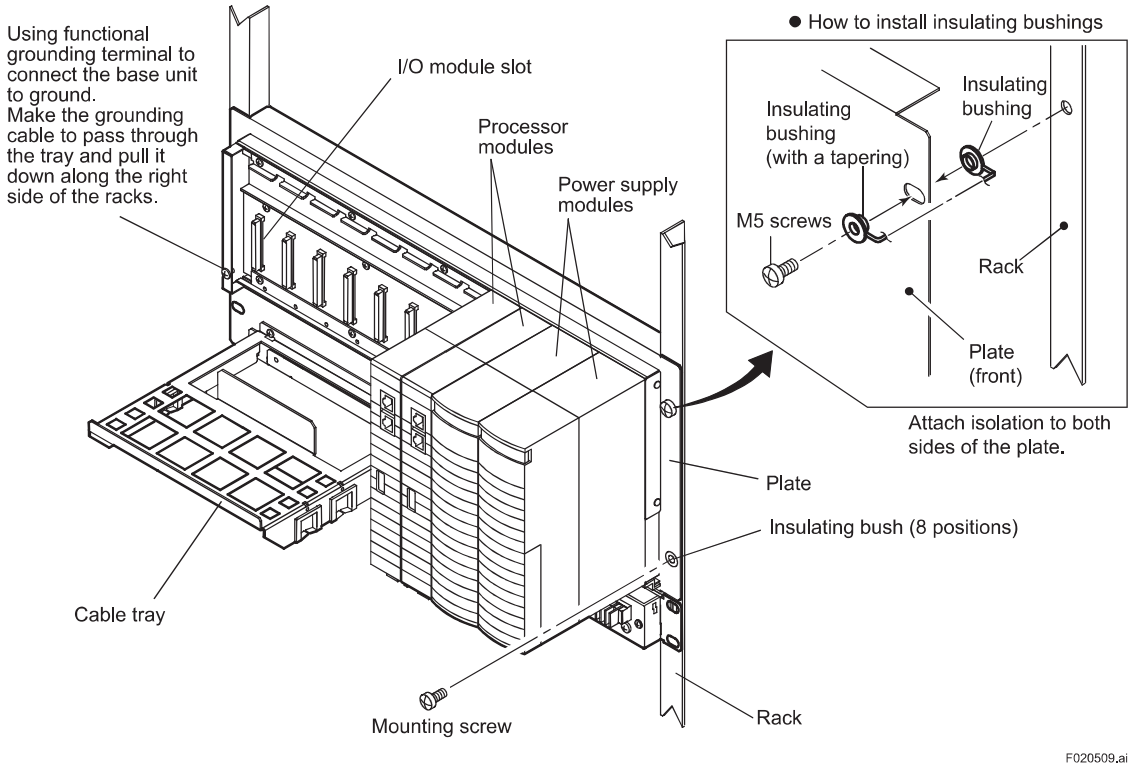


Figure Mounting SSC50D on Rack

IMPORTANT

The safety control unit or safety node unit or Unit for Optical Bus Repeater Module has no power supply switch. It is recommended that an external switch or breaker be provided to turn the power on and off.

CAUTION

If multiple node units are present, connect individual ground wires to terminals on the base units.

Installation Direction

Install the device in the rack with the screws in the vertically correct direction.

Check the installation direction by referring to SD (External Dimensions).

TIP

When the device is supplied with power even if it is temporary, the device must be installed on the rack.

Placing the device on a desk etc. and laying it on its side should be avoided.

The device may become malfunction if the heat radiated from the device cannot be cooled smoothly.

Providing Space for Heat Radiation

Leave space at the top and bottom of rack-mount equipment to permit heat radiation.

- Separate the top of the instrumentation board at least 100 mm away from the ceiling, and cut a ventilation hole of 200 cm2 or larger in the ceiling or install a ventilation fan.
- Keep at least 50 mm between the back of the equipment and the instrumentation panel or wall.
- When installing an 19-inch rack mount devices on the same rack, maintain a 3-unit spacing (1 unit: 44.45 mm) between devices. Above the installed devices, there are a number of openings for ventilation purposes on the trays.
- When putting cables on the trays, make sure that the openings are not blocked so as to ensure the airflow through the ventilation openings.

Providing Area for Servicing

When mounting devices in the 19-inch rack, the mounting plate cut out of instrumentation panel, and so on, leave an area for servicing.

Leave an area for servicing.

- All the work to connect cables to 19-inch rack mountable devices and I/O modules will be performed from the front.
- The work to confirm indicator lamps, configure card settings, and remove/insert cards will be performed from the front.
- The front is the area for wiring and servicing. Leave at least 1000 mm of space at the front.

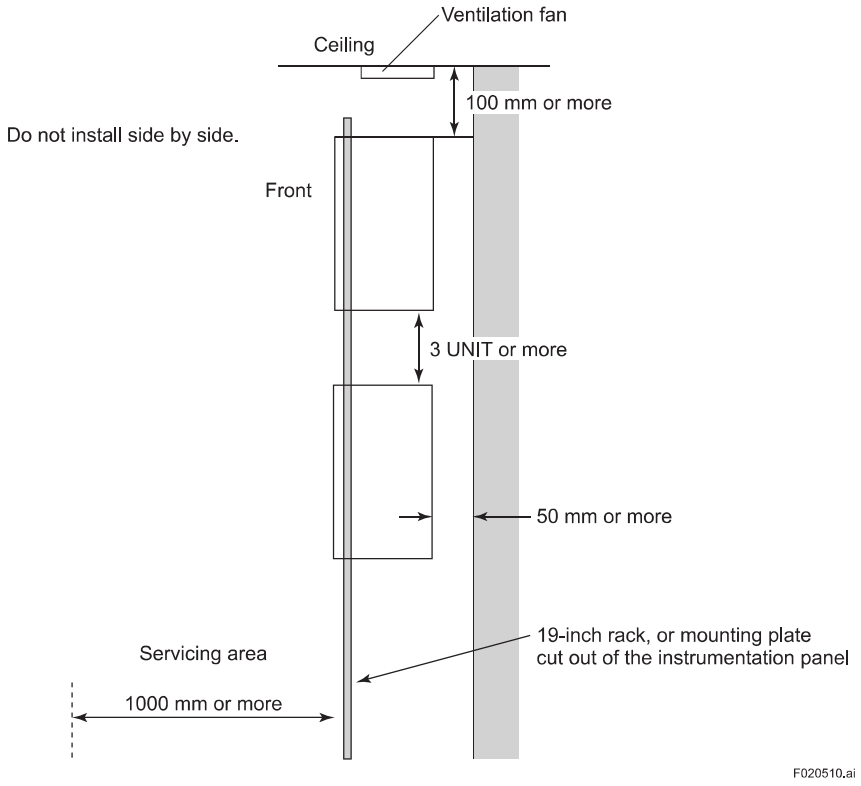


Figure Space Required for Rack-mount Equipment

2.5.3 DIN Rail Mountable Devices

The following devices can be mounted to a DIN rail.

Node interface unit: S2NN30D-□□□0□□□□□
Base plate with disconnecting terminal: S2BN1D-0□□□□
Terminal boards: SBA4D, S1BB4D, SBT4D, SBR4D, SBD2D, SBD3D, SBD4D, A2BM4
Relay boards: SBM54D
Universal conversion board: S1XEU4D

IMPORTANT

Install a DIN rail mountable device inside a metal cabinet.

To meet the Safety Standards and EMC Standards, the devices must be installed in a lockable metal cabinet.

The cabinet must conform to IEC/EN/CSA 61010-2-201 or provide degrees of protection IP3X or above and IK09 or above.

Notes on Installation

CAUTION

For installation, secure ample working space and work in a team for safety.

Providing Space for Heat Dissipation

Leave space at the top and bottom of the device to permit heat dissipation.

- Separate the top of the instrumentation board at least 100 mm away from the ceiling, and cut a ventilation hole of 200 cm2 or larger in the ceiling or install a ventilation fan.
- Do not block the openings (ventilation holes) in the top and bottom surfaces of the device.
- A 1-unit (44.45 mm) or more space shall be provided between the Node Interface Unit and other base plates.

Providing Area for Servicing

Leave an area for servicing.

- All the work to connect cables to DIN rail mountable devices and I/O modules will beperformed from the front.
- The work to confirm indicator lamps, configure card settings, and remove/insert cards will be performed from the front.
- The front is the area for wiring and servicing. Leave at least 1000 mm of space at the front.

Compatible DIN Rail

Table Compatible DIN Rail Symbols (DIN 60715, JIS C 2812, IEC 60715, EN50022)

Cross section shape type symbol	Width - height symbols	Material (chemical symbol)
TH	35-7.5	Fe or Al

Installation of DIN Rail

- Install a DIN rail in a metal mounting plate with screws at 120-mm or less intervals.
- When mounting a DIN rail mountable device to a DIN rail, confirm that the device is securely fixed after the mounting.
- A DIN rail for S2BN1D must be electrically insulated from a cabinet using insulating bushing.

Mounting Space

S2NN30D and S2BN1D require spaces, as shown below, to slide in to the positions when mounting to the DIN rail. Refer to the General Specifications (GS) for the external dimensions.

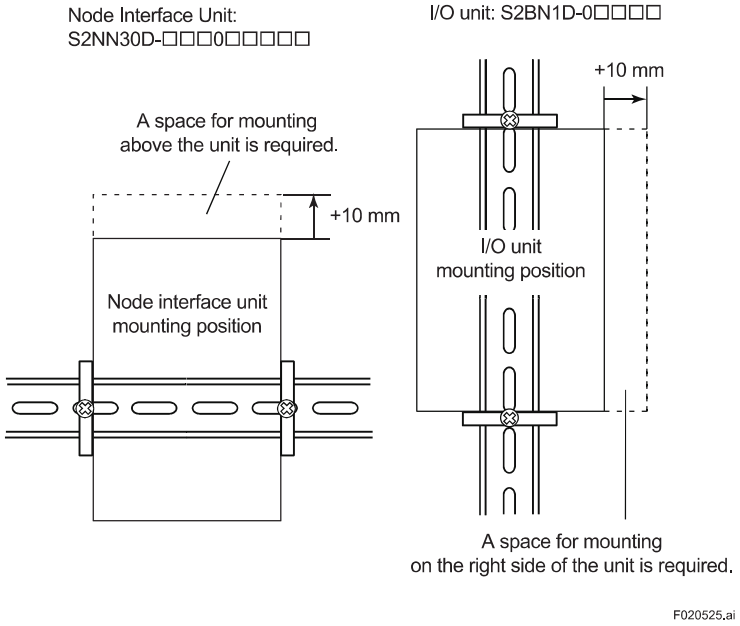


Figure Mounting Space (Front View)

Grounding

Be sure to ground the equipment using the ground terminal of the base plate. Even if there is electrical conduction between the base plate and wall surface via the mounting mechanism, the equipment must be grounded using the functional ground terminal.

Mounting

- When mounting S2BN1D I/O Units vertically on the DIN rail, insert stoppers on top and bottom of each unit. When those I/O units are mounted close by, only one stopper in between two I/O units will do. Another stopper is required for the I/O unit mounted on the top shelf.
- When mounting the units horizontally on the DIN rail, insert stoppers on both sides of the unit.

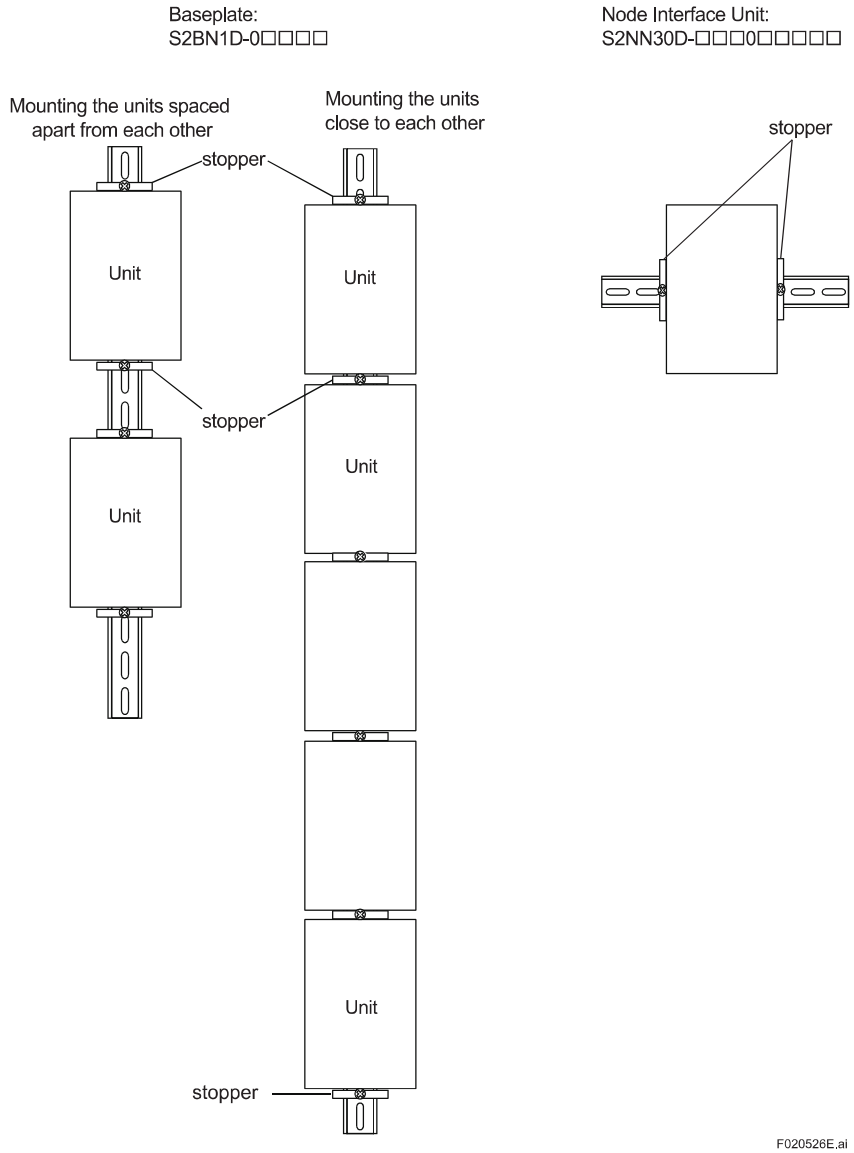


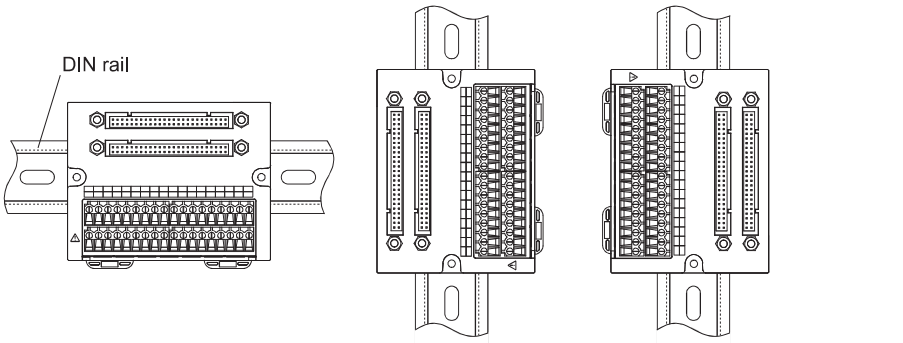
Figure Mounting stopper to the DIN rail

Terminal Board and Relay Board Mounting Directions

Mount a terminal board and a relay board in the directions as shown in the below figure.

When mounting SBD2D in the direction of b or c, the following conditions must be met.

- When the ambient temperature is 60 °C or lower, the total load current of the SBD2D must be kept within the specified value of 8 A or lower.
- When the ambient temperature is at 70 °C, the total load current must be 6 A or lower.
- In case the ambient temperature is in between 60 and 70 °C, reduce the total load current from 8 A maximum by the rate of 0.2 A/°C.



Remarks for Installating to a DIN Rail

On the back of DIN rail mountable terminal board, there are two bumps (projections) for fixing screws on the wall. Be sure not to let mechanical interference happen between these bumps and screw tops from the DIN rail. The height of the shaded areas in the below figures must be kept as 2.5 mm or shorter than the DIN rail surface.

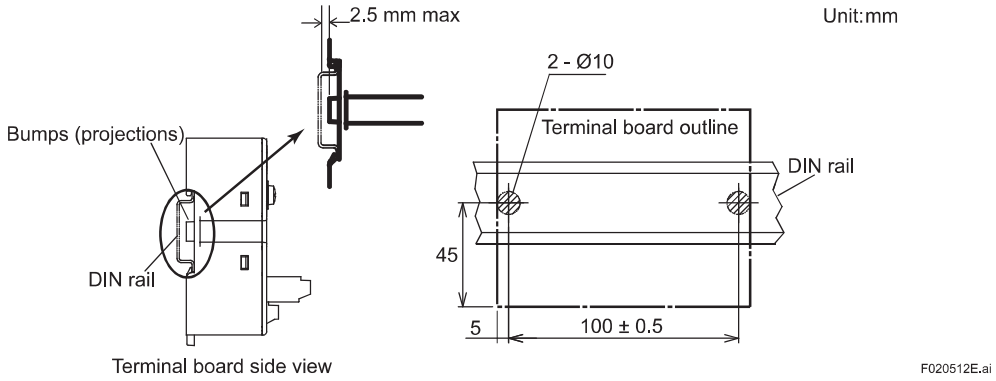


Figure Mounting SBA4D to DIN rail for terminal board

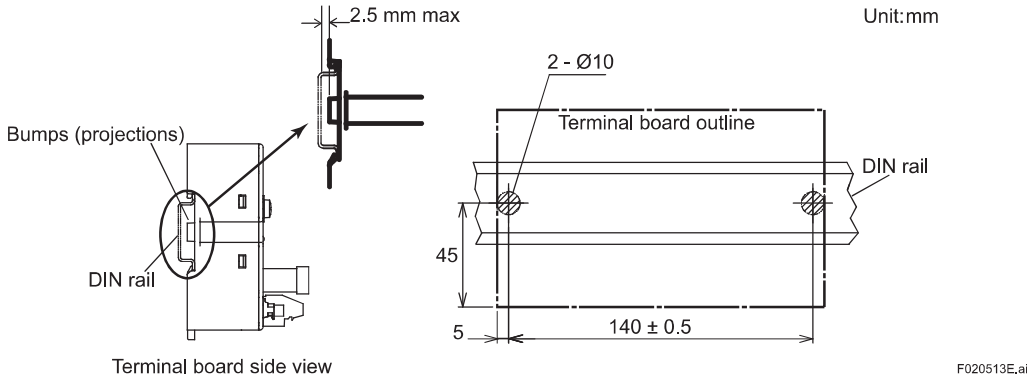


Figure Mounting A2BM4, SBD2D, SBD3D, and SBD4D to DIN rail for terminal board

Cautions of the Power Source for the Loads of SBM54D

In the case of using multiple power sources for the loads of SBM54D, there are cautions of the load voltage.

When the load voltage is different between loads.

All of the load voltages must be in either the range below.

- Load voltages ≤ 100 V
- 50 V < Load voltages ≤ 150 V

Cautions of the Digital Output Module when SBM54D is Used

The functions of disconnection diagnosis, ON pulse diagnosis and OFF pulse diagnosis for SDV541 must be disabled when SBM54D is used.

2.5.4 Wall Mountable Devices

The following devices can be mounted to a wall with screws.

Node interface unit:	S2NN30D-□□□□1□□□□
Base plate with disconnecting terminal:	S2BN1D-1□□□□
Barrier base plate:	S2BN4D-1□□□□
	S2BN5D-1□□□□
Terminal board:	A2BM4

IMPORTANT

Install a wall mountable device inside a metal cabinet.

To meet the Safety Standards and EMC Standards, the devices must be installed in a lockable metal cabinet.

The cabinet must conform to IEC/EN/CSA 61010-2-201 or provide degrees of protection IP3X or above and IK09 or above.

DIN rail specifications:

Notes on Installation

Providing Space for Mounting

S2BN4D need to be slide when this is mounted to a wall. For this reason, provide a space shown in the following figure. Refer to the General Specifications (GS 32P06P10-01EN) for the external dimensions.

Unit: S2BN4D-1□□□□

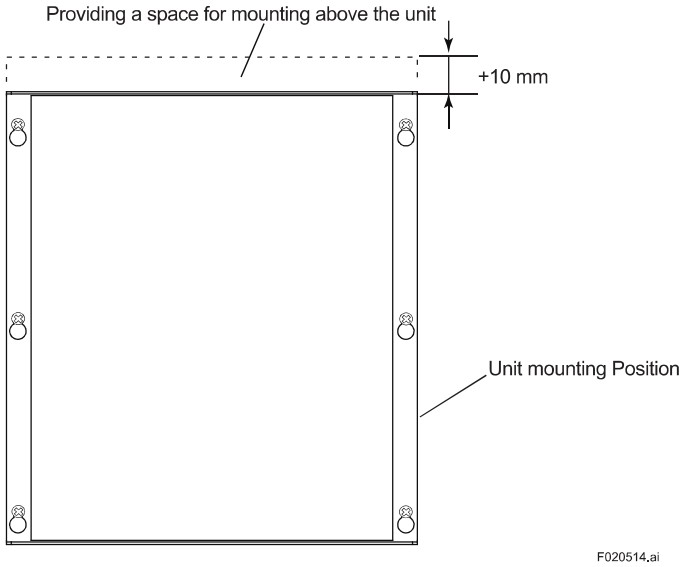


Figure Providing a Space for Mounting (Front View)

Providing Space for Heat Dissipation

Leave space to permit heat dissipation just as for a DIN rail mountable device.

Providing Area for Servicing

Leave an area for servicing just as for a DIN rail mountable device.

Grounding

Be sure to ground the equipment using the functional ground terminal provided on the base plate.

Mounting of Base Plate

- Mount a wall mountable device to a metal mounting plate using screws.
- To ground the S2BN4D at a single point, the back plate of S2BN4D must be insulated from mounting plate.

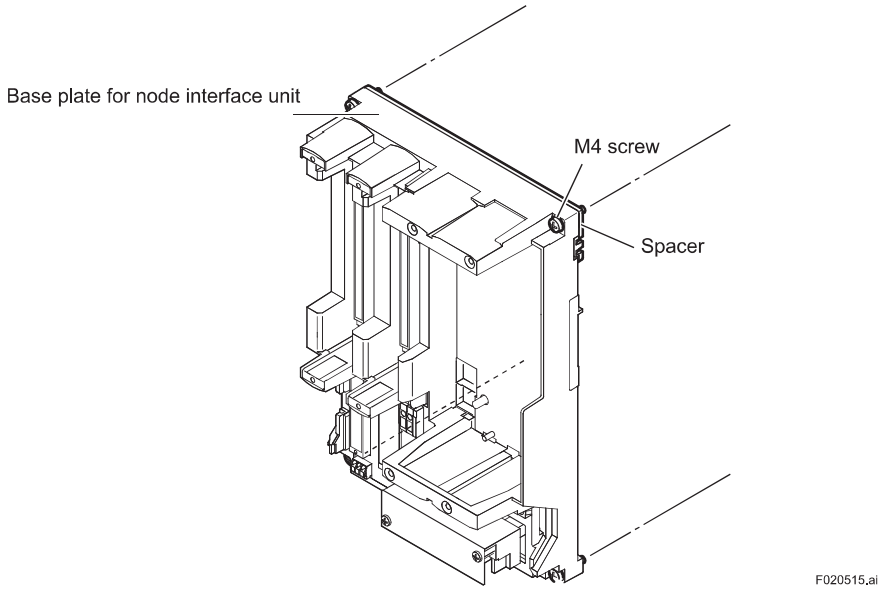


Figure Example of Mounting Node Interface Unit to Wall

Table Screw and Washer for Wall Mounting

Model	Screw diameter	Screw length	Washer Type/Washer Outer diameter	Tightening Torque (N•m)
S2NN30D	M4	Accessory (Retainer screw)		0.8 to 1.0
S2BN1D	M4	Accessory (Retainer screw)		0.8 to 1.0
S2BN4D (*1)	M4	— (*2)	Plane washer / 9 mm or smaller	1.2
S2BN5D	M4	16 mm or longer	(When the washer is not used)	1.2
		18 mm or longer	Plane washer / 8 mm or smaller	

*1: A back plate of S2BN4D is connected to functional grounding terminal. In order to ground at a single point, insulate the back plate from mounting plate using insulated supporter.
*2: The screw length depend on an insulated supporter specification. The screw length is decided using the thickness of the S2BN4D back plate (1.6 mm) and a washer.

SEE ALSO For the screw mounting dimensions for wall mounting, refer to the General Specifications (GS) for the corresponding device.

Remarks for Mounting on a Wall Surface

The following figure shows the screw installation dimensions for a wall mountable terminal board. Installation screws for the terminal board are not supplied and should be purchased separately. You need two installation screws. If you are using binding heads, use M4 screws with a length of at least 10 mm. If you are using screws with washers, use M4 screws with a length of at least 12 mm. The screw tightening torque is approximately 0.8 N·m.

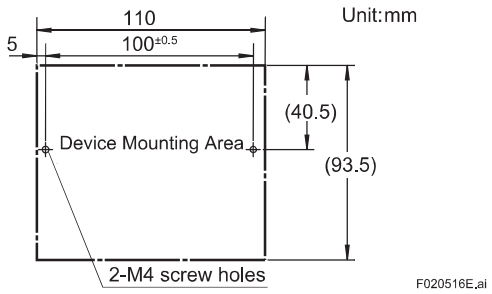


Figure Screw Installation Dimensions for the A2BM4, SBA4D, SBT4D, and SBR4D

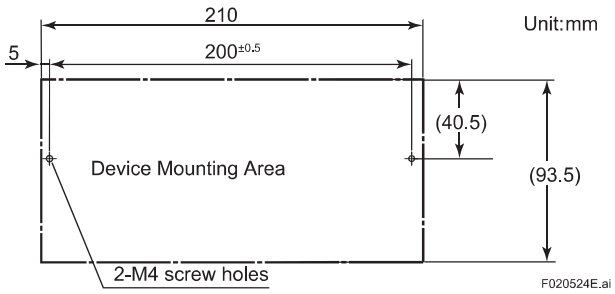


Figure Screw Installation Dimensions for the S1BB4D

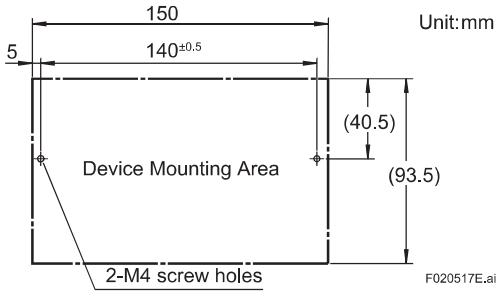


Figure Screw Installation Dimensions for the SBD2D, SBD3D, and SBD4D

Grounding

Ground the equipment at a single point using the functional ground terminal provided on the base plate.

Installation Direction

Mount the device to the wall with the screws in the vertically correct direction. Check the installation direction in General Specifications (GS).

2.5.5 Installation Guideline for Cabinet (FIO)

Installation Guideline for Rittal Cabinet (Up to 11 Nodes)

The following shows examples and notes for installing a safety control unit and up to 10 safety node units in the Rittal TS8 cabinet.

Applicable Cabinet

Rittal TS8 cabinet (W: 800 mm D: 800 mm H: 2000 mm)

Temperature Conditions

- If a safety control unit is equipped with a fan unit, the ambient temperature of the cabinet must be 50°C or lower. If it is not equipped with a fan unit, the ambient temperature of the cabinet must be 30°C or lower.
- Ambient temperature of the safety control unit and safety node units in the cabinet must satisfy the temperature values specified in GS (General Specifications).

Installation Conditions

- Applicable units
  Safety Control Unit S2SC70☐/SSC60☐/SSC50☐/SSC57☐: 1 unit
  Safety Node Unit SNB10D and Unit for Optical ESB Bus Repeater Module SNT10D: Up to 10 units
  Primary Power Supply Bus Unit AEP7D and AEPV7D: Up to 2 units
  Other heat-generating devices must not be installed in the cabinet.
- Fan configuration
  Configuration of door fans, node fans, and roof vent

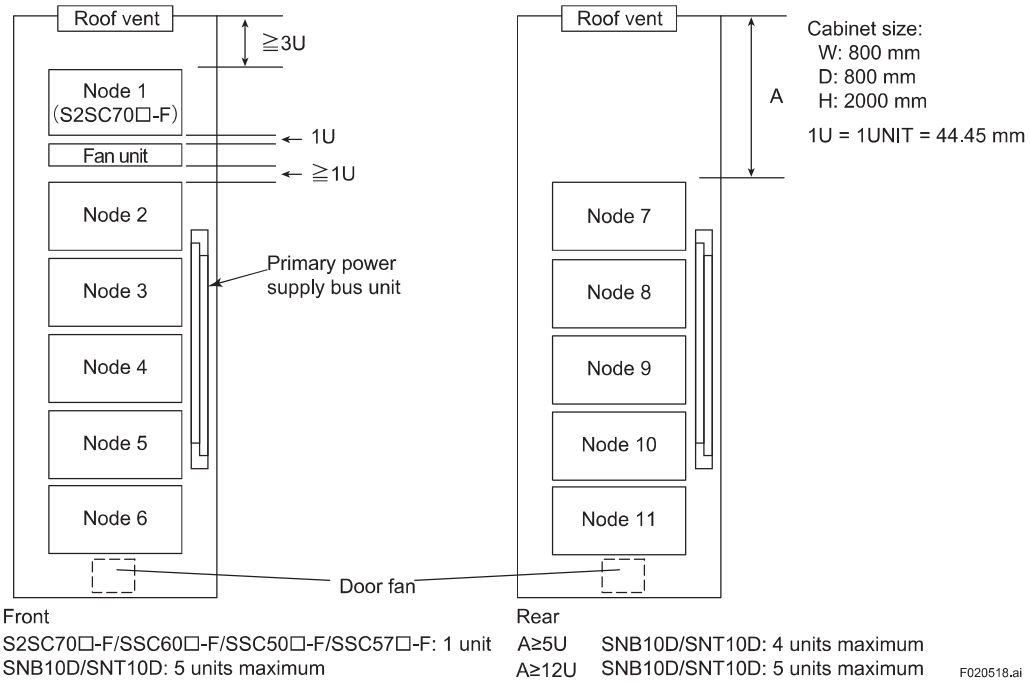


Figure Installation of S2SC70☐/SSC60☐/SSC50☐/SSC57☐ for Rittal cabinet (with Fan Unit)

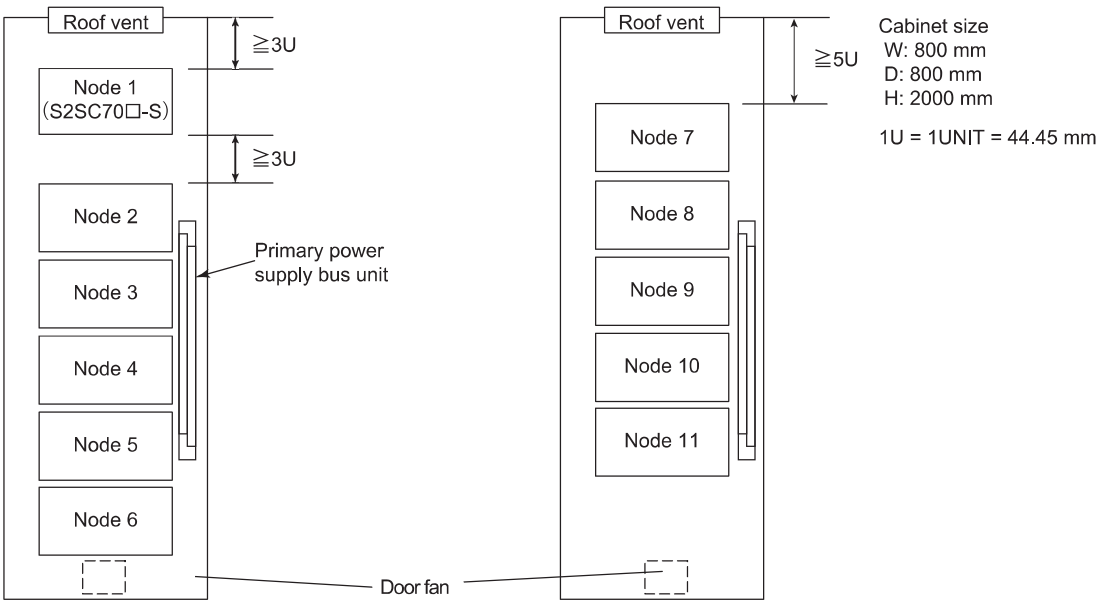


Figure Installation of S2SC70☐/SSC60☐/SSC50☐/SSC57☐ for Rittal cabinet (without Fan Unit)

- Fan specifications
  Door fan (on one side): Maximum air flow rate 230 m^3/h or more
  The roof vent must be larger than the opening area of the door fan.
- I/O module installation restrictions
  Refer to and follow the installation restrictions specified in "■ NODE UNIT MOUNTING RESTRICTIONS" in the "ProSafe-RS Outline of I/O Modules" (GS 32Q06K20-31E).

■ Installation Guideline for Rittal Cabinet (Up to 14 Nodes)

The following shows examples and notes for installing a safety control unit and up to 13 safety node units in the Rittal TS8 cabinet. If the units are installed under the following conditions, the temperature rise in the cabinet compared to the ambient temperature of the cabinet is 10°C or lower.

● Applicable Cabinet

Rittal TS8 cabinet (W: 800 mm D: 800 mm H: 2000 mm)

● Temperature Conditions

- Ambient temperature of the cabinet must be 50°C or lower.
- Ambient temperature of the safety control unit and safety node units in the cabinet must satisfy the temperature values specified in GS (General Specifications).

Installation Conditions

- Applicable units
  Safety Control Unit S2SC70□-F/SSC60□-F: 1 unit
  Safety Node Unit SNB10D and Unit for Optical ESB Bus Repeater Module SNT10D: Up to 13 units
  Primary Power Supply Bus Unit AEP7D and AEPV7D: Up to 2 units
  Other heat-generating devices must not be installed in the cabinet.

- Fan configuration
  There are the following two types of fan configurations.
  Type 1: Configuration of door fans, node fans, and door vents
  Type 2: Configuration of door fans, node fans, and roof vent

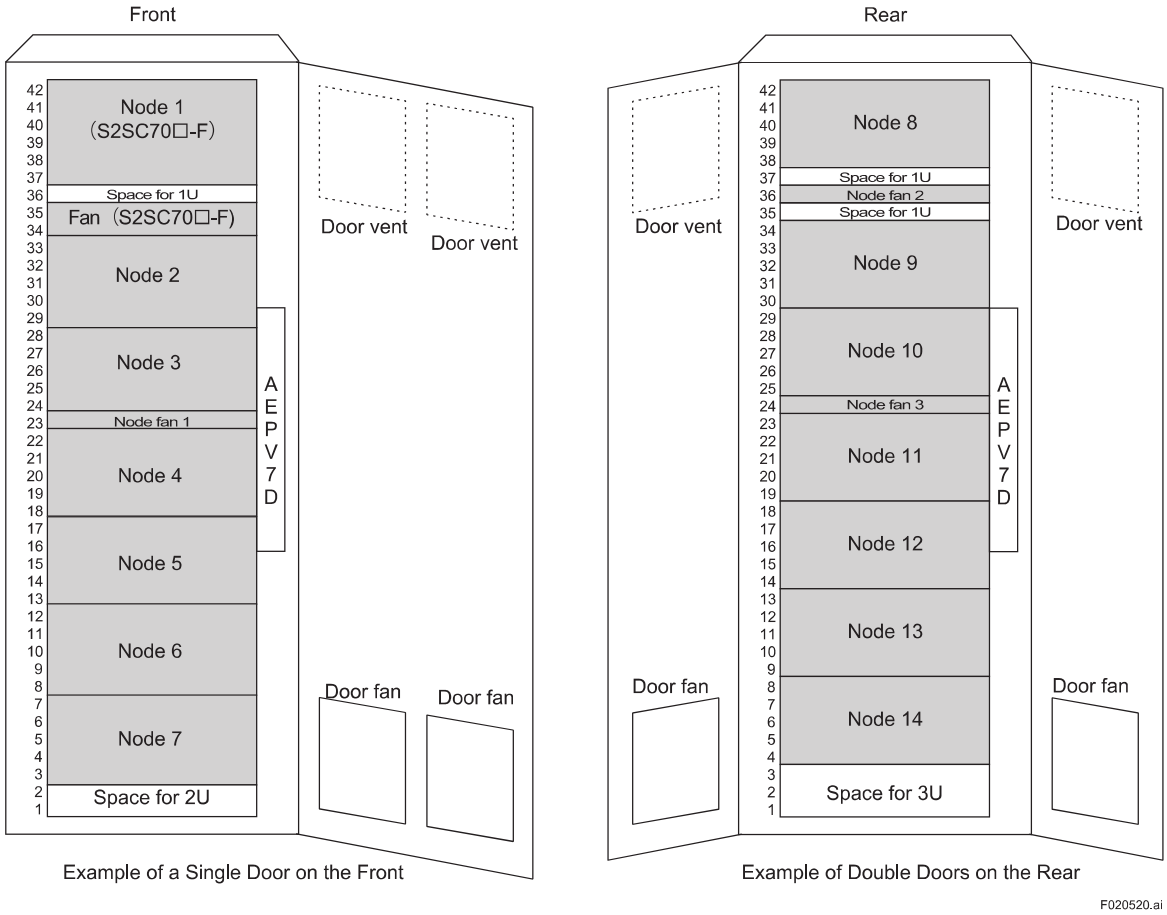


Figure Fan Configuration of Type 1 and Installation Positions in the Cabinet

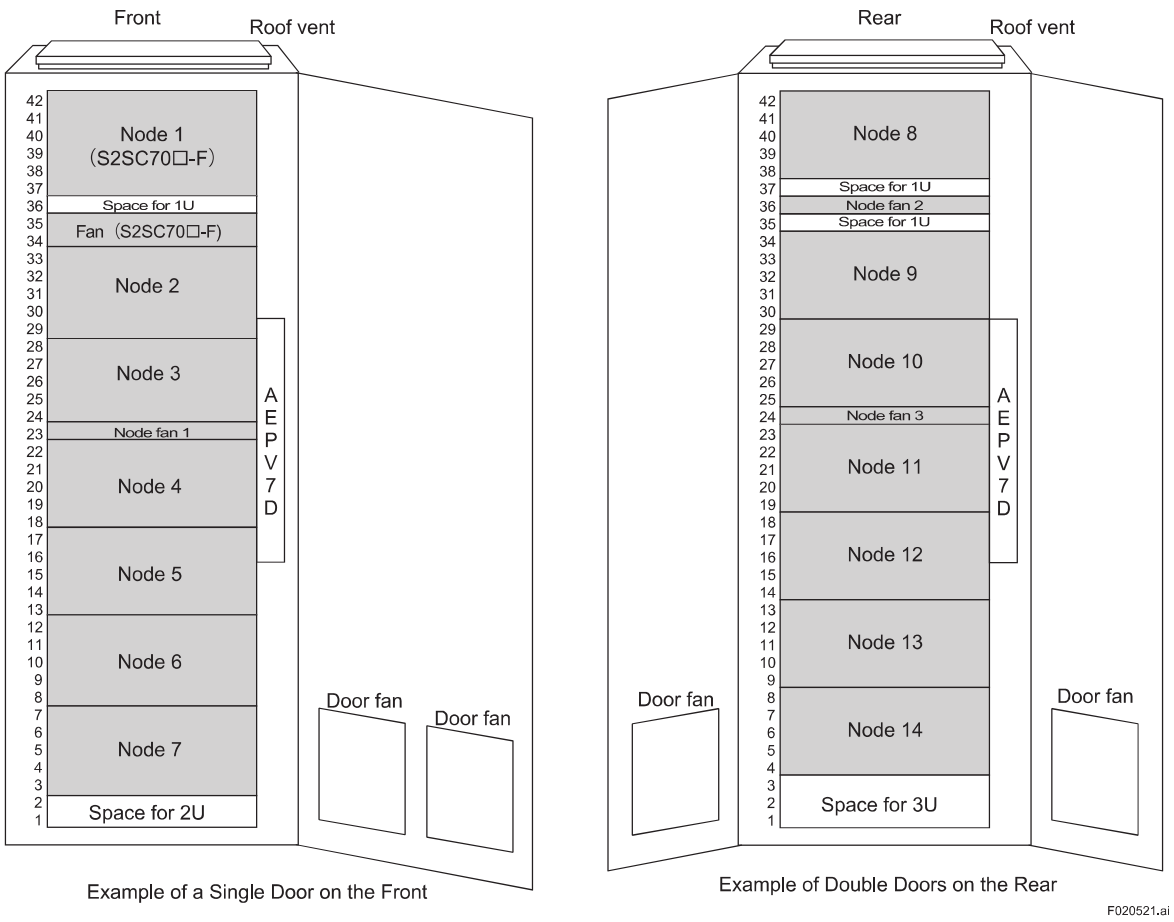


Figure Fan Configuration of Type 2 and Installation Positions in the Cabinet

The required number of node fans varies depending on the number of nodes to be installed.

Table Number of Nodes to Be Installed and Need to Install Fans

	Location No. (*1)	7 units on one side	6 units on one side	5 units on one side	4 units on one side
Front	37-42	Node 1 (S2SC70□-F)	Node 1 (S2SC70□-F)	Node 1 (S2SC70□-F)	Node 1 (S2SC70□-F)
	34-35	Fan (S2SC70□-F)	Fan (S2SC70□-F)	Fan (S2SC70□-F)	Fan (S2SC70□-F)
	29-33	Node 2	Node 2	Node 2	Node 2
	24-28	Node 3	Node 3	Node 3	Node 3
	23	Node Fan 1	Node Fan 1	—	—
	18-22	Node 4	Node 4	Node 4	Node 4
	13-17	Node 5	Node 5	Node 5	—
	8-12	Node 6	Node 6	—	—
	3-7	Node 7	—	—	—
Rear	38-42	Node 8	Node 8	Node 8	Node 8
	36	Node Fan 3	Node Fan 2	Node Fan 2	—
	30-34	Node 9	Node 9	Node 9	Node 9
	25-29	Node 10	Node 10	Node 10	Node 10
	24	Node Fan 3	Node Fan 3	—	—
	19-23	Node 11	Node 11	Node11	Node 11
	14-18	Node 12	Node 12	Node 12	—
	9-13	Node 13	Node 13	—	—
	4-8	Node 14	—	—	—

—: Not installed
*1: Location numbers correspond to the installation positions in the figure above.

- Fan specifications
  Door fan (on one side): Maximum air flow rate 210 m^3/h or more
  Node fan: Maximum air flow rate 480 m^3/h or more
  The door vent and roof vent must be larger than the opening area of the door fan.
- I/O module installation restrictions
  Refer to and follow the installation restrictions specified in “■ NODE UNIT MOUNTING RESTRICTIONS” in the “ProSafe-RS Outline of I/O Modules” (GS 32Q06K20-31E).
- Detecting a fan failure
  It is recommended to monitor the rotation of the fans or the temperature in the cabinet to detect a fan failure.

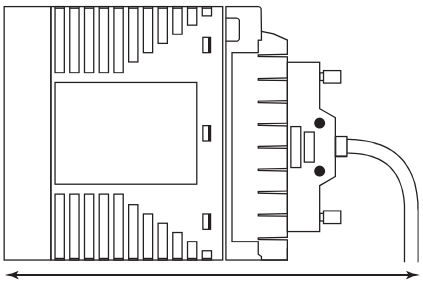
Notes on Installation

Depth of Cabinet

The following table shows the depth from the blunt curb of the signal cable to the edge of the rack, when the signal cable is connected with the I/O module in a cabinet.

Table Depth of cabinet

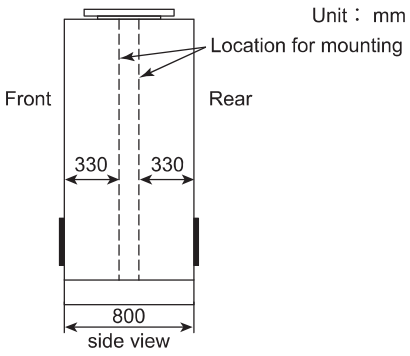
I/O Module	Depth from the cable blunt curb to the edge of the rack (mm)
SDV144	230
SDV521	290
SDV526	250
SDV531	230
SDV53A	260
SDV541	230



Depth from the blunt curb of the signal cable to the edge of the rack

F020522.ai

Location



F020523.ai

2.5.6 Installation Guideline for Cabinet (N-IO)

Installation Guideline for Rittal cabinet for N-IO

This section describes examples of the maximum number of N-IO system equipment (except for equipment for RIO System Upgrade) installed in general-purpose cabinets.

The following shows the common specifications to the examples of cabinets for N-IO system that are explained later.

Cabinet Specifications

The following cabinet is assumed to be used.

Table Cabinet Dimensions

W	D	H	Material	Product example
800 mm	800 mm	2000 mm (+100 mm) (*1)	Metal	Rittal TS8808 series

*1: 100 mm is the height of the channel base.

Table Specifications of a cabinet ambient temperature and an air supply / air exhaust port (In case N-IO SCU is included in a cabinet.)

Cabinet ambient temperature	Air supply port	Air flow	Area of an air supply/ air exhaust port (Panel cut of a cabinet)	Product example	Remarks
40 ºC or less	Fan	Door fan 230 m^3/h or more	Air supply port 60000 mm^2 or more Air exhaust port 60000 mm^2 or more	Rittal SK3239 series (Fan)	• Be sure to mount two push-fit door fans on each side in case of a failure. • The air flow and the area in the left show the total value on each side.

Table Specifications of a cabinet ambient temperature and an air supply / air exhaust port (In case only N-IO nodes (Non-Intrinsic Safety Barrier) are included in a cabinet.)

Cabinet ambient temperature	Air supply port	Air flow	Area of an air supply/ air exhaust port (Panel cut of a cabinet)	Product example	Remarks
50 ºC or less	Fan	Door fan 40 m^3/h or more	Air supply port 16000 mm^2 or more Air exhaust port 60000 mm^2 or more	Rittal SK3237 series (Fan)	• It is recommended to mount two push-fit door fans on each side in case of a failure. • The air flow and the area in the left show the total value on each side.
40 ºC or less	Outlet filter	- (*1)	Air supply port 60000 mm^2 or more Air exhaust port 60000 mm^2 or more	Rittal SK3239.200 (Outlet filter)	• Be sure to mount two outlet filters on each side in case of a failure such as filter clogging.

*1: When not mounting a fan, be sure to secure a ventilation path in the cabinet.

Table Specifications of a cabinet ambient temperature and an air supply / air exhaust port (In case only N-IO nodes (Intrinsic Safety Barrier) are included in a cabinet.)

Cabinet ambient temperature	Air supply port	Air flow	Area of an air supply/ air exhaust port (Panel cut of a cabinet)	Product example	Remarks
50 ºC or less	Fan	Door fan 230 m^3/h or more	Air supply port 60000 mm^2 or more Air exhaust port 60000 mm^2 or more	Rittal SK3239 series (Fan)	• Be sure to mount two or more push-fit door fans on each side in case of a failure. • The air flow and the area in the left show the total value on each side.

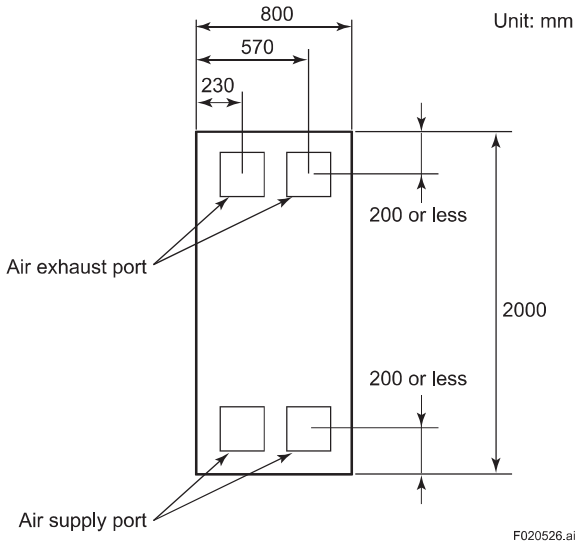
Notes

The following shows the common notes to the examples.

- The ventilation for each modules shall not be blocked.
- The mounting plate for mounting the IOBP shall be made of metal, regardless of whether DIN rail or panel mounting.
- A DIN rail shall be made of metal.
- For mounting restrictions other than the above, refer to the General Specifications (GS).

Position of an air supply / air exhaust port

In this mounting example, arrange an air supply / air exhaust port as follows.



Note: This is the dimension from the end face of the cabinet. (Not the dimension from the end face of the cabinet door.)

Figure Position of an air supply/ air exhaust port

Conventions

The following shows the common abbreviations used and their explanations.

Abbreviations	Explanations
SCU	Safety Control Unit
NIU	Node Interface Unit (for N-IO)
IOBP	I/O Base Plate
IOBP_IS	I/O Base Plate for Intrinsic Safety explosion protection
NIO node	Consists of NIU and IOBP/IOBP_IS.
Unit	Unit of 19 inch rack. 1 Unit = 44.45 mm
Side	One of the front and the back of a cabinet. (e.g., side, one side)

Example of Mounting Multiple SCUs for N-IO in a Cabinet

Temperature conditions

In this example, the ambient temperature is assumed to be the following.

Cabinet ambient temperature	40 °C or less

Maximum numbers of units that can be mounted

Type	Model	Number of units that can be mounted per side
SCU	S2SC70D S2SC70S (Except for S2SC70□-S)	Up to 4

Heat-generating devices other than the above shall not be mounted in the cabinet.

Mounting conditions

- SCU shall be mounted with a 3-unit or more space from the top-shelf mounting position of the cabinet.
- A 1-unit or more space shall be provided between the fan unit of a SCU and the SCU on the bottom shelf.
- Devices that block the convective air flow from the fan unit of a SCU or door fans to each module shall not be mounted.

The following shows how to mount multiple SCUs for N-IO in a cabinet:

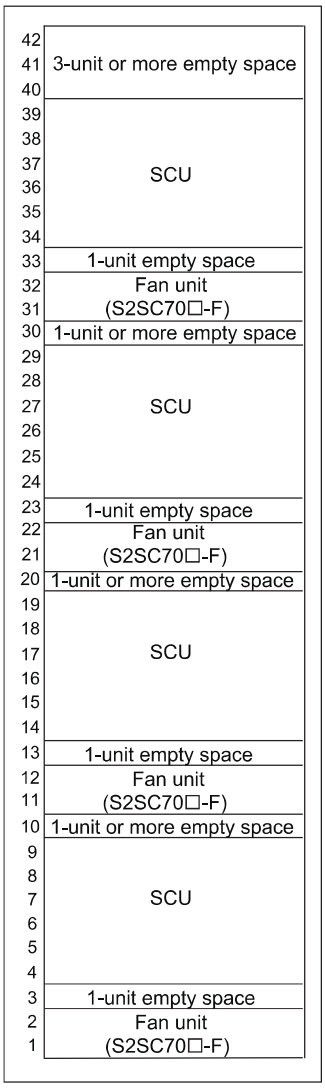


Figure Example of Mounting Multiple SCUs for N-IO in a Cabinet

Example of Mounting an SCU for N-IO and N-IO Nodes in a Cabinet

Temperature conditions

In this example, the ambient temperature is assumed to be the following.

Cabinet ambient temperature	40 °C or less

Maximum numbers of units that can be mounted in case of this example

Type	Model	Number of units that can be mounted per side
SCU	S2SC70S/S2SC70D (Except for S2SC70□-S)	Up to 1
NIU	S2NN30D	Up to 1
IOBP	S2BN1D	Up to 6 (2 rows × 3 shelves)

Heat-generating devices other than the above shall not be mounted in the cabinet.

Mounting conditions

- The SCU on the top shelf shall be mounted with a 100-mm or more space from the cabinet ceiling.
- A 1-unit (= 44.45 mm) or more space shall be provided between NIU and IOBP.
- A circulation fan unit shall be mounted on the shelf below the SCU with a 1-unit space. A 1-unit or more space shall be provided under the circulation fan unit.
- Suitable length of signal cables and power cables should be used.

The following shows how to mount an SCU for N-IO and N-IO nodes in a cabinet:

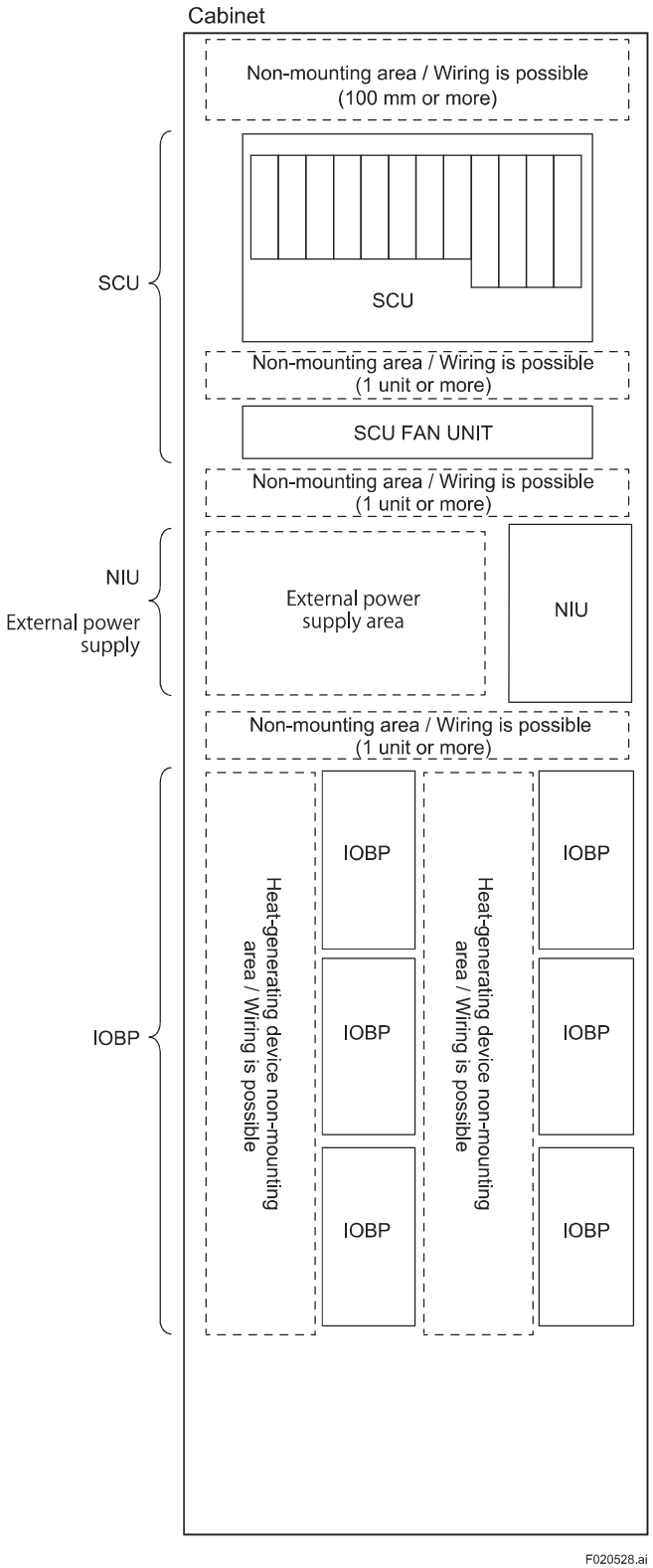


Figure Example of Mounting an SCU for N-IO and N-IO Nodes in a Cabinet

Example of Mounting an SCU for N-IO and N-IO Nodes in a Cabinet (In case of field wiring via terminal board)

Temperature conditions

In this example, the ambient temperature is assumed to be the following.

Cabinet ambient temperature	40 °C or less

Maximum numbers of units that can be mounted in case of this example

Type	Model	Number of units that can be mounted per side
SCU	S2SC70S/S2SC70D (Except for S2SC70□-S)	Up to 1
NIU	S2NN30D	Up to 2
IOBP	S2BN1D	Up to 12 (3 rows × 4 shelves)

Mounting conditions

- The SCU on the top shelf shall be mounted with a 100-mm or more space from the cabinet ceiling.
- A 1-unit (= 44.45 mm) or more space shall be provided between NIU and IOBP.
- A circulation fan unit shall be mounted on the shelf below the SCU with a 1-unit space.

  A 1-unit or more space shall be provided under the circulation fan unit.
- Suitable length of signal cables and power cables should be used.

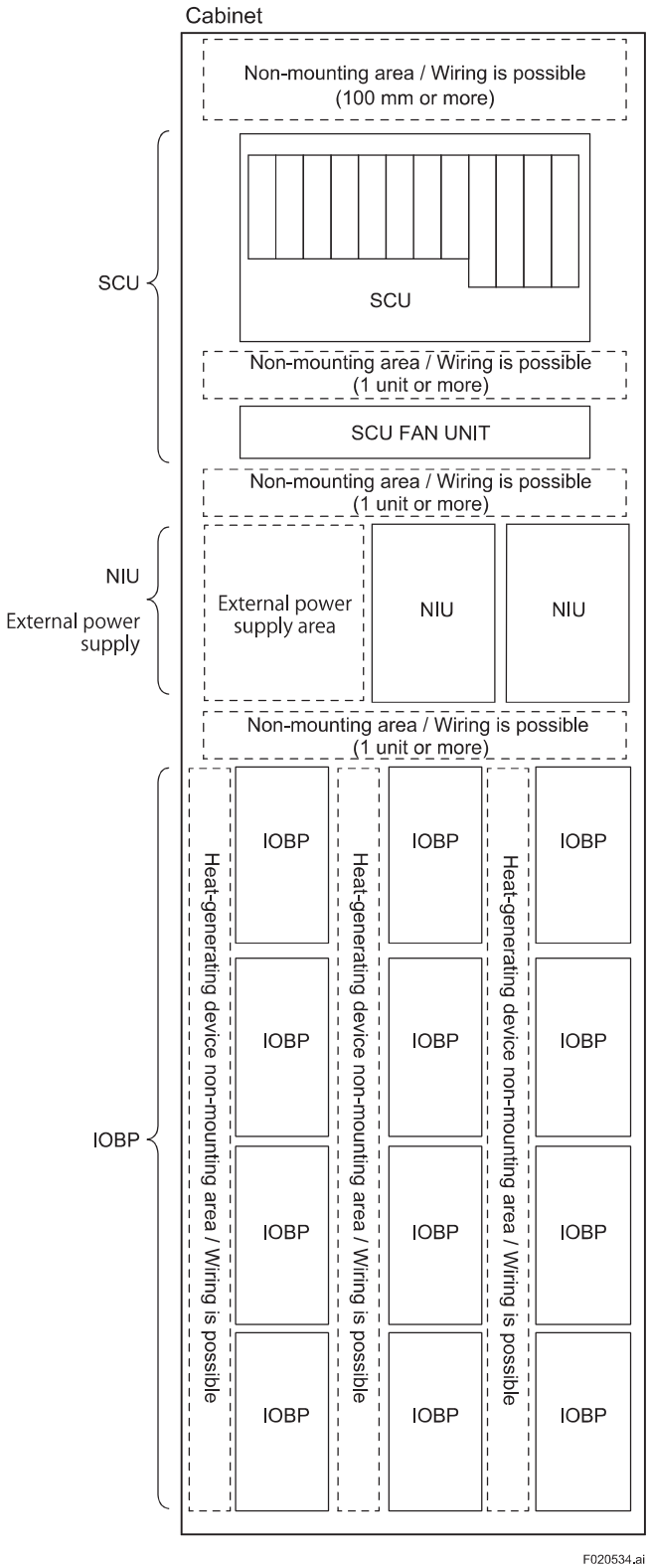


Figure Example of Mounting an SCU for N-IO and N-IO Nodes in a Cabinet (IOBP×3 columns mounted)

Example of Mounting N-IO Nodes (Non-Intrinsic Safety Barrier) in a Cabinet

Temperature conditions

In this example, the ambient temperature is assumed to be the followings.

Cabinet ambient temperature	50 °C or less

Maximum numbers of units that can be mounted in case of this example

Type	Model	Number of units that can be mounted per side
NIU	S2NN30D	Up to 2
IOBP	S2BN1D	Up to 10 (2 rows × 5 shelves)

Heat-generating devices other than the above shall not be mounted in the cabinet.

Mounting conditions

- The NIU shall be mounted with a 100-mm or more space from the cabinet ceiling.
- A 1-unit (= 44.45 mm) or more space shall be provided between NIU and IOBP.
- Suitable length of signal cables and power cables should be used.

The following shows how to mount N-IO nodes (Non-Intrinsic Safety barrier) in a cabinet:

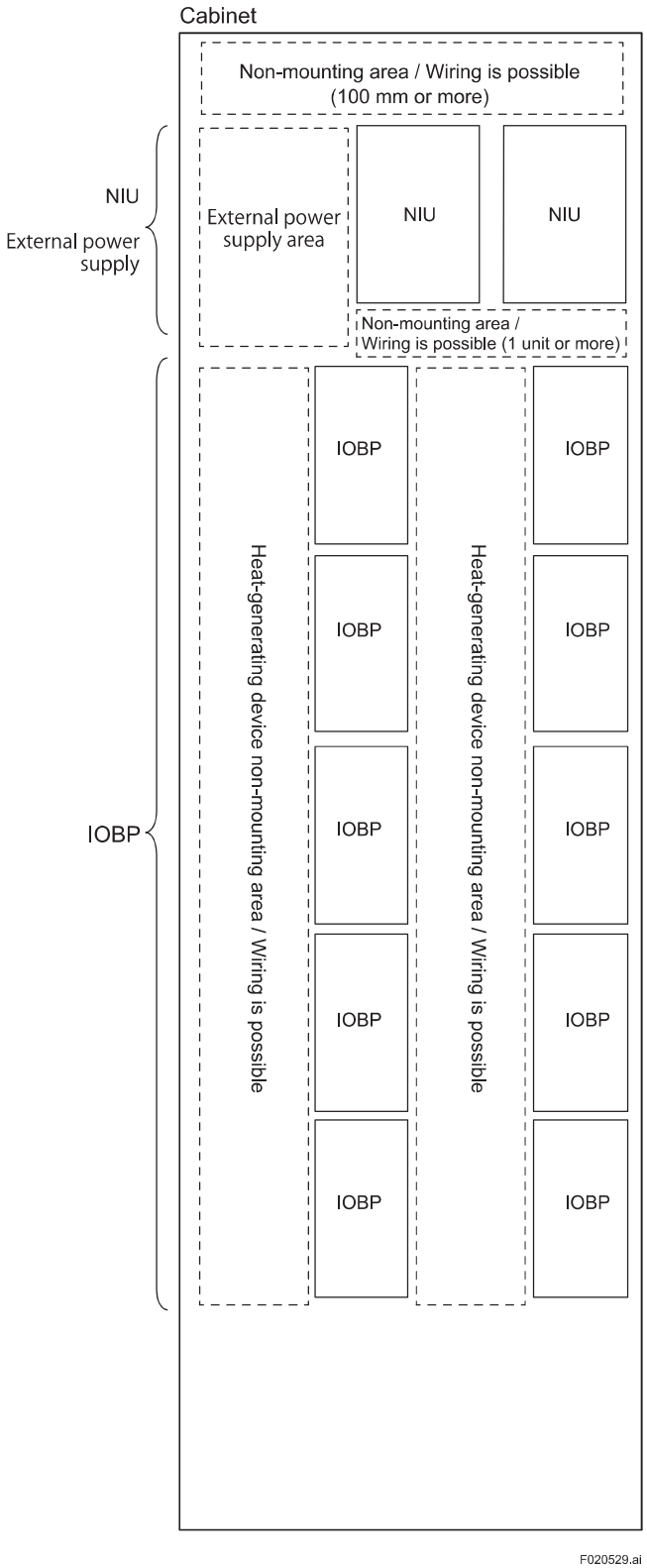


Figure Example of Mounting N-IO Nodes (Non-Intrinsic Safety barrier) in a Cabinet

Example of Mounting N-IO Nodes (Non-Intrinsic Safety Barrier) in a Cabinet (In case of field wiring via terminal board)

Temperature conditions

In this example, the ambient temperature is assumed to be the following.

Cabinet ambient temperature	50 °C or less

Maximum numbers of units that can be mounted in case of this example

Mounting surface of cabinet	Type	Model	Number of units that can be mounted per side
Mounting surface of external power supply	NIU	S2NN30D	Up to 3
	IOBP	S2BN1D	Up to 15 (3 rows x 5 shelves)
Non-mounting surface of external power supply	NIU	S2NN30D	Up to 3
	IOBP	S2BN1D	Up to 18 (3 rows x 6 shelves)

Mounting conditions

- The NIU shall be mounted with a 100-mm or more space from the cabinet ceiling.
- A 1-unit (=44.45 mm) or more space shall be provided between NIU and IOBP.
- When using a DIN rail, be sure to install a DIN rail on the mounting plate. Fixing at the both ends of a DIN rail and not fixing at the middle.
- Suitable length of signal cables and power cables should be used.

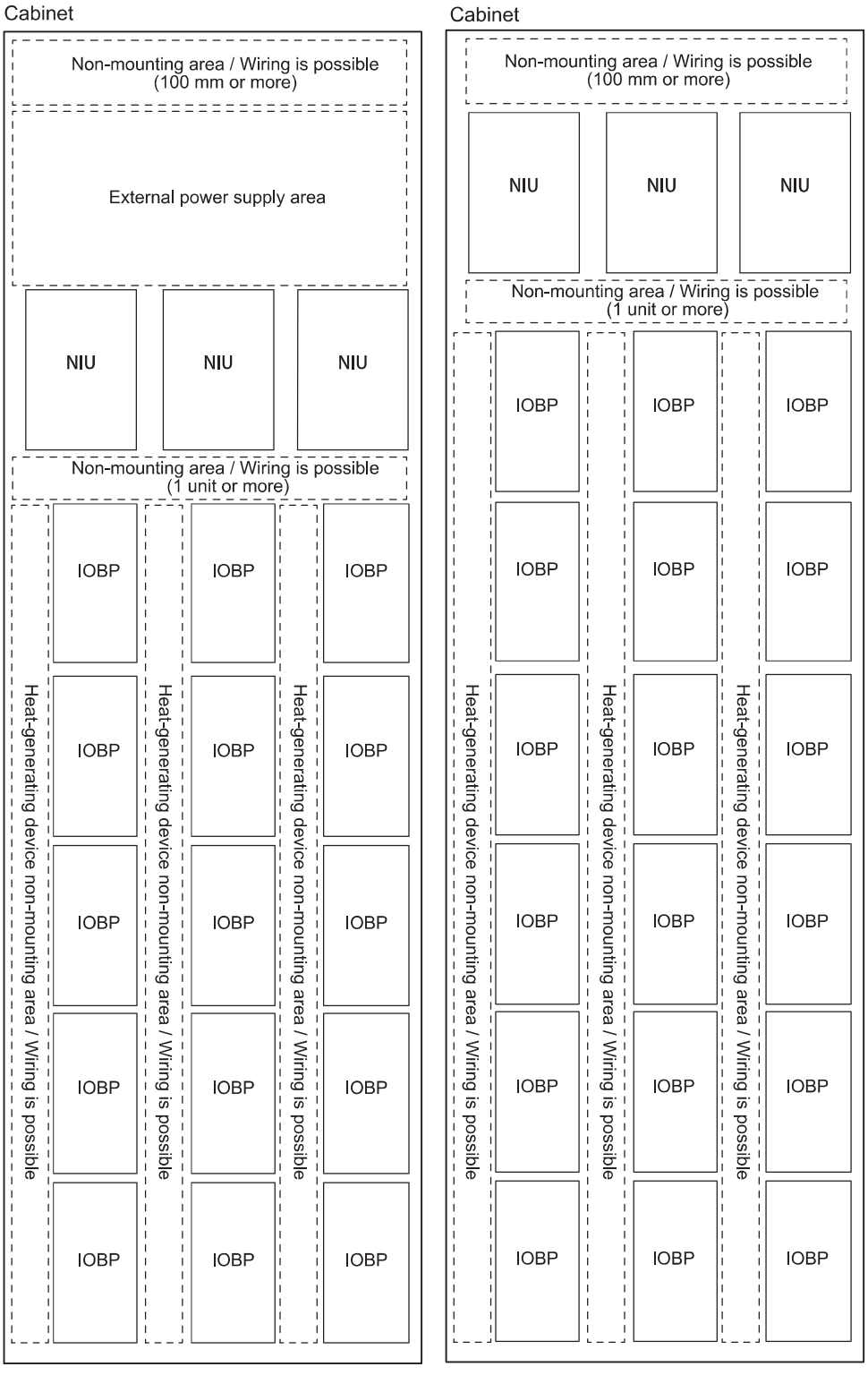


Figure Example of Mounting N-IO Nodes (Non-Intrinsic Safety barrier) in a Cabinet

Example of Mounting N-IO Nodes (Intrinsic Safety Barrier) in a Cabinet

Temperature conditions

In this example, the ambient temperature is assumed to be the followings.

Cabinet ambient temperature	50 °C or less

Maximum numbers of units that can be mounted in case of this example

Type	Model	Number of units that can be mounted per side
NIU	S2NN30D	Up to 2
IOBP_IS	S2BN4D or S2BN5D	Up to 8 (2 rows × 4 shelves) Up to 10 (2 rows × 5 shelves)

Heat-generating devices other than the above shall not be mounted on the same mounting plate.

IOBP cannot be mounted.

Mounting conditions

- The NIU shall be mounted with a 100-mm or more space from the cabinet ceiling.
- A 1-unit (= 44.45 mm) or more space shall be provided between NIU and IOBP_IS.
- Suitable length of signal cables and power cables should be used.
- Mounting the devices in the cabinet should be in line according to the intrinsic safety standard.

The following shows how to mount N-IO nodes (Intrinsic Safety barrier) in a cabinet:

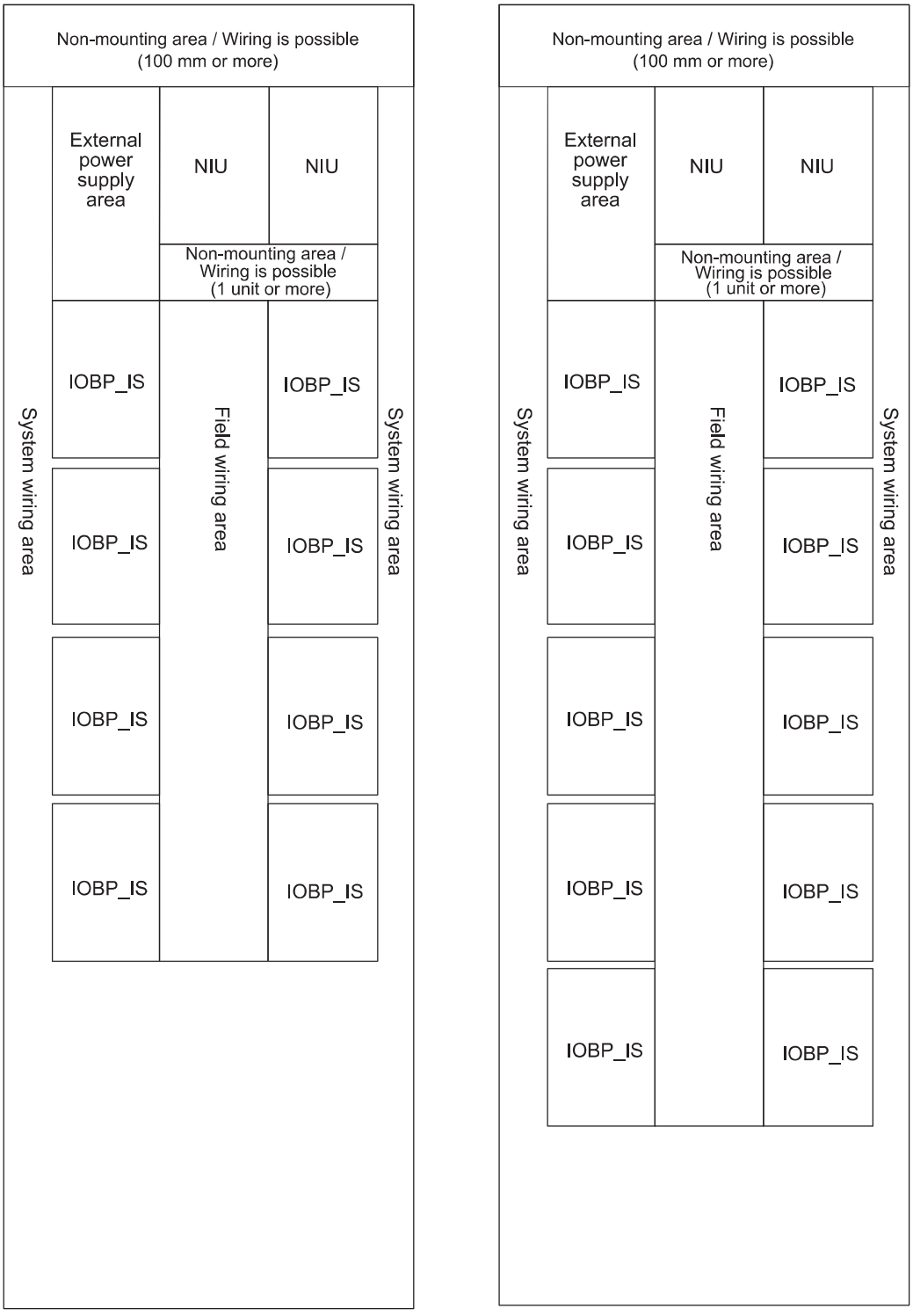


Figure Example of Mounting N-IO Nodes (Intrinsic Safety Barrier) in a Cabinet

Junction Box for N-IO System

This section describes examples of the maximum number of N-IO system equipment (except for equipment for RIO System Upgrade) installed in general-purpose junction boxes.

The following shows the common specifications to the examples of junction boxes for N-IO system that are explained later.

Junction Box Specifications

The following junction box is assumed to be used.

Table Junction Box Dimensions

W	D	H	Material
800 mm	300 mm	1000 mm	Metal

Product examples

Table The area of an air supply/air exhaust port

	Area
Air supply port	—
Air exhaust port	—

—: Not required

Table The requirement of a door fan

	Air flow
Door fan	—

—: Not required

Table Product examples

	Manufacturer	Model
Junction Box	Rittal	AE1180 series

Notes

The following shows the common notes to the examples.

- The ventilation for each system shall not be blocked.
- The mounting plate for mounting the IOBP and IOBP_IS shall be made of metal, regardless of whether DIN rail or panel mounting.
- A DIN rail shall be made of metal.
- For mounting restrictions other than the above, refer to the General Specifications (GS).
- When using a DIN rail, be sure to install a DIN rail on the mounting plate.
  Fixing at the both ends of a DIN rail and not fixing at the middle.

Conventions

The following shows the common abbreviations used and their explanations.

Abbreviations	Explanations
NIU	Node Interface Unit or Base Plate for Node Interface Unit
IOBP	Base Plate
IOBP_IS	Base Plate Intrinsic Safety explosion protection
Unit	Unit of 19 inch rack. 1 Unit = 44.45 mm

Example of Mounting N-IO Nodes (Non-Intrinsic Safety Barrier) in a Junction Box

Temperature conditions

In this example, the ambient temperature is assumed to be the followings.

Junction Box ambient temperature	50 °C or less

Maximum numbers of units that can be mounted

	Type	Model	Number of units that can be mounted per side
Per junction box	NIU	S2NN30D	Up to 1
	IOBP	S2BN1D	Up to 4 (2 rows × 2 shelves)
	Other	Heat-generating device (*1)	heat generation: 40 W or less

*1: The device to be mounted shall be selected from those that have the ambient temperature range of +15 °C or more.

Heat-generating devices other than the above shall not be mounted in the junction box.

In this example, IOBP_IS cannot be mounted.

Mounting conditions

- Mount the NIU on the upper left in the junction box basically.
- Do not mount the IOBP so that its heat-generating part (adaptor or I/O) is located immediately under the N-ESB Bus module (S2EN501). The IOBP may be mounted immediately under the power supply of the NIU (S2PW50x).
- The NIU shall be mounted in the left upper location of the junction box with a 2-unit or more space from the ceiling.
- A 1-unit or more space shall be provided between the NIU and IOBP.
- To mount heat-generating devices other than NIU and IOBP shall be mounted with 30-mm intervals on the right of the NIU on the top shelf. The specifications of the devices shall be observed.

The following shows how to mount N-IO nodes (Non-Intrinsic Safety barrier) in a junction box:

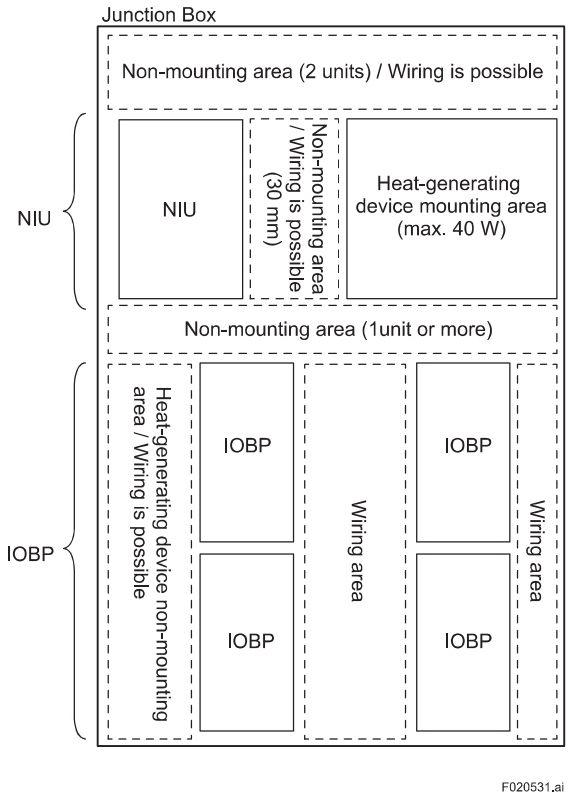


Figure Example of Mounting N-IO Nodes (Non-Intrinsic Safety Barrier) in a Junction Box

Example of Mounting N-IO Nodes (Intrinsic Safety Barrier) in a Junction Box

Temperature conditions

In this example, the ambient temperature is assumed to be the following.

Junction Box ambient temperature	50 °C or less

Maximum numbers of units that can be mounted

	Type	Model	Number of units that can be mounted per side
Per junction box	NIU	S2NN30D	Up to 1
	IOBP_IS	S2BN4D or S2BN5D	Up to 2 (2 rows × 1 shelf)
	Other	Heat-generating device (*1)	heat generation: 20 W or less

*1: The device to be mounted shall be selected from those that have the ambient temperature range of +15 °C or more.

Heat-generating devices other than the above shall not be mounted in the junction box.

In this example, IOBP cannot be mounted.

Mounting conditions

- Do not mount the IOBP_IS so that its heat-generating part (Barrier or I/O) is located immediately under the N-ESB Bus module (S2EN501). The IOBP_IS may be mounted immediately under the power supply of the NIU (S2PW50x).
- The NIU shall be mounted with a 2-unit or more space from the ceiling of the junction box.
- A 2-unit or more space shall be provided between the NIU and IOBP_IS.
- To mount heat-generating devices other than NIU and IOBP_IS shall be mounted with 30-mm intervals on the right of the NIU on the top shelf. The specifications of the devices shall be observed.

The following shows how to mount N-IO nodes (Intrinsic Safety barrier) in a junction box:

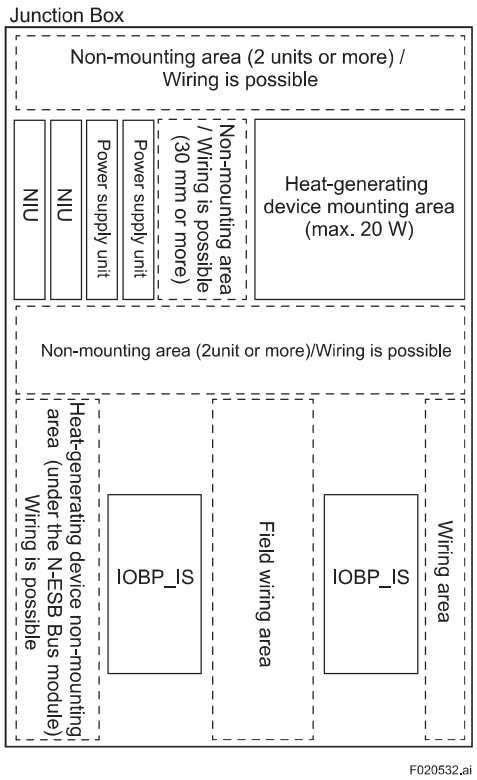


Figure Example of Mounting N-IO Nodes (Intrinsic Safety Barrier) in a Junction Box

CAUTION

The wiring that will be intrinsic safety circuits must be installed so that they are electrically separated from the wiring of non-intrinsic safety circuits, including the in-cabinet wiring. Install the wiring according to the IEC 60079-14 standards or the requirements for explosion-proof wiring of the country where the system is used.

Example of Mounting N-IO Nodes (Mixture of Intrinsic Safety Barrier and Non-Intrinsic Safety Barrier) in a Junction Box

Temperature conditions

In this example, the ambient temperature is assumed to be the following.

Junction Box ambient temperature	50 °C or less

Maximum numbers of units that can be mounted

	Type	Model	Number of units that can be mounted per side
Per junction box	NIU	S2NN30D	Up to 1
	IOBP	S2BN1D	Up to 2 (1 row × 2 shelves)
	IOBP_IS	S2BN4D or S2BN5D	Up to 1 (1 row × 1 shelf)
	Other	Heat-generating device (*1)	heat generation: 20 W or less

*1: The device to be mounted shall be selected from those that have the ambient temperature range of +15 °C or more.

Heat-generating devices other than the above shall not be mounted in the junction box.

Mounting conditions

- Do not mount the IOBP/IOBP_IS so that its heat-generating part (Barrier or I/O) is located immediately under the N-ESB Bus module (S2EN501). The IOBP/IOBP_IS may be mounted immediately under the power supply of the NIU (S2PW50x).
- The NIU shall be mounted with a 2-unit or more space from the ceiling of the junction box.
- A 2-unit or more space shall be provided between the NIU and IOBP/IOBP_IS.
- To mount heat-generating devices other than NIU and IOBP/IOBP_IS shall be mounted with 30-mm intervals on the right of the NIU on the top shelf. The specifications of the devices shall be observed.

The following shows how to mount N-IO nodes (mixture of Intrinsic Safety barrier and Non-Intrinsic Safety barrier) in a junction box:

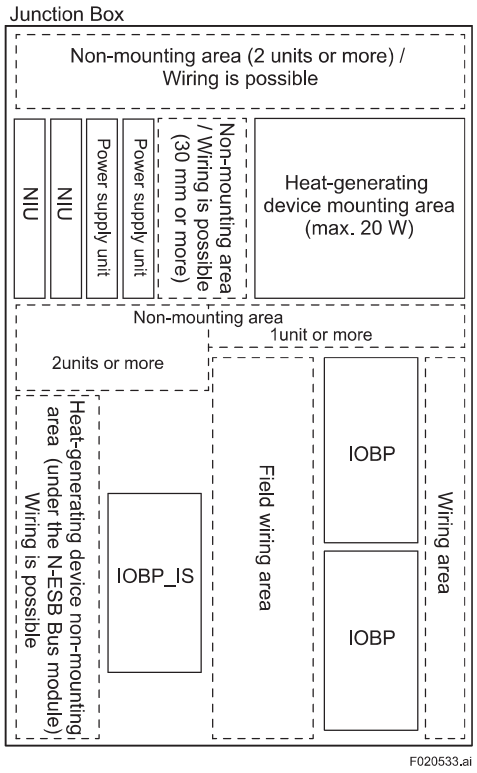


Figure Example of Mounting N-IO Nodes (Mixture of Intrinsic Safety Barrier and Non-Intrinsic Safety Barrier) in a Junction Box

CAUTION

The wiring that will be intrinsic safety circuits must be installed so that they are electrically separated from the wiring of non-intrinsic safety circuits, including the in-cabinet wiring. Install the wiring according to the IEC 60079-14 standards or the requirements for explosion-proof wiring of the country where the system is used.

2.5.7 Desktop Equipment

There are SENG (PCs), general-purpose printers, etc. as the devices used on the desks.

When installing any devices on the desks, take care about the following:

- It should provide a level horizontal surface for the PC or printer.
- A work space should be preserved to connect the cables.
- Support rising cables to prevent their weight from being applied to connectors directly. Keep a space of 100 mm radius or more around the connectors.
- Do not place the desk such as to expose the PC to direct sunlight or high humidity.

2.5.8 Installing Control Network Interface Card

This section describes how to install VI702 Control Network interface card. The card is installed in a PCI Express slot of an SENG PC to connect it to the Control Network.

SEE ALSO

- The steps described below are based on general-purpose PC/AT compatible machines. For details, refer to the manual for the specific PC.
- For the station address setting, refer to the Safety Control Stations (Hardware), IM 32P06C10-01EN or IM 32Q06C10-31E.

Card Installation Procedure

1. Set the station address for the control bus interface card.
2. Turn off the computer and unplug the power cord for safety.
3. Remove the PC cover.
4. Remove the slot cover.
5. Insert the control bus interface card in the slot. Make certain that the card is properly set in the slot.
6. Attach the computer cover.
7. Write the station address on a seal (sticker) and attach it to the front of the PC or in another similarly easy-to-view place.

SEE ALSO

- For the electrostatic protection, refer to 1.5.2, “Countermeasures against Static Electricity.”
- For the control bus connections, refer to 3.7, “Connecting Bus Cable.”

3. Cabling

This section describes how to cable the installed system equipment.

Connecting terminals for power, grounding, and signal cables are shown in figures.

The figures also show how to connect the SENG to field control units, and optical fiber cables to the optical bus repeaters.

3.1 Cables and Terminals

It is recommended that you use flexible, thin, easy-to-bend, twisted-pair cables to connect the terminals of the system equipment. Use solderless (crimp-on) terminals with insulating cover, which have low contact resistance little aging.

Rigid cables make cabling work difficult and exert unnecessary force on the terminals, which may result in system failures.

Cables with the temperature rating of an ambient temperature plus 10 °C or more must be used.

As for the following models, cables with the temperature rating as shown in the below Table must be used.

Table Rating temperature of Cables

Models	Cables	Temperature rating of Cables
SBD2D,SBD3D,SBD4D	Signal Cables (including READY terminal)	An ambient temperature plus 20 °C or more
	Input Power Cables	An ambient temperature plus 30 °C or more
SBM54D	Signal Cables (excluding READY terminal)	An ambient temperature plus 40 °C or more
	Input Power Cables Signal Cables (READY terminal)	An ambient temperature plus 20 °C or more
S1BB4D	Input Power Cables	An ambient temperature plus +30 °C
	Ready terminal	An ambient temperature plus +20 °C
SYEPD4D	Input Power Cables	An ambient temperature plus 30 °C or more
SYEPD5D	Input Power Cables	90 °C or more
AEP7D (100-120 / 220-240 V AC)	Input Power Cables	An ambient temperature plus 30 °C or more
AEP7D (24 VDC)	Input Power Cables	An ambient temperature plus 50 °C or more
AEPV7D (100-120 / 220-240 V AC)	Input Power Cables	An ambient temperature plus 30 °C or more
AEPV7D (24 VDC)	Input Power Cables	An ambient temperature plus 40 °C or more
S2BN1D	Field Power Cables	An ambient temperature plus 20 °C or more
S2BN4D	I/O Cables	An ambient temperature plus 20 °C or more
S2BN5D	Grounding Cables	An ambient temperature plus 20 °C or more
S2PW503/S2PW504	Input Grounding Cables	An ambient temperature plus 30 °C or more
A2BM4	Terminal board	An ambient temperature plus 20 °C or more

Signal Cables

Nominal conductor cross-sectional area:
For FIO Node: 0.75 to 2.00 mm^2
For N-IO Node: 0.75 to 2.50 mm^2 (AWG 20~14)
Sleeve for spring clamp terminals:
0.5 to 1.5 mm^2 (AWG 20~16)
For SED2D: 0.75 to 5.5 mm^2

Example of suitable cables:
600 V polyvinyl chloride insulated wires (IV); IEC 60227-3/JIS C 3307
Polyvinyl chloride insulated wires for electrical apparatus (KIV); IEC 60227-3/JIS C 3316
600 V Grade heat-resistant polyvinyl chloride insulated wires (HIV); IEC 60227-3/JIS C 3317
Heat-resistant PVC wire (UL1015/UL1007)
PVC insulated and PVC sheathed control cables (CVV); JIS C 3401

Alarm and Control Circuit Cables

Nominal conductor cross-sectional area: 0.13 to 2.5 mm^2
Node Interface Unit External Alarm input terminal: 0.5 to 2.5 mm^2 (AWG 20~14)
Other than above: 0.5 to 1.25 mm^2

Example of suitable cables:
600 V polyvinyl chloride insulated wires (IV); EC 60227-3/JIS C 3307
Polyvinyl chloride insulated wires for electrical apparatus (KIV); IEC 60227-3/JIS C 3316
Heat-resistant PVC wire (UL1007)

Power Cables

Nominal conductor cross-sectional area:
For rack-mounted 100-120 V AC /220-240 V AC-driven equipment: 1.25 to 2.0 mm^2
For rack-mounted 24 V DC-driven equipment: Minimum 2.0 mm^2
For N-IO I/O Base plates S2BN1D (Field Power Supply terminal): 3.5 to 5.5 mm^2
For N-IO Barrier Base plates (Barrier Power Supply terminal): 0.5 to 1.5 mm^2
Node Interface Unit: 1.25 mm^2 (AWG 16) Double Insulation structure
For cabinets AC 100-120/220-240 V-driven: Minimum 8.0 mm^2
For cabinets DC 24 V-driven equipment: Minimum 14.0 mm^2

Example of suitable cables:
600 V polyvinyl chloride insulated wires (IV); IEC 60227-3/JIS C 3307
Polyvinyl chloride insulated wires for electrical apparatus (KIV); IEC 60227-3/JIS C 3316

Note: Use cables capable of supplying current required by respective pieces of equipment with low voltage drop.

Grounding Cables

SEE ALSO See Section 1.4, “Grounding,” for wiring of grounding cables connecting grounding bars of different cabinets and/or panels to each other.

Nominal conductor cross-sectional area:
For Node Interface Unit: Minimum 2.0 mm^2 (AWG14)
For N-IO I/O Base plates: Minimum 2.0 mm^2 (AWG14)
For N-IO Barrier Base plates: Minimum 2.0 mm^2 (AWG14)
Grounding cables connecting cabinets
AC 100-120/220-240/V-driven to protective grounding system:
Minimum 5.5 mm^2
Grounding cables connecting cabinets DC 24 V-driven to protective grounding system:
Minimum 8.0 mm^2

Example of suitable cables:
600 V polyvinyl chloride insulated wires (IV); EC 60227-3/JIS C 3307
Polyvinyl chloride insulated wires for electrical apparatus (KIV); IEC 60227-3/JIS C 3316

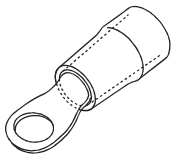
Cable Terminals

Use the specified solderless terminals and sleeves for pressure clamp terminal on the end of terminal-connected cables, providing low contact resistance, high durability, and low aging.

Solderless Lug

CAUTION

- Be sure to use solderless terminals with insulating sheath.
- Use solderless terminals and crimp tools from the same manufacturer.
- Use appropriate crimp tools meeting the cable size.



F030101.ai

Figure Solderless Terminal with Insulating Sheath

Sleeve for pressure clamp terminal and spring clamp terminal

When connecting the process I/O signal to the pressure clamp terminal of the I/O module, strip the cable coating (without a sleeve) or attach a sleeve to the cable.

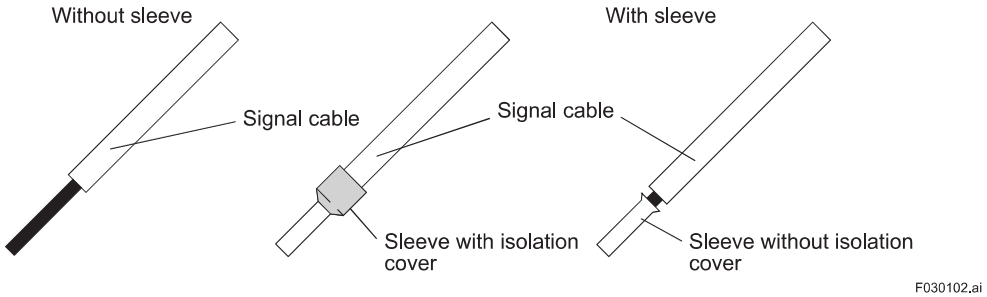


Figure Sleeve for Pressure Clamp Terminal and spring clamp terminal

CAUTION

- Use a sleeve for pressure clamp terminal and a clamp tool from the same manufacturer.
- Use a sleeve for pressure clamp terminal and a clamp tool which suit the cable size.
- Use a sleeve which meet the following DIN standards.
  Sleeve without insulating cover (DIN 46 228/1)
  Sleeve with insulating cover (DIN 46 228/4)

Bending radius of the cable

When connecting a cable to a system instrument, ensure to secure the minimum bending radius of the cable.
The minimum bending radius is either the value shown in the cable manufacturer's specifications or six-fold of the cable conductor diameter, whichever is bigger should be applied.

3.2 Connecting Power

Power is connected either by using a grounding bipolar three-prong plug or by wiring to terminals.

The safety control unit and safety node unit in the ProSafe-RS have no power switch. So, it is recommended that a breaker be installed for each piece of equipment in the same room, for maintenance and safety requirements.

CAUTION

- Lay power cables 1 cm or more away from signal cables.
- Use power and ground cables conforming to the safety standards of each country.

Type and Maximum Length of Power Cables

Formulas are given below for determining the type and the maximum length (m) of branch cables from an indoor low-voltage main line.

- The standard type of cable used (nominal cross sectional area) is equivalent to JIS C 3312.
- Calculate the maximum power cable length from the following conditions as shown in the figure.
  However, the power cable must meet the conditions described as “AC Power Specification” in Section 1.3. The conditions in Section 1.3 always take top priority.

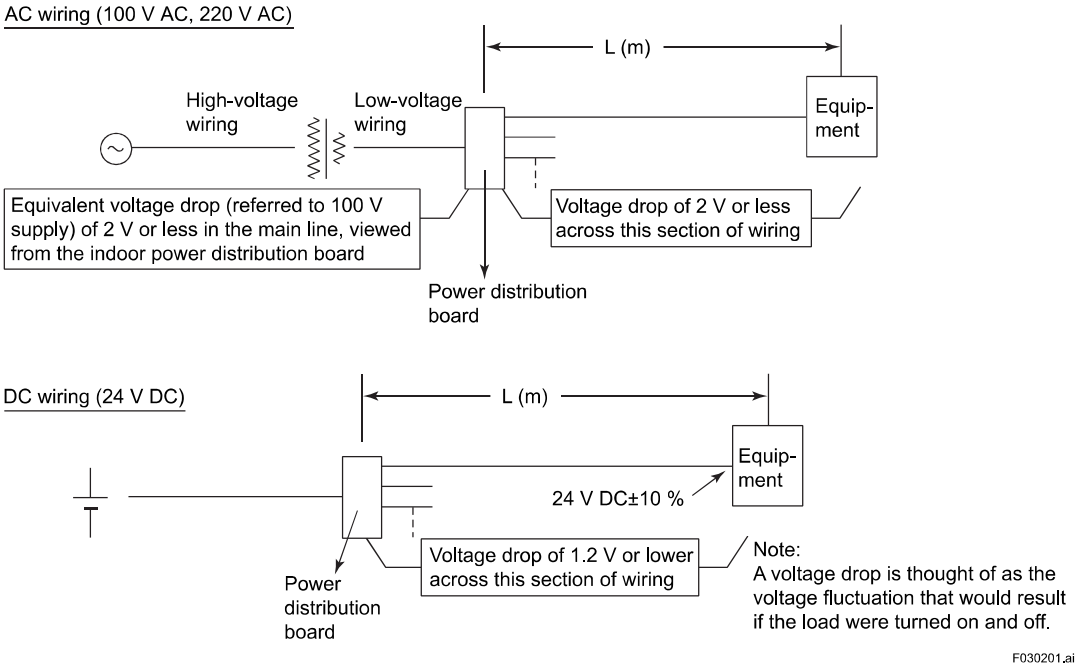


Figure Maximum Cable Length Calculation Conditions

[Maximum power cable length calculation]

Use the following formula to calculate the maximum power cable length:

(a) 100 V AC and 220 V AC models

$$L\,(m) = \frac{\text{Voltage drop across wiring}}{\text{Conductor resistance (ohm/km)} \times \text{(Number of cores)} \times \text{Equipment current consumption}} \times 1000$$

F030202.ai

(b) 24 V DC model

$$L\,(m) = \frac{\text{Voltage drop across wiring}}{\text{Conductor resistance (ohm/km)} \times \text{(Number of cores)} \times \text{Equipment current consumption}} \times 1000$$

F030203.ai

Note: In the formulas above, the voltage drop across wiring is assumed to be 2 V for AC power supplies and 1.2 V for DC power supplies; the number of cores is two; and the conductor resistance is as specified in the table below.

Table Wire Nominal Cross Sectional Areas and Resistances

Wire nominal cross sectional area	5.5 mm^2	8 mm^2	14 mm^2	22 mm^2
Wire conductor resistance	3.37 ohm/km	2.39 ohm/km	1.36 ohm/km	0.82 ohm/km

Power Cable Termination

Cable Termination

Use solderless lugs for power cables (see Figure).

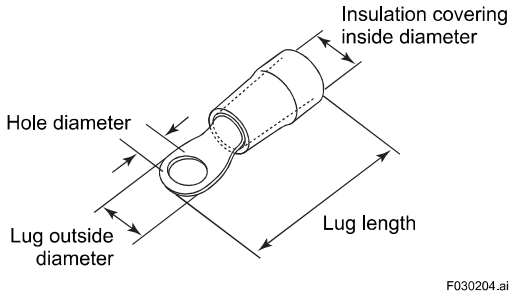


Figure Solderless (crimp-on) Lug

Solderless (crimp-on) Lug Specifications

The solderless lug to use must have the dimensions given in table according to the nominal cross sectional area of the power cable for which the lug is to be used.

Table Solderless Lug Dimensions

Nominal cross sectional area (mm^2)	Screw used (mm)	Hole diameter (mm)	Lug outside diameter (mm)	Lug length (mm)	Insulation covering inside diameter (mm)
1.25	4	4.3 or more	8.2 or less	approx.21	3.6 or more
2.0	4	4.3 or more	8.7 or less	approx.21	4.3 or more
8.0	6	6.3 or more	12.2 or less	approx.41	7.0 or more
5.5	5	5.3 or more	9.7 or less	approx.29	5.9 or more
22.0	8 (hexagon head bolt)	8.3 or more	16.8 or less	approx.50	11.0 or more

CAUTION

- Always use solderless lugs with insulating covering.
- Always use solderless lugs and crimp-on tool manufactured by the same manufacturer.
- The crimp-on tool must be matched to the wire thickness.

Sleeve Terminal Processing

Perform the following terminal processing for the primary power supply input with pressure clamp terminal.

Use a sleeve with insulating cover which meet the DIN 46 228/4.

CAUTION

- Use sleeves and a tool that are from the same manufacturer.
- Use sleeves and a tool that are suitable for the cable thickness.
- Connect the cable properly by inserting the wires all the way into the pressure clamp terminals.

Strip the cable coating at the end of the cable and then attach a sleeve. The sleeve specifications differ depending on the cable thickness. The sleeve specifications are shown in the following table.

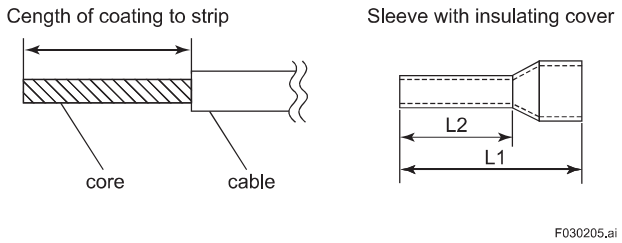


Figure Terminal Processing

Table Cable termination example of Sleeve with Insulating Cover

Nominal crosssectional area (mm^2)	Length to strip (mm)	Sleeve dimensions (mm)	
		L1	L2
1.25 (AWG16)	10	14	8

Power Distribution Boards

Power distribution boards are normally provided by the customer. Figures show examples of AC and DC power distribution boards.

AC Power Distribution Board

The power cables is branched to each unit by way of a circuit breaker.
Each power system uses three terminals (AC and ground: ISO M4 to M6 screws).

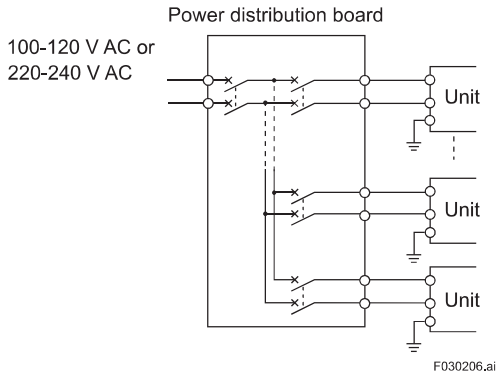


Figure AC Power Distribution Board

24 V DC Power Distribution Board

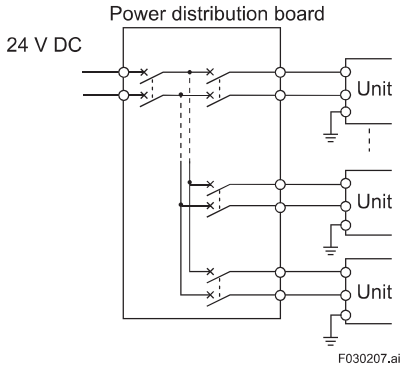


Figure 24 V DC Power Distribution Board

SEE ALSO For equipment grounding, see Section 3.4, “Power and Ground Cabling.”

Terminal Connection

The power supply terminals and the grounding terminals of each equipment are as follows.

Table The power supply terminals and the grounding terminals of each equipment

Category	Model	Power supply Type	Power supply terminal	Grounding terminal	Grounding Type
Field Control Unit	S2SC70S/D	Power Supply Input	M4 Screw	M4 Screw	Functional grounding
	SSC60S/D, SSC50S/D, SSC57S/D	Power Supply Input			
Node unit	SNB10D	Power Supply Input			
Unit	SNT10D	Power Supply Input			
Router	AVR10D	Power Supply Input			
	AW810D	Power Supply Input			
Node Interface Unit	S2NN30D	Power Supply Input	Pressure clamp	M4 Screw	• Functional grounding (24 V DC) • Protective grounding (Other than 24 V DC)
		Base Plate		M4 Screw	Functional grounding
I/O Unit	S2BN1D	Power Supply Input	Dedicated cable model: S2KPB10 (M4 Screw)	M3 Screw	Functional grounding
		Field Power Supply Input	M4 Screw		
	S2BN4D	Power Supply Input	Dedicated cable model: S2KPB10 (M4 Screw)	M4 Screw	Grounding for explosion protection
		Barrier Power Supply Input	M4 Screw		
	S2BN5D	Power Supply Input	Dedicated cable model: S2KPB10 (M4 Screw)	M4 Screw	Grounding for explosion protection
		Barrier Power Supply Input	M4 Screw		
Power supply bus unit	AEPV7D (Style 2 or the future models)	Power Supply Input	M4 Screw	M4 Screw	• Functional grounding (24V DC) • Protective grounding (Other than 24V DC)
		Power Supply Output	Dedicated 5 pins connector		

Conduit Power-cabling

Conduit cabling using cable glands is recommended to lay a power cable at the entrance of the cabinet for the following reasons:

To prevent the power cable from making contact with metallic plates or putting its weight on the power connection terminal.

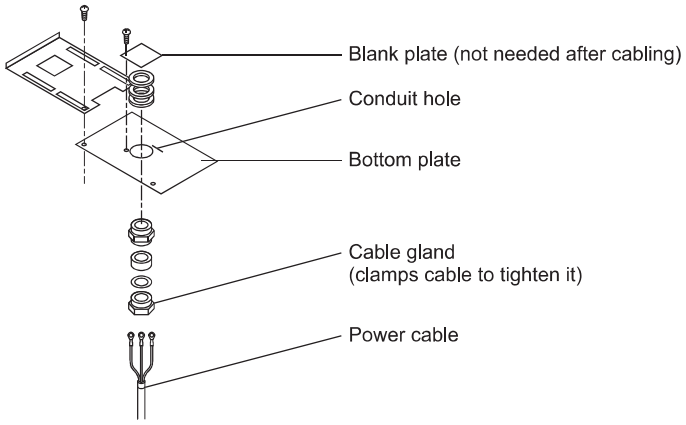


Figure Conduit Hole & Cable Gland

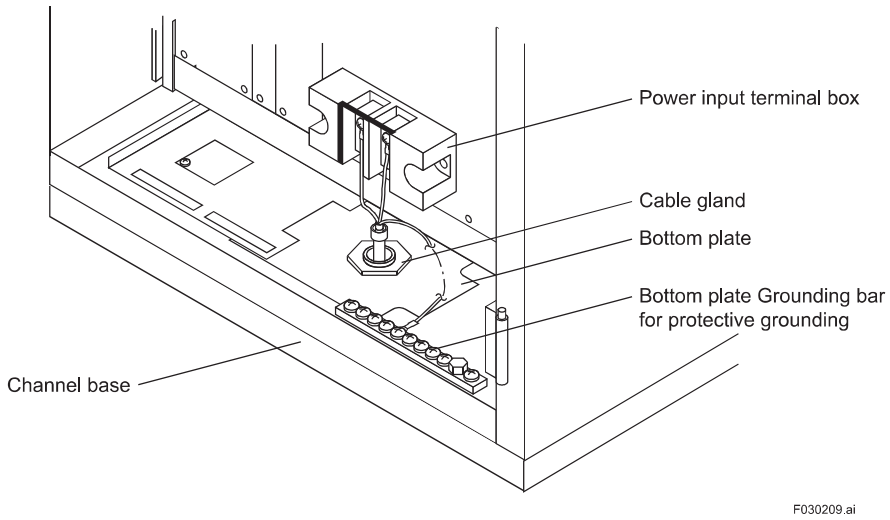


Figure Conduit Cabling

3.3 Connecting Ground Cable

Connect ground cables for the ProSafe-RS as follows:



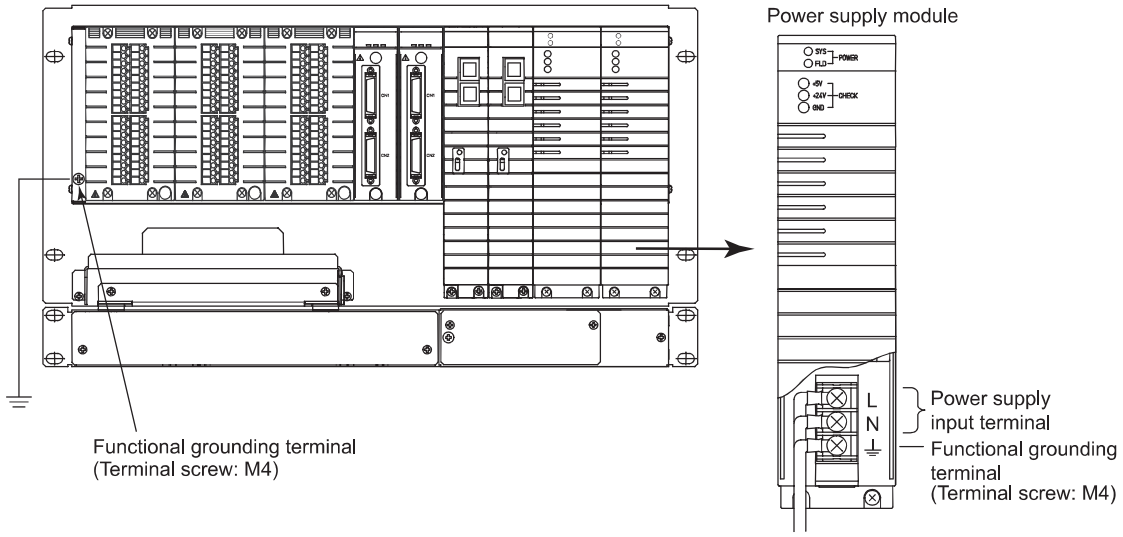
CAUTION

- Connect the terminal connection type device to the protective conductor terminal.
- Connect a power cable of the plug-in device to a grounded socket. The equipment case is grounded when the power cable is plugged in.

3.4 Power and Ground Cabling

The following figures illustrate how to connect power and grounding cables for ProSafe-RS hardware equipment.

S2SC70S/S2SC70D Safety Control Unit



Note: The same cable connections can be applied to SSC60S/SSC60D/SSC50S/SSC50D/SSC57S/SSC57D.

Figure S2SC70S/S2SC70D Cable Connections

SNB10D Safety Node Unit

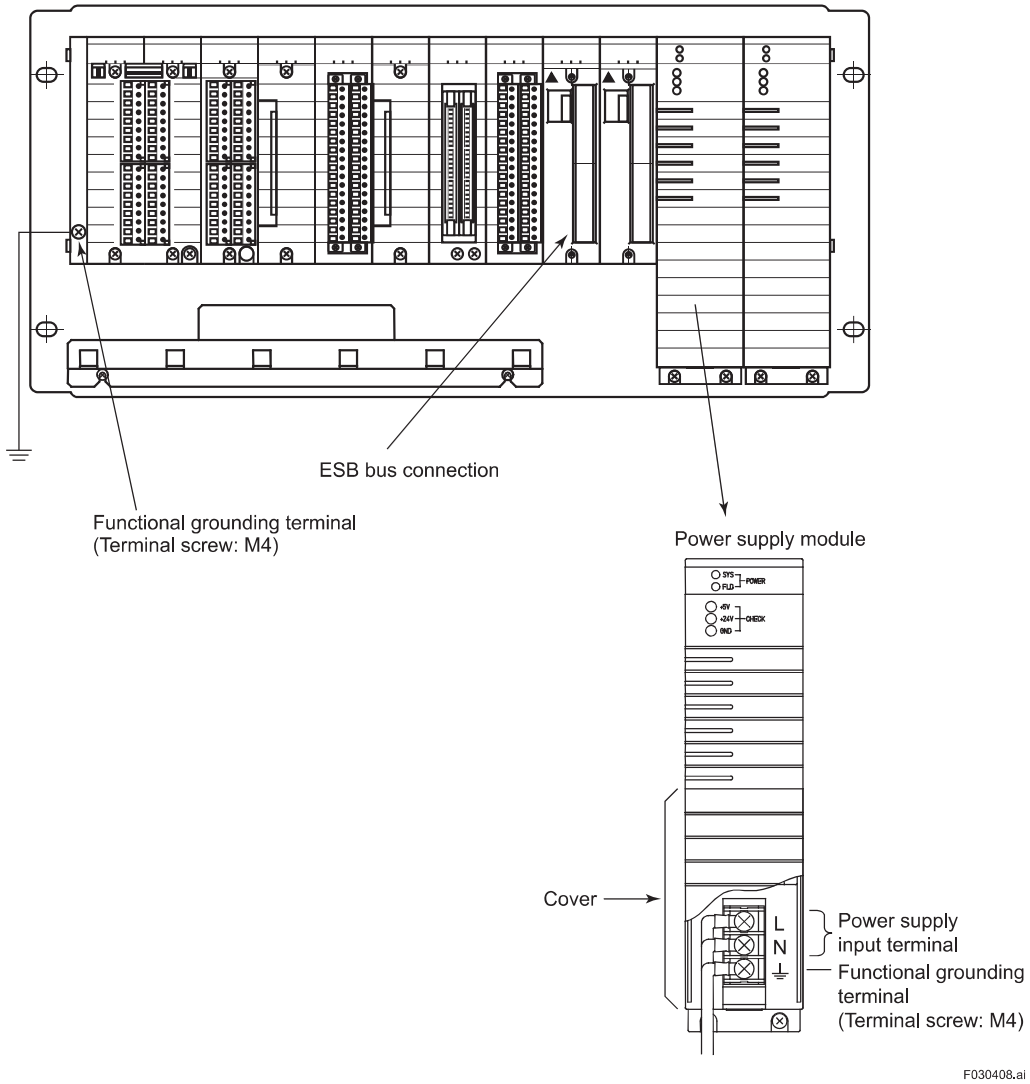


Figure SNB10D Power Cable Connection

An example of installing a node unit in a general-purpose cabinet along with an AEPV7D Power Supply Bus Unit is shown.

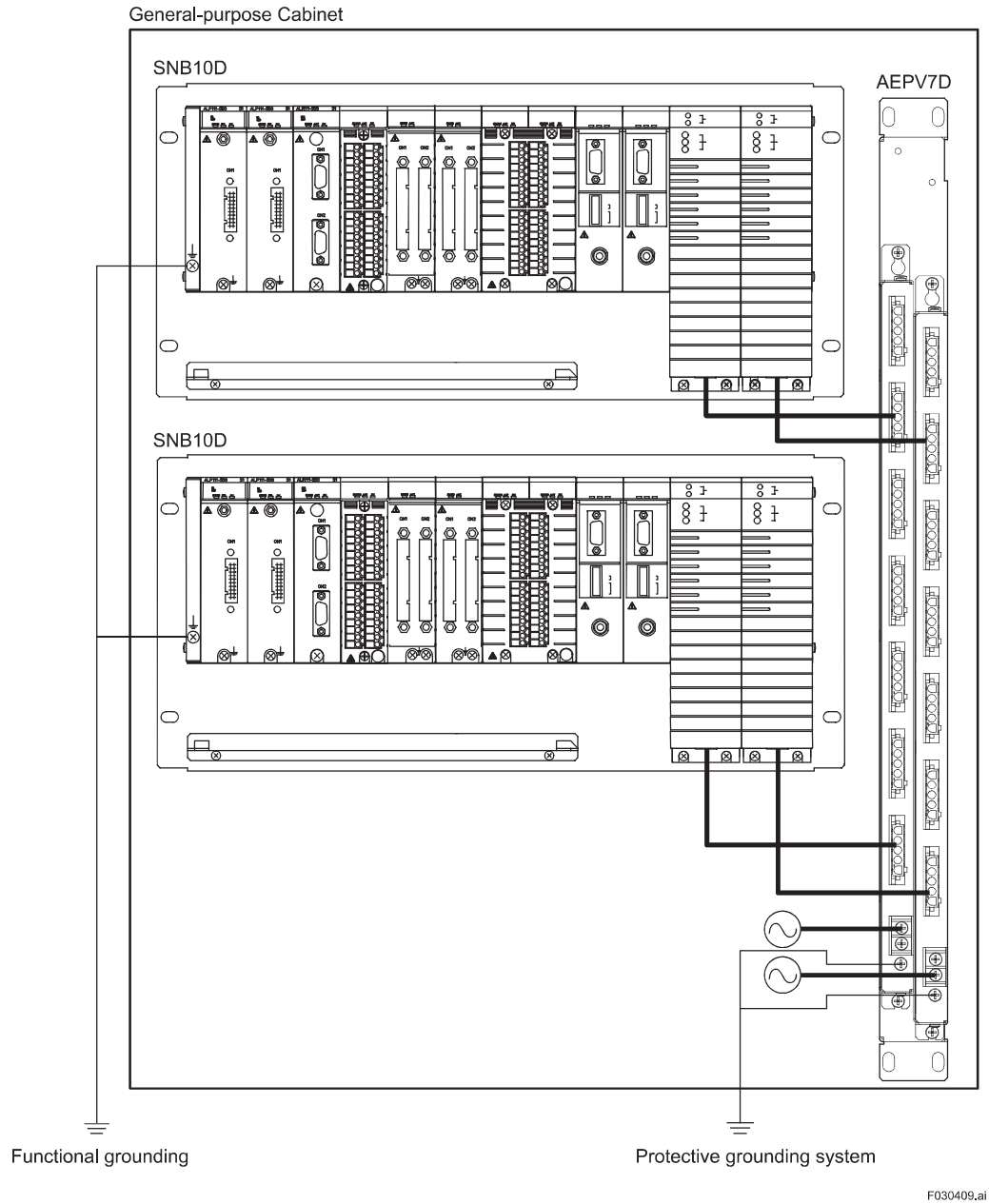


Figure Example of Installing AEPV7D in a General-purpose Cabinet (Dual AC Power Supply Line)

An example of installing a node unit in a general-purpose cabinet along with an AEP7D Primary Power Supply Bus Unit is shown.

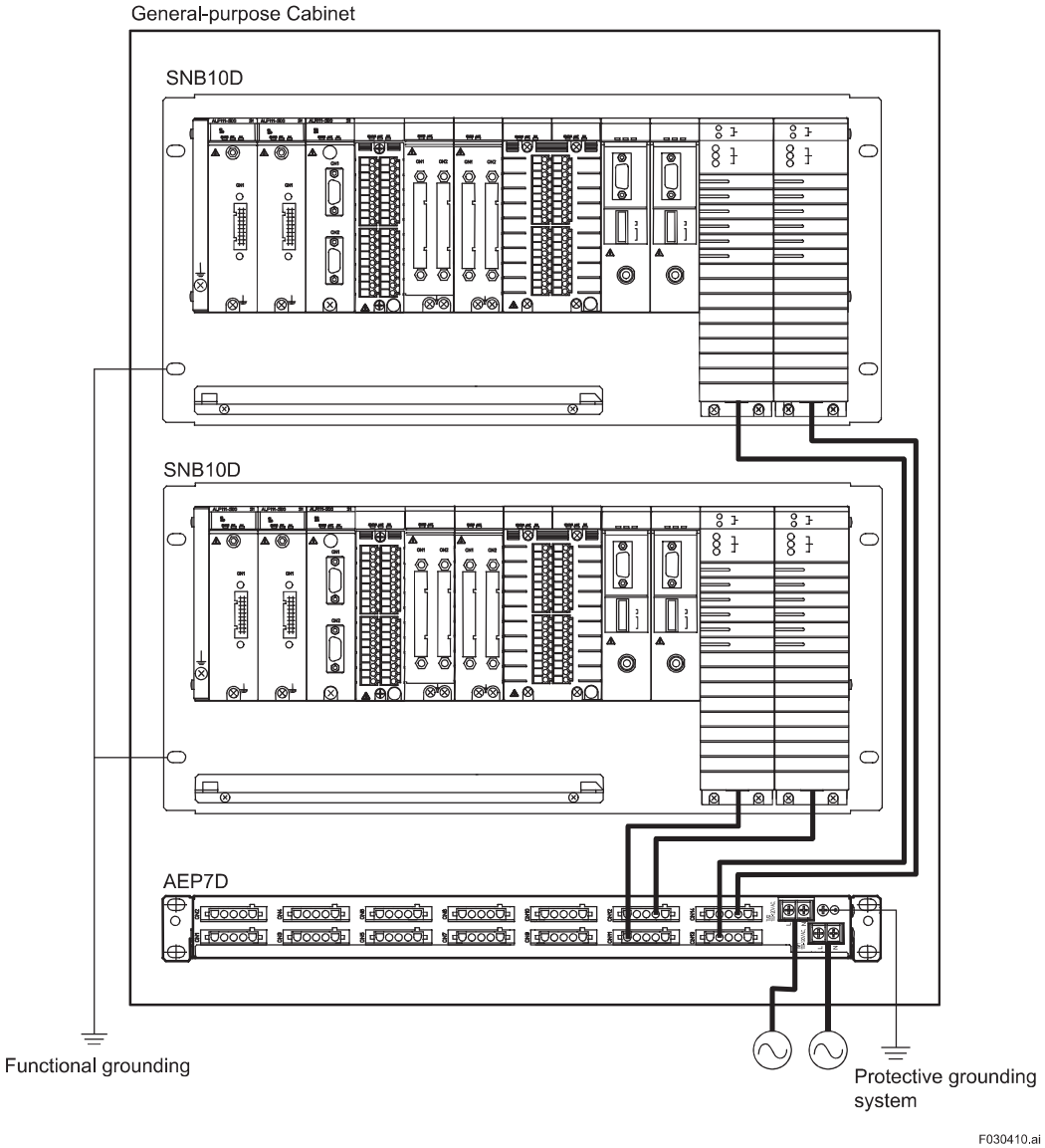


Figure Example of Installing AEP7D in a General-purpose Cabinet (Dual AC Power Supply Line)

SNT10D Unit for Optical Bus Repeater Module

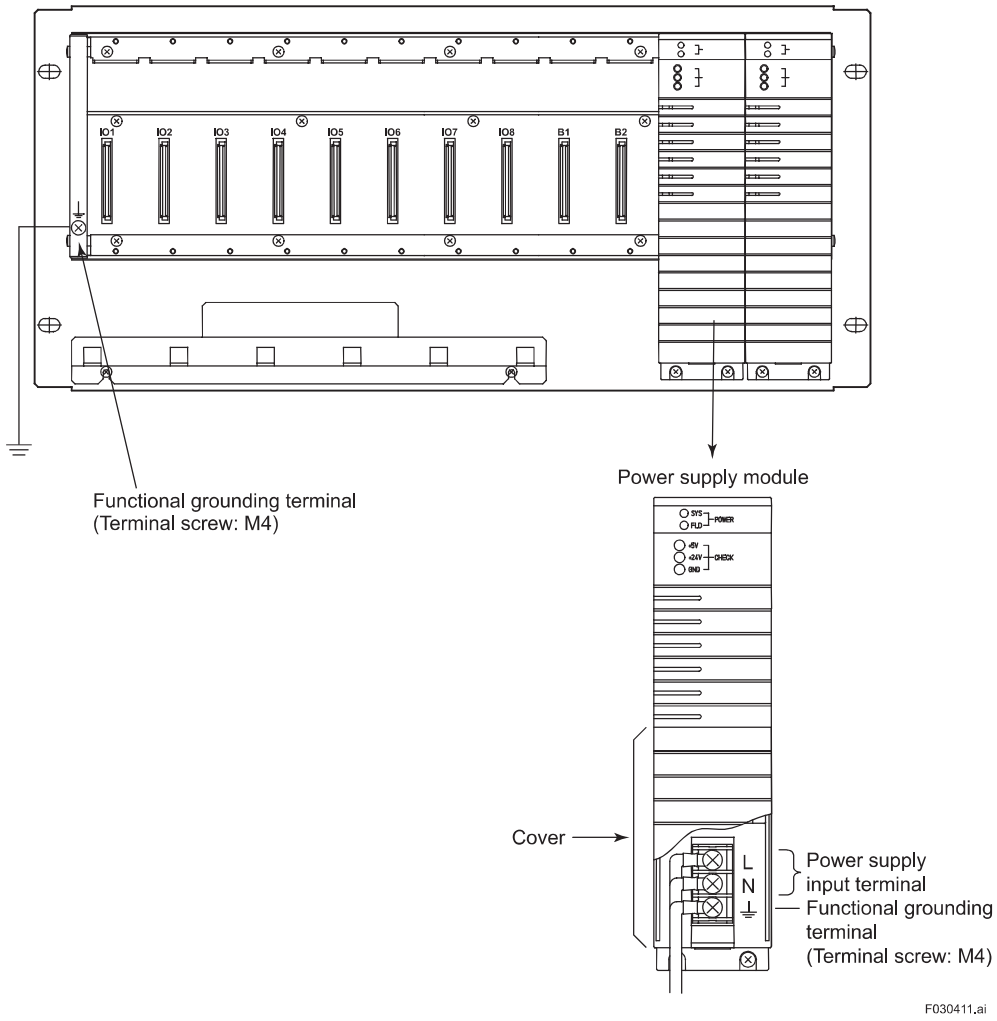


Figure SNT10D Power Cable Connection

S2NN30D Node Interface Unit

Connecting Power Supply with NIU and IOU

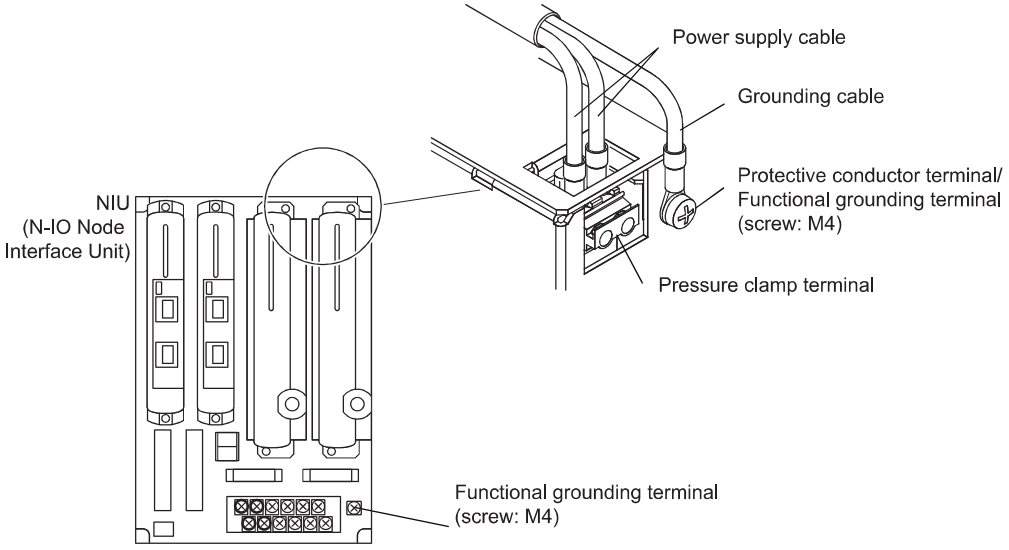


Figure Connecting Power Supply with Node Interface Unit

S2BN1D Base Plate with disconnecting terminal

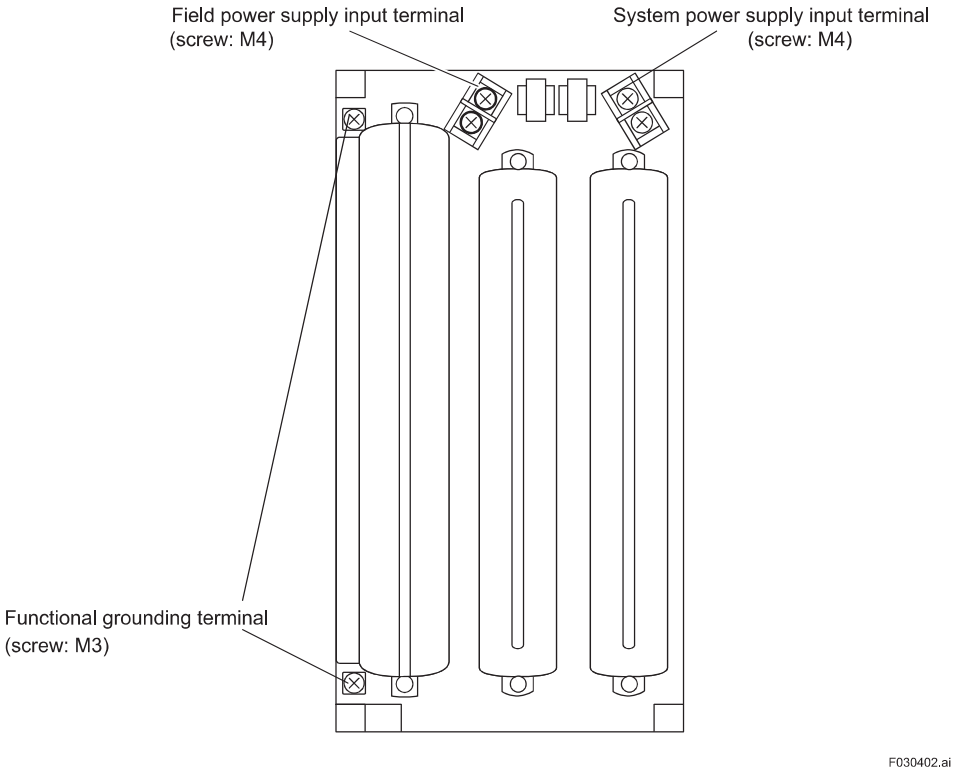


Figure S2BN1D-□1□□□, -□2□□□

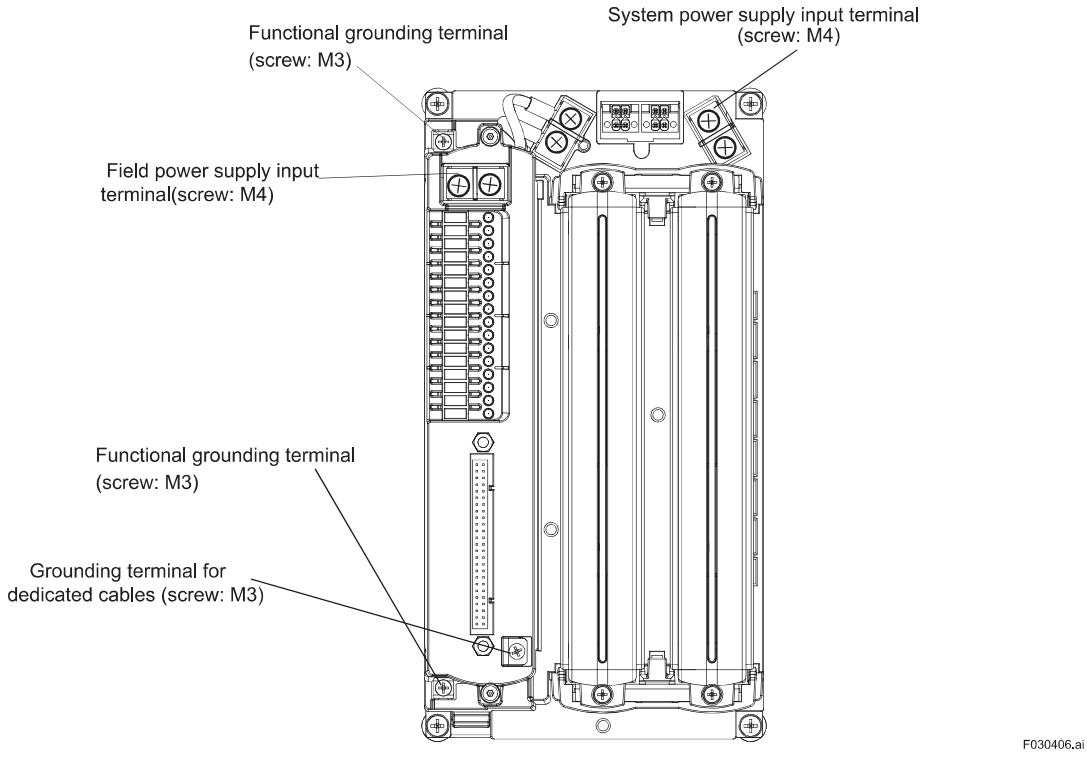
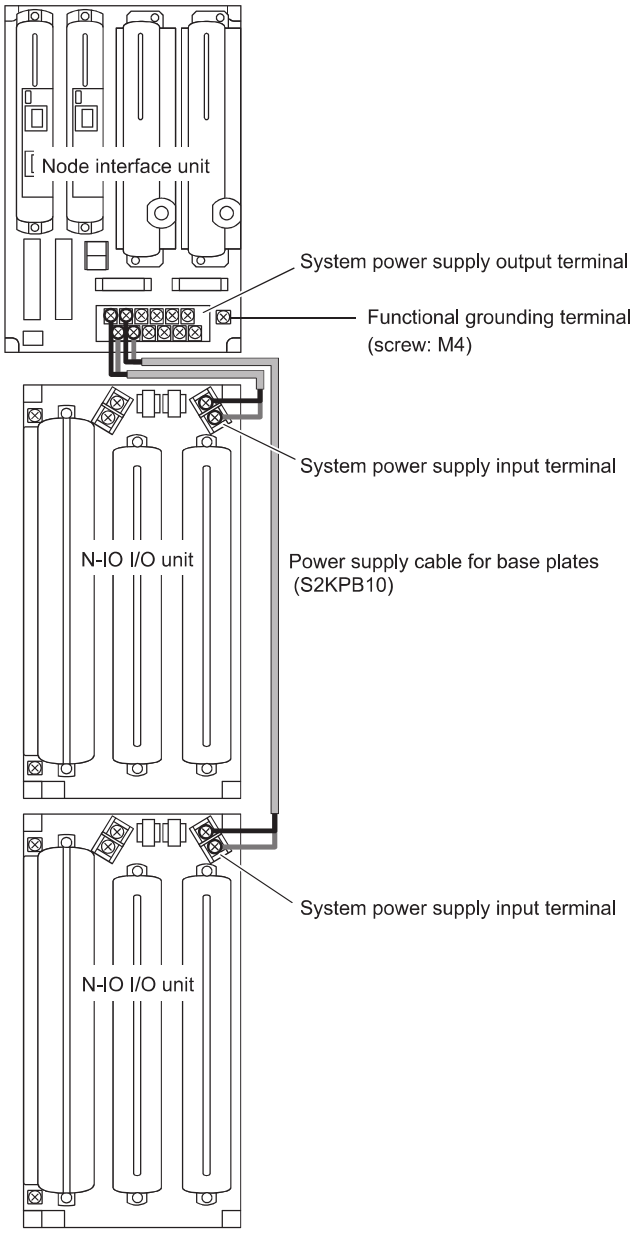


Figure S2BN1D-□9□□□

Connecting Power Supply with Node Interface Unit and I/O Units



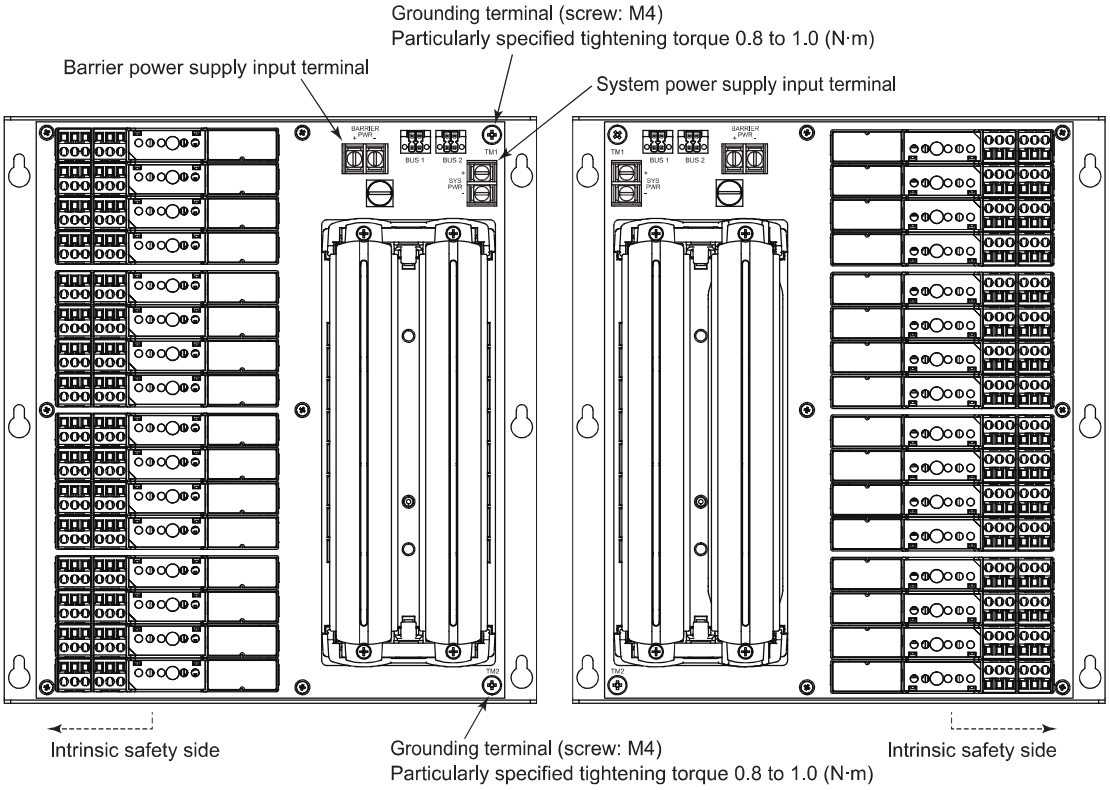
CAUTION

NIU and N-IO I/O Units can be installed in only the same cabinet.

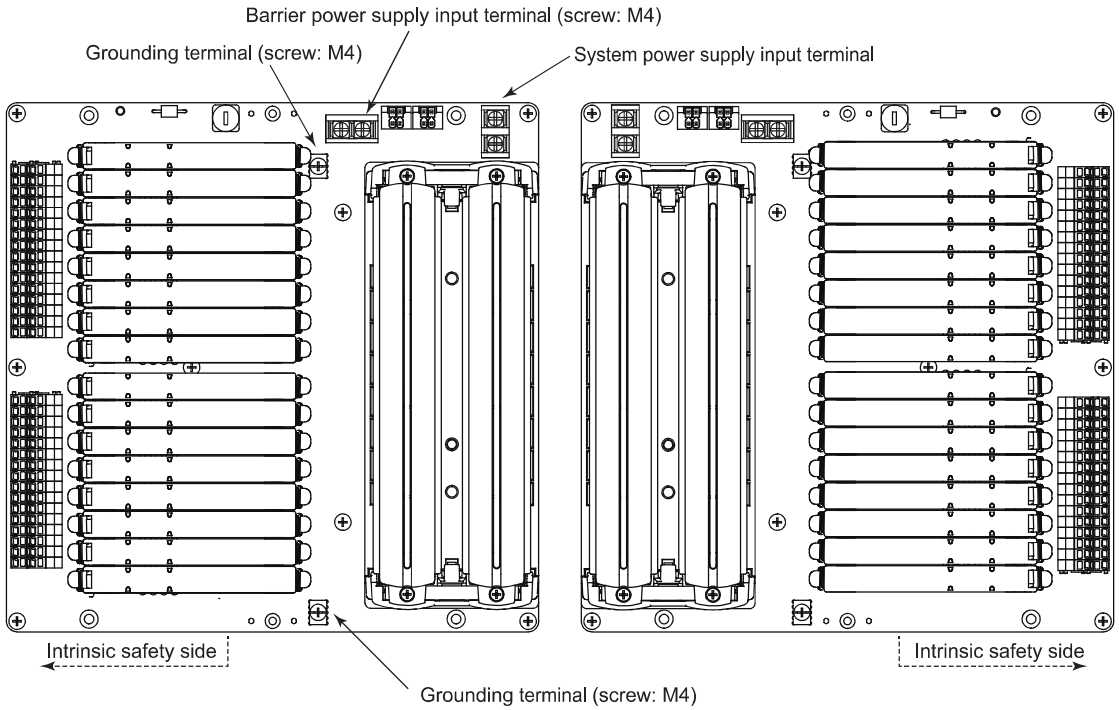
When connecting a Power Supply Cable for Base Plate to a N-IO node, ensure to keep the minimum bending radius of the cable.

The minimum bending radius of the Power Supply Cable is six-fold of the diameter of the cable.

S2BN4D Base Plate for Barrier (MTL)

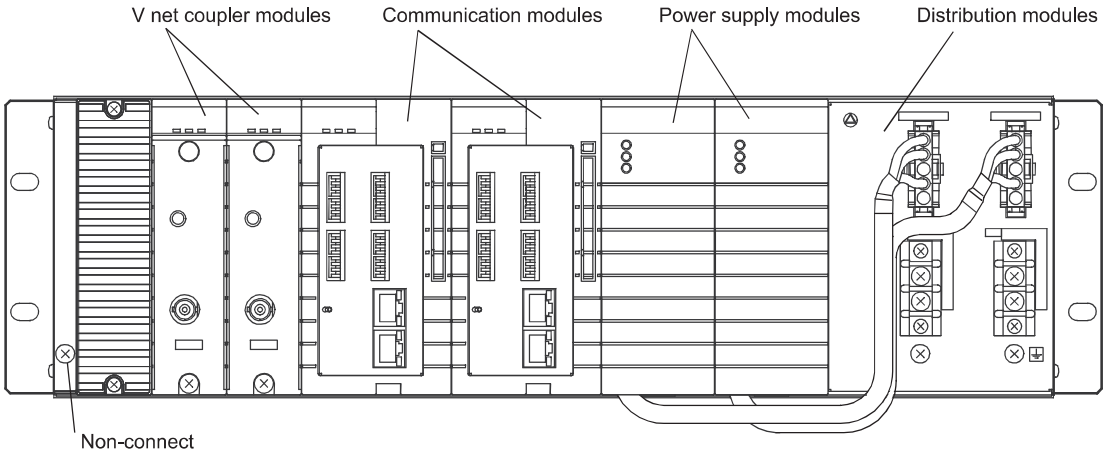


S2BN5D Base Plate for Barrier (P+F)



F030404.ai

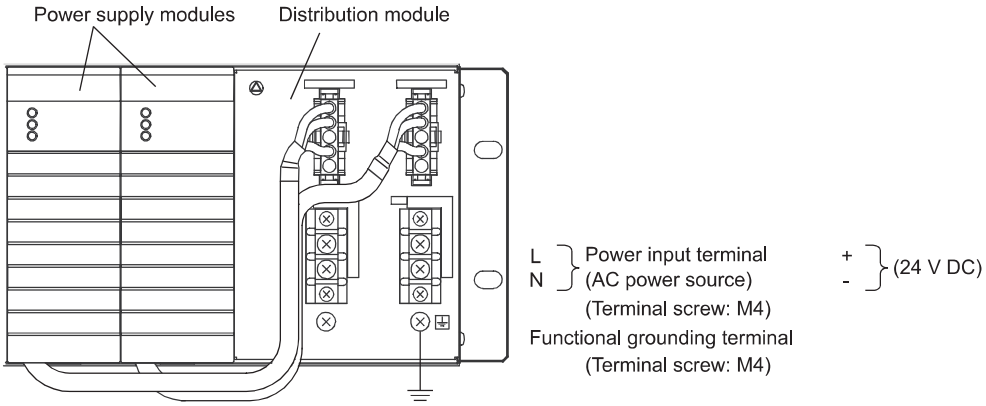
AVR10D Duplexed V net Router



F030412.ai

Cabling for Power Supply

The figure below shows the connection terminals for power supply cables.



F030413.ai

Power Cable Connection

IMPORTANT

When power to the V net router is turned off, communications with the areas within the coverage of the V net service are disabled. The service coverage area needs to be taken into consideration when designing a system to supply power to the V net router (e.g. providing an independent power source for the V net router).

AW810D Wide Area Communication Router

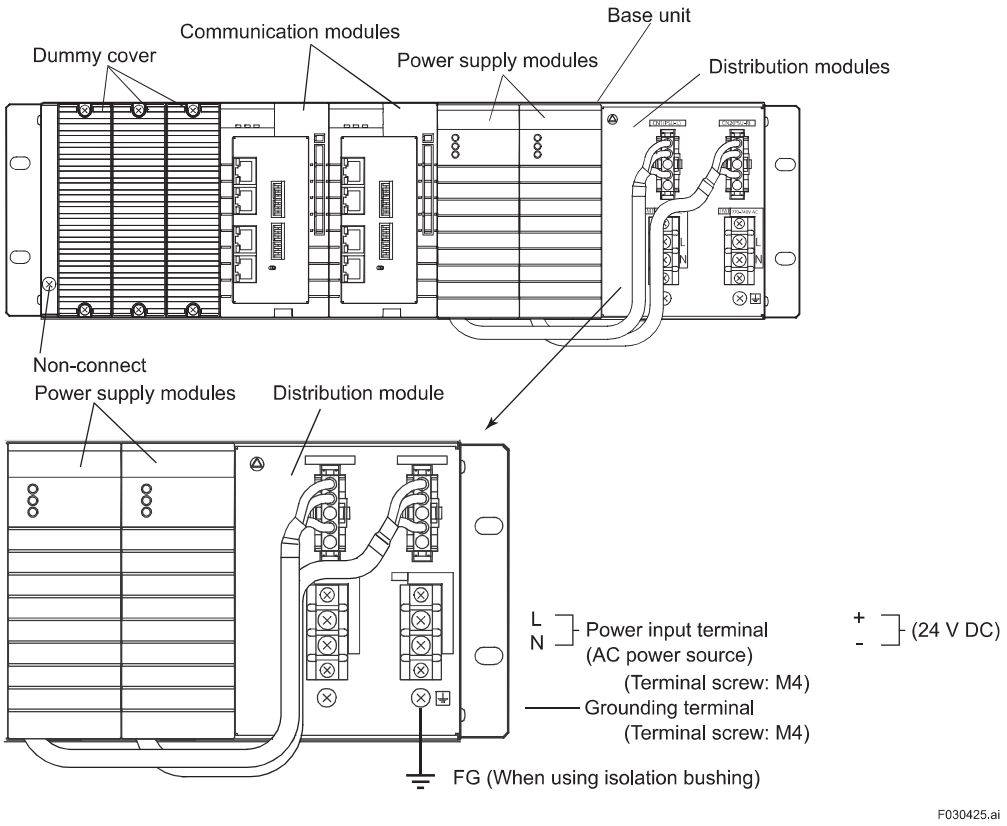


Figure AW810D Wide Area Communication Router Power Cable Connection

IMPORTANT

When power to the Wide Area Communication router is turned off, communications with the areas within the coverage of the Vnet/IP service are disabled. The service coverage area needs to be taken into consideration when designing a system to supply power to the Wide Area Communication router (e.g. providing an independent power source for the Wide Area Communication router).

SEA4D Analog Terminal Board

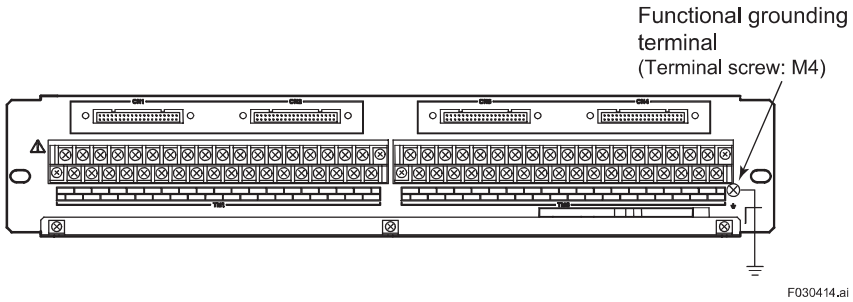


Figure SEA4D Ground Cable Connection

SED2D Digital Terminal Board

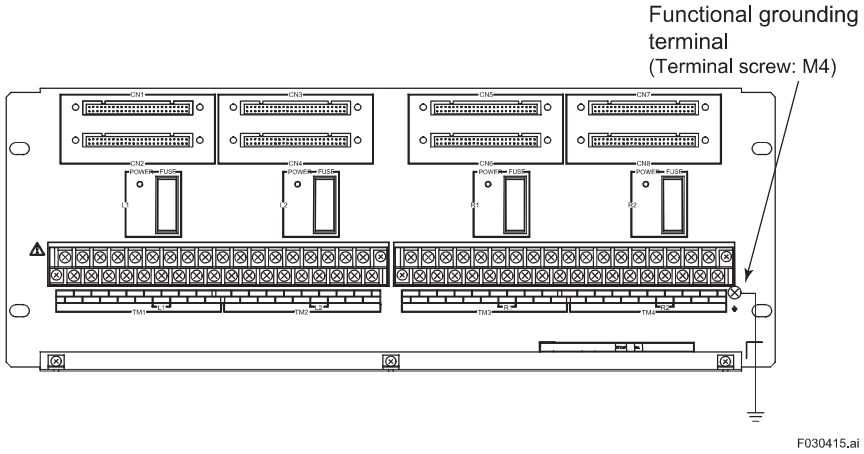


Figure SED2D Ground Cable Connection

SED3D Digital Terminal Board

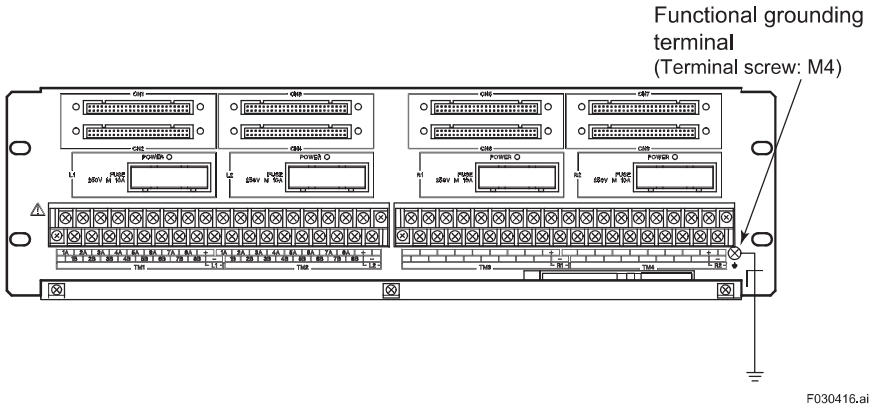


Figure SED3D Ground Cable Connection

SED4D Digital Terminal Board

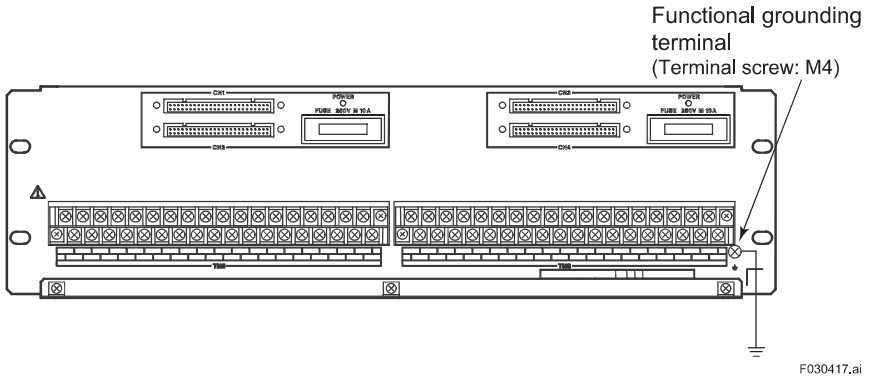


Figure SED4D Ground Cable Connection

SWD2D Digital Terminal Board

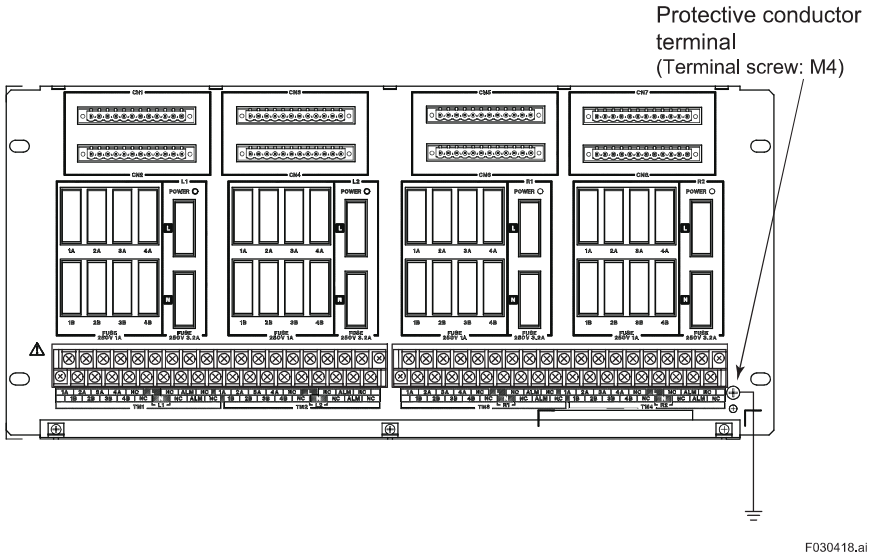


Figure SWD2D Ground Cable Connection

TIP

Terminal Boards such as A2BM4, SBA4D, SBT4D, SBR4D, SBD2D, SBD3D, SBD4D and S1BB4D don't have a grounding terminal.

SRM53D Relay Board for Digital Output

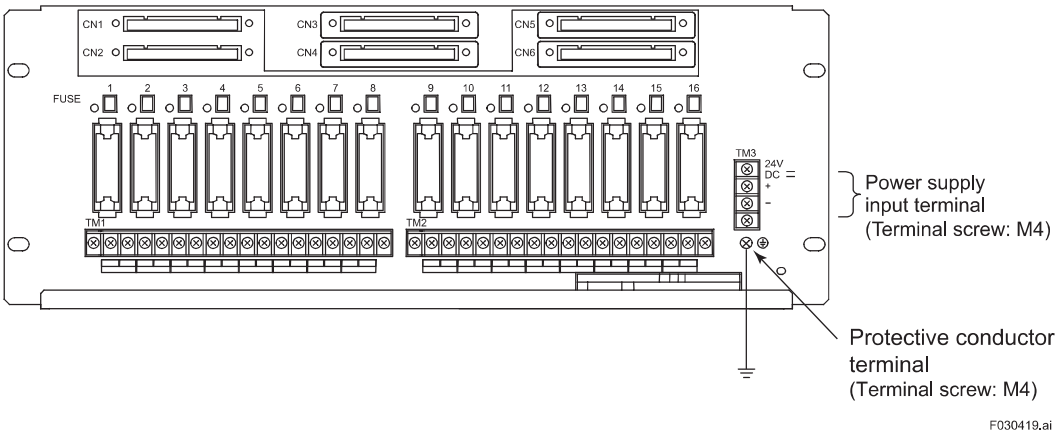


Figure SRM53D Ground Cable Connection

SRM54D Relay Board for Digital Output

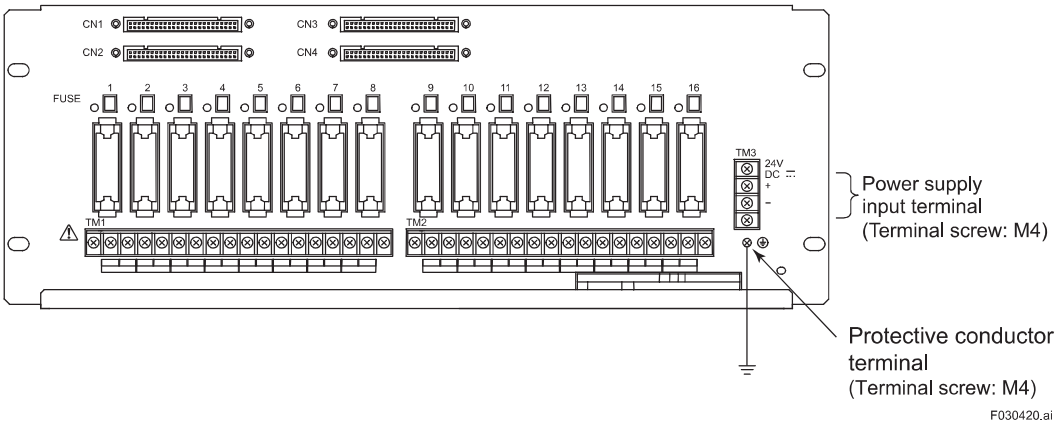


Figure SRM54D Ground Cable Connection

SBM54D Relay Board for Digital Output: DIN rail mount type

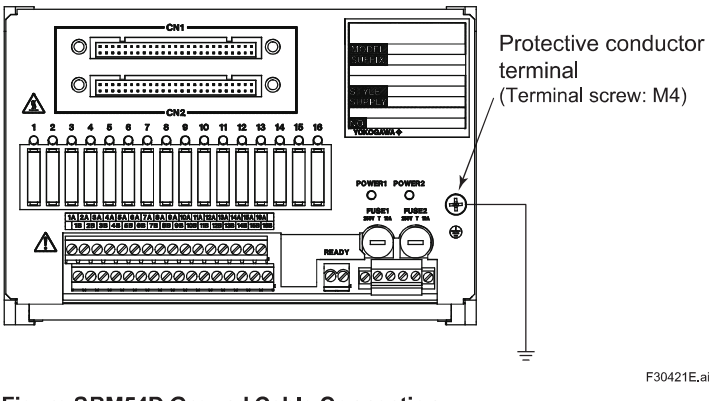


Figure SBM54D Ground Cable Connection

Example of System Cabinet Installation and Grounding Wiring

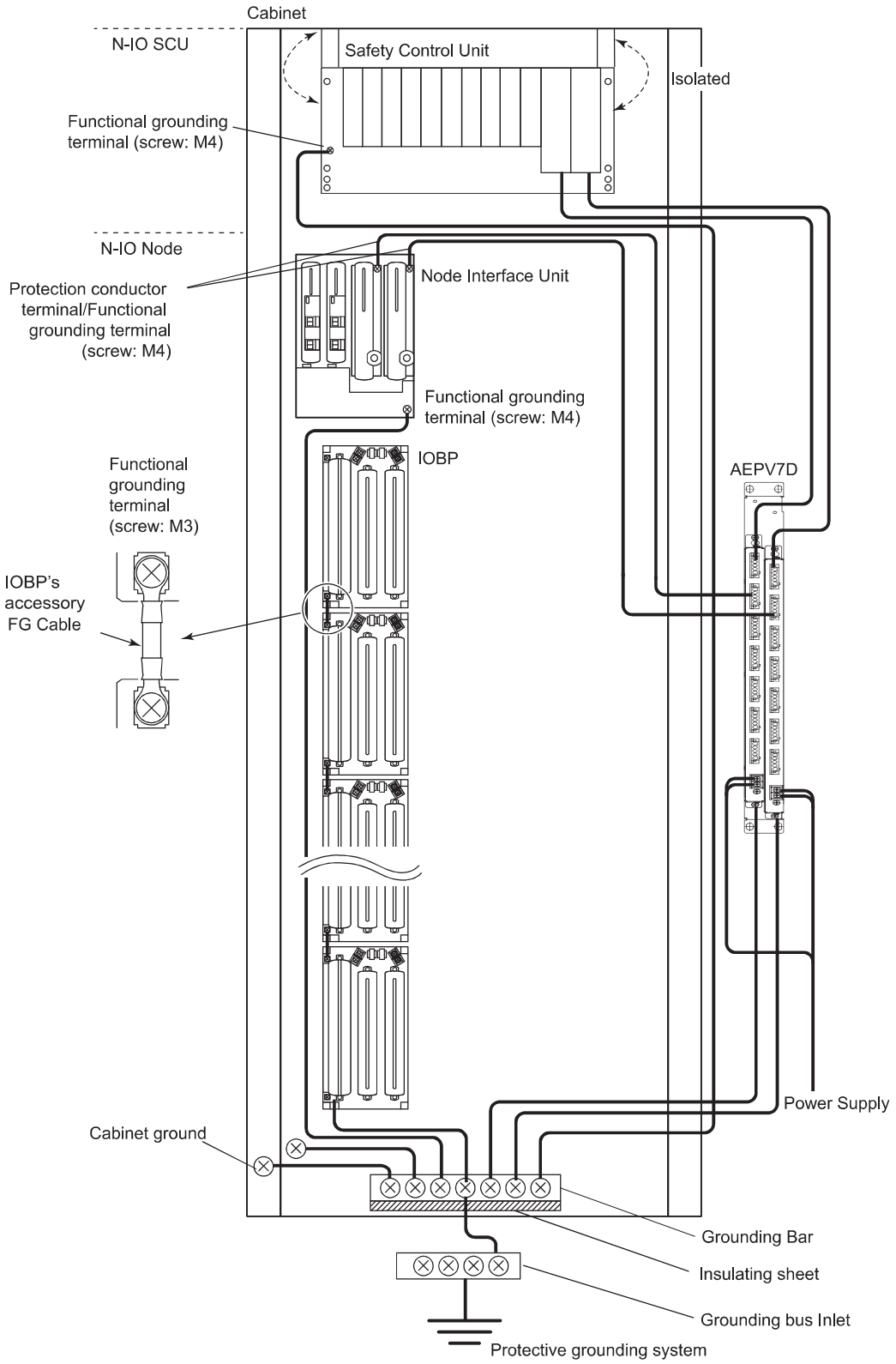


Figure N-IO system devices installation and grounding wiring (Cabinet)

WARNING

The wiring that will be intrinsic safety circuits must be installed so that they are electrically separated from the wiring of non-intrinsic safety circuits, including the in-cabinet wiring. Install the wiring according to the IEC 60079-14 standards or the requirements for explosion-proof wiring of the country where the system is used.

Example of Junction Box Installation and Grounding Wiring

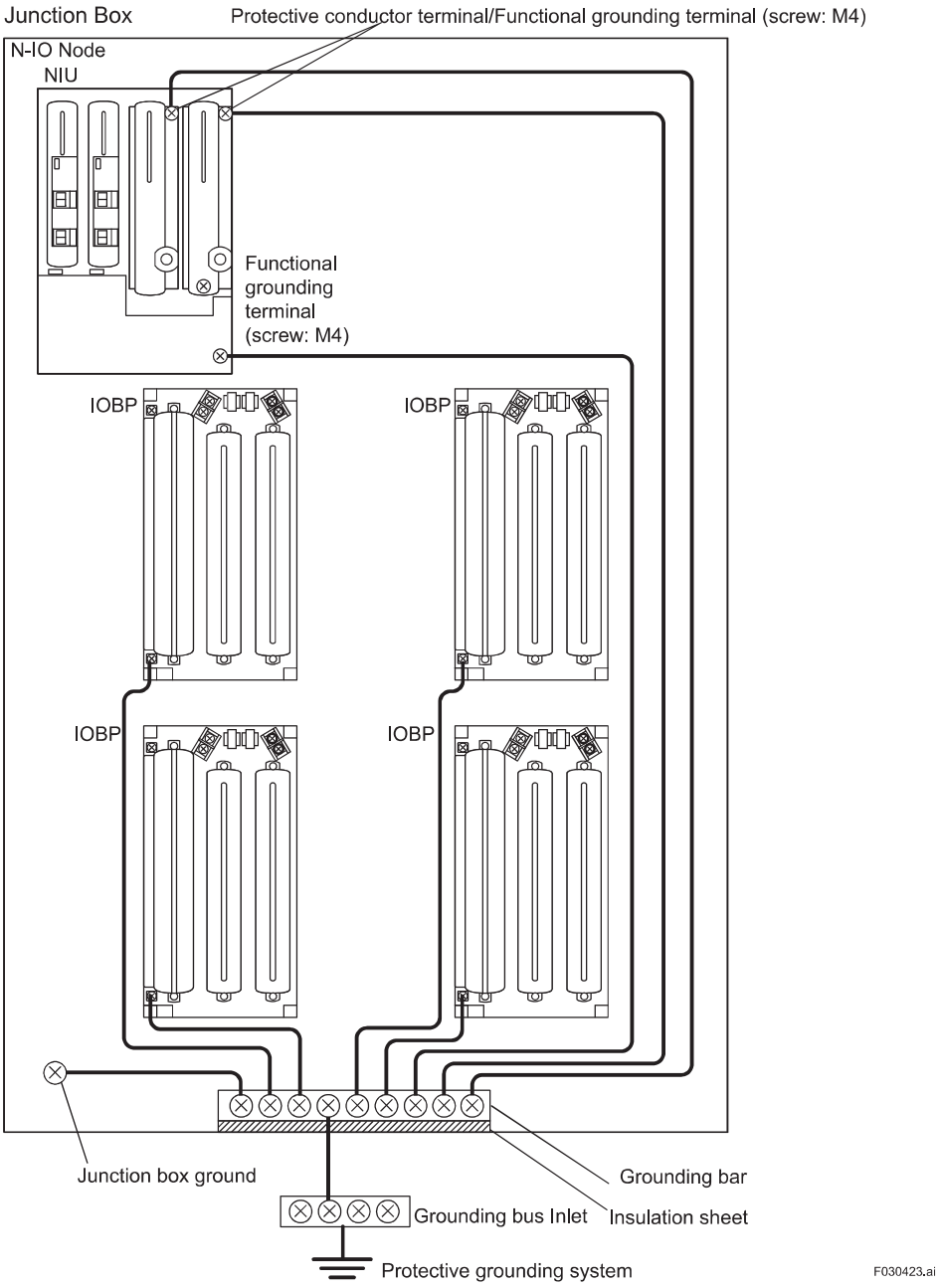
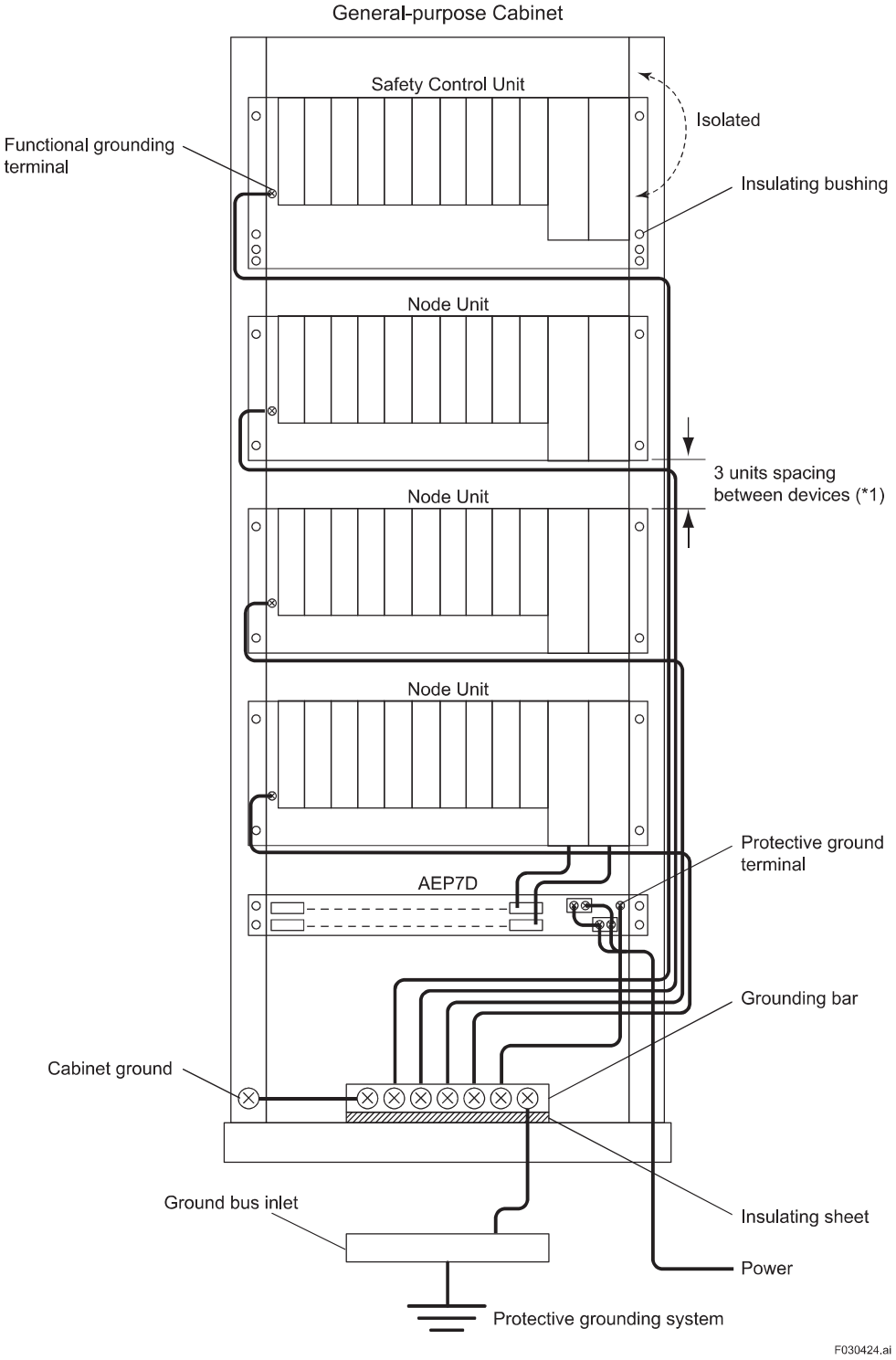


Figure Example of N-IO Node devices Installation and grounding wiring

19-inch Rack-mount Devices and Wiring (For FIO)

An example of wiring when SCU, Node Unit, ANB10 or ANB11 is mounted to a general-purpose cabinet in the following:



*1: Keep a space of 3U or more for heat radiation.

Figure 19-inch Rack-mount Devices and Wiring

3.5 Connecting Signal Cable

The terminal blocks or connectors of I/O modules are the interface of the field signals. When connecting the field signals to I/O modules via a dedicated cable and a terminal board, the terminal board becomes the interface of the field signals.

CAUTION

Do not ground the secondary side of the field power supply connected to the digital input module SDV144 style code S1 to S3.

Process I/O Signal Connection

- Power, control bus, and signal cables must be separately laid. Avoid laying them in parallel.
- In case of using multicore cables for field wiring, do not share one multicore cable with I/O modules of different voltage types (i.e. 48 V DC and 24 V DC).
  48 V DC: SDV53A
  24 V DC: SDV144, SDV521, SDV531, SDV541
- The use of group-shielded twisted-pair cables is recommended for analog signal input specifically in order to prevent induction noise. A twisted-pair cable pitch of 50 mm or less should be used and the shielded cables must be grounded.
- The use of twisted-pair cables is also recommended for digital signals.
- The twisted-pair cable has the following advantages over a solid wire:
  - More flexible for easy curving and cabling in limited spaces.
  - With good contact and durable in using a solderless contact.
- Signal cables must be clamped so that their weight does not affect terminals.
- Use solderless lug or pressure clamp terminal contact when process I/O signals are connected with terminals.
- Be careful when laying cables so as not to place excessive force on the cables.
- Field wiring to the each channel of the terminal board shall be connected independently, and shall not be shared with other channels by crossover wiring.

When mixing AI and DO in the same multi-core cable (N-IO I/O Unit)

When mixing analog input (AI) signal and digital output (DO) signal in the same multi-core cable, take the following influence from DO pulse diagnostics or ON/OFF operation into consideration.

- The accuracy for Analog input function may be worse by several tens of µA depending on the type, length of a cable and DO load current.
- A delay may occur in updating the HART event.

Solderless Lug

CAUTION

- Use the solderless contact with an insulation covering.
- Use the solderless contact and crimp tools of the same manufacturer.
- Use correct-size crimp tools according to cable sizes.

Pressure Clamp Terminal

CAUTION

- The ProSafe-RS uses pressure clamp terminals for signal connections to the I/O modules.
- For the cable connection with a sleeve attached, use a sleeve and a clamp tool from the same manufacturer.
- Use a clamp tool suitable for the cable size.
- When the door is attached or detached for cable connection, be sure to then OFF the power of the main unit before connecting or disconnecting a cable.

Spring Clamp Terminal

CAUTION

- The ProSafe-RS uses a spring clamp terminal for signal connection of N-IO.
- For cable connection with a sleeve attached, use a sleeve and a clamp tool from the same manufacturer.
- Use a clamp tool which suits the cable thickness.

Channel Fuse

CAUTION

Due to the short circuit between the input channel of a digital input module and the ground, the protection fuse mounted in front of the module may be blown up. To avoid the blow of the protection fuse, it is recommended to use a fuse (50 mA, fast-blow type) to each input channel. This important notice is applied for digital input module SDV144 style code S1 to S3.

Signal Cable Termination

Solderless Lug

- Solderless lug specifications
  The specifications for solderless lugs are determined by the nominal cross sectional area of the power cable for which lugs are used, lug screws, terminal dimensions, and the like.

Table Solderless Lug Dimensions

Cable nominal cross sectional area (mm^2)	Screw used (mm)	Hole diameter (mm)	Lug outside diameter (mm)	Lug length (mm)	Insulation covering inside diameter (mm)	Dimension "C" (mm)	Remarks
1.25	3.5 (*1)	3.7 or more	6.8 or less	Approx. 21	3.6 or more	4.0 or more	
2.0	3.5 (*1)	3.7 or more	6.8 or less	Approx. 21	3.6 or more	4.0 or more	
1.25	4 (*2)	4.3 or more	8.2 or less	Approx. 21	3.6 or more	7.0 or more	
2.0	4 (*2)	4.3 or more	8.7 or less	Approx. 21	4.3 or more	7.1 or more	
5.5	4 (*2)	4.3 or more	8.7 or less	Approx. 25	5.8 or more	5.9 or more	Only SED2D

*1: Recommended tightening torque is 0.8 N•m.
*2: Recommended tightening torque is 1.2 N•m.

CAUTION

- Always use solderless lugs with insulated covering.
- Always use solderless lugs and crimp-on tool manufactured by the same manufacturer.
- The crimp-on tool must be matched to the wire thickness.

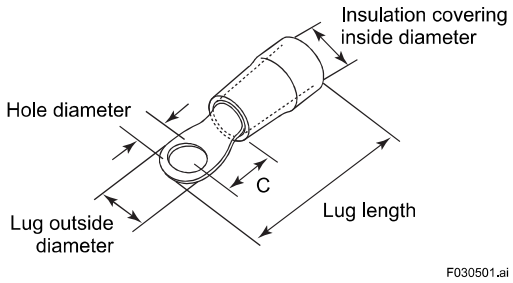


Figure Solderless Lug

Pressure Clamp Terminal (for Pressure Clamp Terminal Block) (for terminal block, terminal board, and relay board)

- Terminal processing
  When connecting the process I/O signal to the pressure clamp terminal of an I/O module, strip the cable coating (without a sleeve) or attach a sleeve to the cable. The following shows the length of the coating stripped for cases when a sleeve is not used and when it is used.

SBT4D, STA4S, STA4D, STB4S, and STB4D

Table Without a sleeve

Cable thickness (mm^2)	Peel-off Length (mm)
0.5 to 2 (AWG20 to 14)	11

When using a sleeve, a cable must have terminal processing in accordance with the instructions of the sleevemanufacturer. Use one of the following sleeves is recommended.

Sleeve without insulating cover (DIN 46 228/1) Sleeve with insulating cover (DIN 46 228/4)

Table With a sleeve

Cable nominal cross sectional area (mm^2)	When using a sleeve with insulating cover			When using a sleeve without insulating cover	
	Peel-off length (mm)	Sleeve dimensions		Peel-off length (mm)	Sleeve dimensions
		Total length (mm)	Contact section length (mm)		Total length (mm)
0.5	12	16	10	10	10
0.75	12	16	10	10	10
1	12	16	10	10	10
1.25 to 1.5	12	16	10	10	10

A2BM4, SBR4D, SBA4D, SBD2D, SBD3D, SBD4D, SBM54D, and S1BB4D

Table Without a sleeve

Cable thickness (mm^2)	Peel-off length (mm)
0.5 to 2.5 (AWG20 to 14)	7

When using a sleeve, a cable must have terminal processing in accordance with the instructions of the sleevemanufacturer. Use one of the following sleeves is recommended.

Sleeve without insulating cover (DIN 46 228/1) Sleeve with insulating cover (DIN 46 228/4)

Table With a sleeve

Cable nominal cross sectional area (mm^2)	When using a sleeve with insulating cover			When using a sleeve without insulating cover	
	Peel-off length (mm)	Sleeve dimensions		Peel-off length (mm)	Sleeve dimensions
		Total length (mm)	Contact section length (mm)		Total length (mm)
0.5	10	14	8	6	6
0.75	10	14	8	6	6
1	10	14	8	6	6
1.25 to 1.5	10	14	8	7	7
2.5	10	14	8	7	7

Pressure Clamp Terminal, Spring Clamp Terminal (for N-IO Node)

At the end of the signal cables to the following applicable interface, provide the following cable termination:

Table Applicable Interface

Products	Models	Interface	Sleeve Normal cross sectional area (mm^2)
Node Interface Unit	S2NN30D	External alarm input terminal	0.5 ~ 2.5
I/O Unit	S2BN1D	I/O signal terminal (pressure clamp terminal)	0.5 ~ 2.5
		I/O signal terminal (spring clamp terminal)	0.5 ~ 1.5
	S2BN5D	I/O signal terminal (spring clamp terminal)	0.5 ~ 1.5

- When using a sleeve
  At the cable end, peel off the coating and attach a sleeve. The specifications of the sleeve differ, depending on the cable thickness. Provide cable termination according to the following figure and tables:

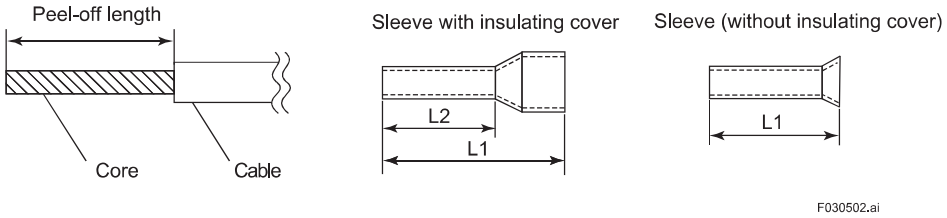


Figure Cable termination (for pressure clamp terminals)

When using a sleeve, a cable must have terminal processing in accordance with the instructions of the sleevemanufacturer. Use one of the following sleeves is recommended.

Sleeve without insulating cover (DIN 46 228/1) Sleeve with insulating cover (DIN 46 228/4)

Table When sleeves with insulating cover are used

Cable nominal cross sectional area (mm^2)	Peel-off length (mm)	Sleeve dimensions (mm)	
		L1	L2
0.5	10	14	8
0.75	10	14	8
1.0	10	14	8
1.5	10	14	8
2.5	10	14	8

Table When sleeves without insulating cover are used

Cable nominal cross sectional area (mm^2)	Peel-off length (mm)	Sleeve dimensions (mm)
		L1
0.5	6	6
0.75	6	6
1.0	6	6
1.5	7	7
2.5	7	7

- When not using a sleeve

Terminal	Cable nominal cross sectional area (mm^2)	Peel-off length (mm)
pressure clamp terminal	0.5 to 2.5 (AWG20 to 14)	8
spring clamp terminal	0.5 to 2.5 (AWG20 to 14)	7

- For I/O Unit Model S2BN4D
  The pressure clamp terminal is on the MTL I.S. barrier. A cable must be prepared separately. Cable specification of field signal depends on the requirements specification of MTL's I.S. barriers. Refer to the instruction manual of I.S. barriers provided by the vendor.

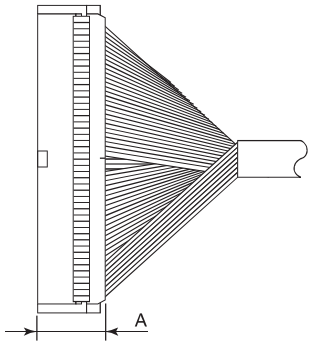
MIL Connector Cover SCCC0☐

SCCC01 (for flat ribbon cables)

When using the SCCC01, use connectors conforming to the following requirements:

- MIL-C-83503-compliant Connector
- Connector with one pin that prevents improper insertion (both 40- and 50-pin connectors)
- The following dimensions must be satisfied:

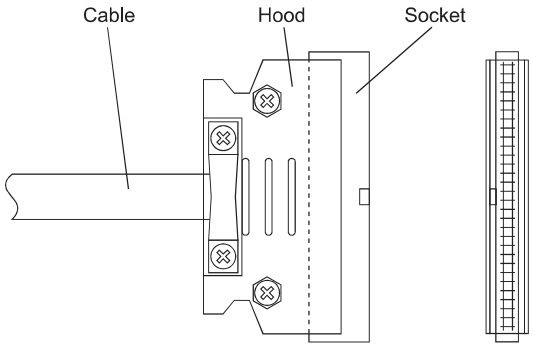
  16.5 mm – B ≤ A ≤ 15.8 mm
  where, A = connector height
  B = engagement length



F030503.ai

Note: For the engagement length, contact the connector manufacturer.

SCCC02 (for separate cables)



F030504.ai

Cables and connectors that can be used for the SCCC02 are listed in the table below.

Manufacturer	Manufacturer's Model	Product Name	Remarks
Japan Aviation Electronics Industry, Limited	PS-D4C50N	Socket	
	PS-HD50	Hood	
	PS-SF-C1-1	Contact	AWG24 to AWG22
Hitachi Cable, Ltd.	UL 2464SB 25P x 22AWG	Cable	

Connecting Signal Cables to Terminals (for FIO)

Connecting to Pressure-clamp Terminal

1. Loosen the cable connecting terminal screw.
2. Strip the cable coating (without a sleeve) or attach a sleeve to the cable, then insert the tip of the cable into the connecting section of the pressure clamp terminal.
3. Fasten the screw using the special tool (a screwdriver conforming to the DIN 5264B standard with a tip width of 0.6 mm and a shaft diameter of 3.5 mm) with a fastening torque of 0.5 N·m.

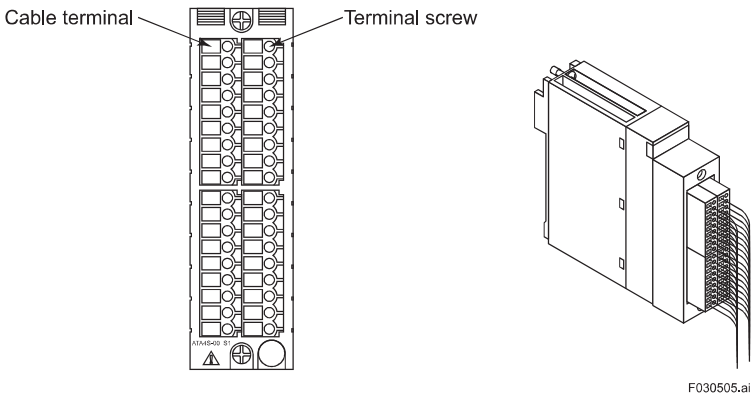


Figure Connecting Signal Cable to Terminal

IMPORTANT

Do not use non-standard signal cables or sleeves. Otherwise improper connection may result.

Be sure to remove the cable sheath just as much as specified, fit the sleeve, and clamp the cable firmly to the terminal.

S2SC70S/S2SC70D/SSC60S/SSC60D/SSC50S/SSC50D/SSC57S/SSC57D and SNB10D Cable Connections

The following shows SNB10D unit cable connections.

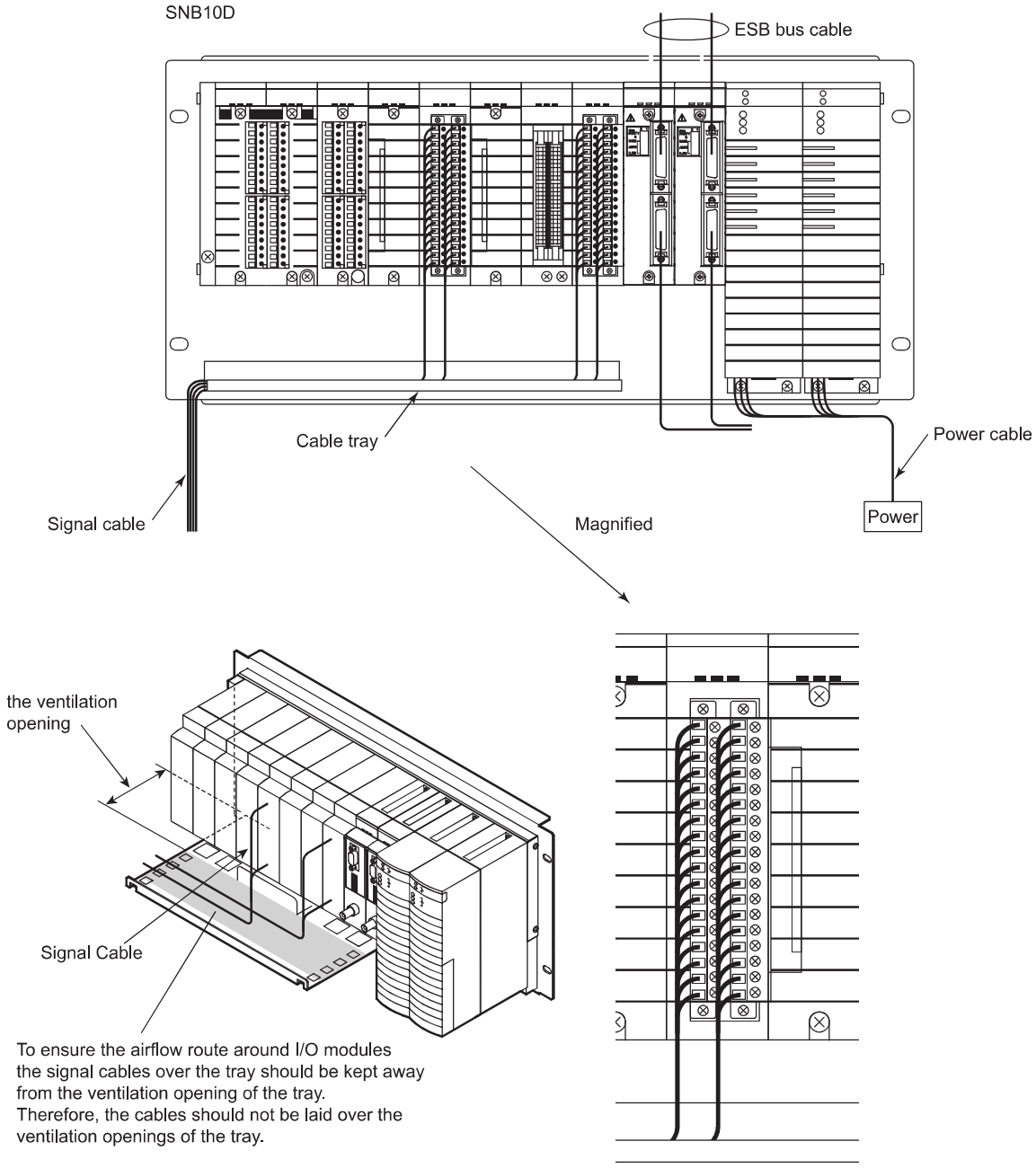


Figure SNB10D Unit Cable Connections

Signal Cabling

IMPORTANT

The signal cable for the top node unit (NU) must be wired at the innermost part in the field control area as the figure shows.

When fixing cables to a clamp, allow enough space so that the cards can be maintained.

Bind the bottom cables to the clamp bar on the channel base.

- Push in the signal cables for the top NU as far as they will go.

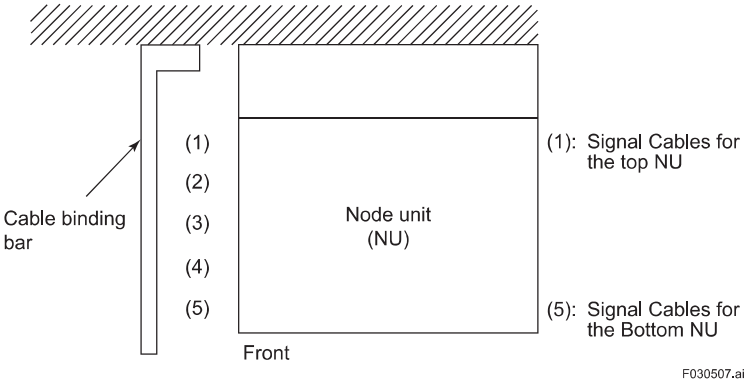


Figure Signal Cabling

I/O Module with Signal Cable Interface Adapter Cabling

When connecting a dedicated cable to an I/O module, ensure to keep the minimum bending radius of the cable.
Place the cable in front of the separator on the cable tray for ventilation.

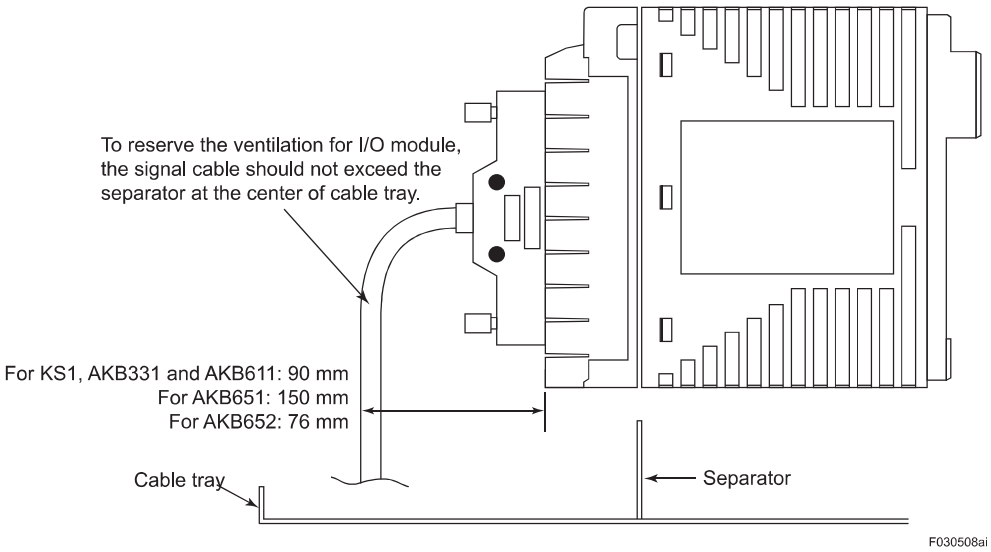


Figure I/O Module with Signal Cable Interface Adapter Cabling

Connecting Signal Cables to Terminals (for N-IO)

Connecting cables to pressure clamp terminals (S2BN1D-□1□□□)

Follow these steps to connect cables to pressure clamp terminals:

1. Open the cover of the terminal block of the base plate for N-IO I/O.
2. Confirming the cable polarity, insert the cable to the pressure clamp terminal. Tighten the screw using the special tool (a screwdriver conforming to the DIN 5264B standard a tip width of 0.6 mm and a shaft diameter of 3.5 mm) with a fastening torque of 0.5 N·m.
3. Pull the cable gently to check that it is fixed securely.
4. Close the cover of the terminal block of the base plate for N-IO I/O.

Connecting cables to spring clamp terminals (S2BN1D-□2□□□)

Follow these steps to connect cables to spring clamp terminals:

1. Open the cover of the terminal block of the base plate for N-IO I/O.
2. Pressingly expand the spring clamp terminal with a flat-blade screwdriver.
3. Insert a cable without pulling out the screwdriver.
4. Pull out the flat-blade screwdriver.
5. Pull the cable gently to check that it is fixed securely.
6. Close the cover of the terminal block of the base plate for N-IO I/O.

N-IO Signal Cabling

IMPORTANT

The signal cable for the top IOBP must be wired at the innermost part in the field control area as the figure shows.
When fixing cables to a clamp, allow enough space so that the cards can be maintained.

Push in the signal cables for the top IOBP as far as they will go.

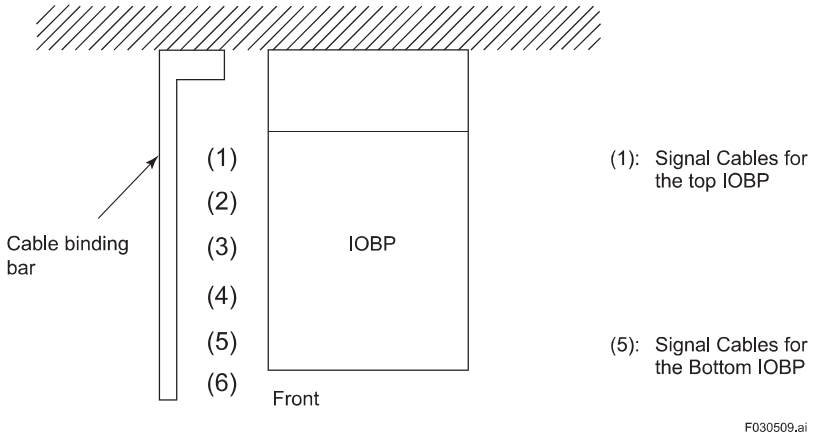
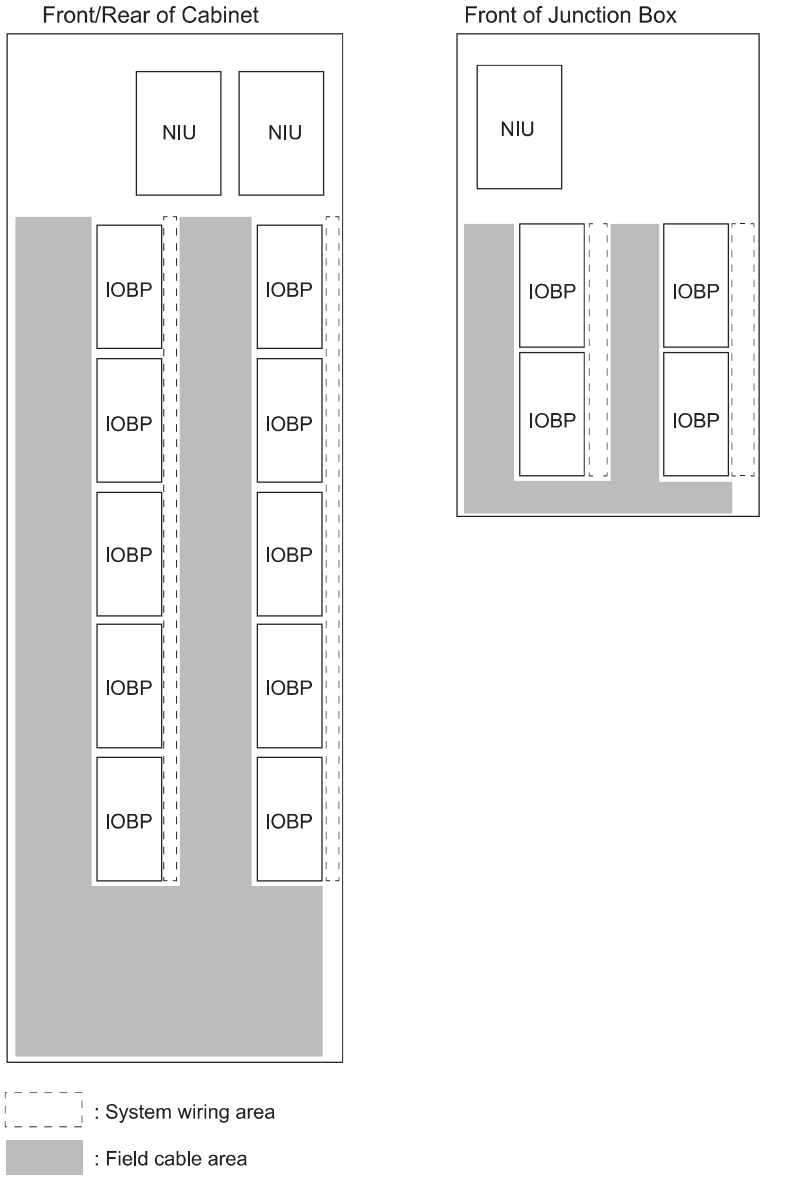


Figure Cabling

Routing Signal Cables (for N-IO)

Field Cable Area

Signal cables from the field enter the Cabinet at the bottom and connected to individual IOBP units in the routes shown in Figure below.



NIU: Node Interface Unit
IOBP: N-IO I/O Base Plate

Figure Area for Signal Cable from Field

Example of Node Interface Unit and I/O Unit cable wiring (Cabinet)

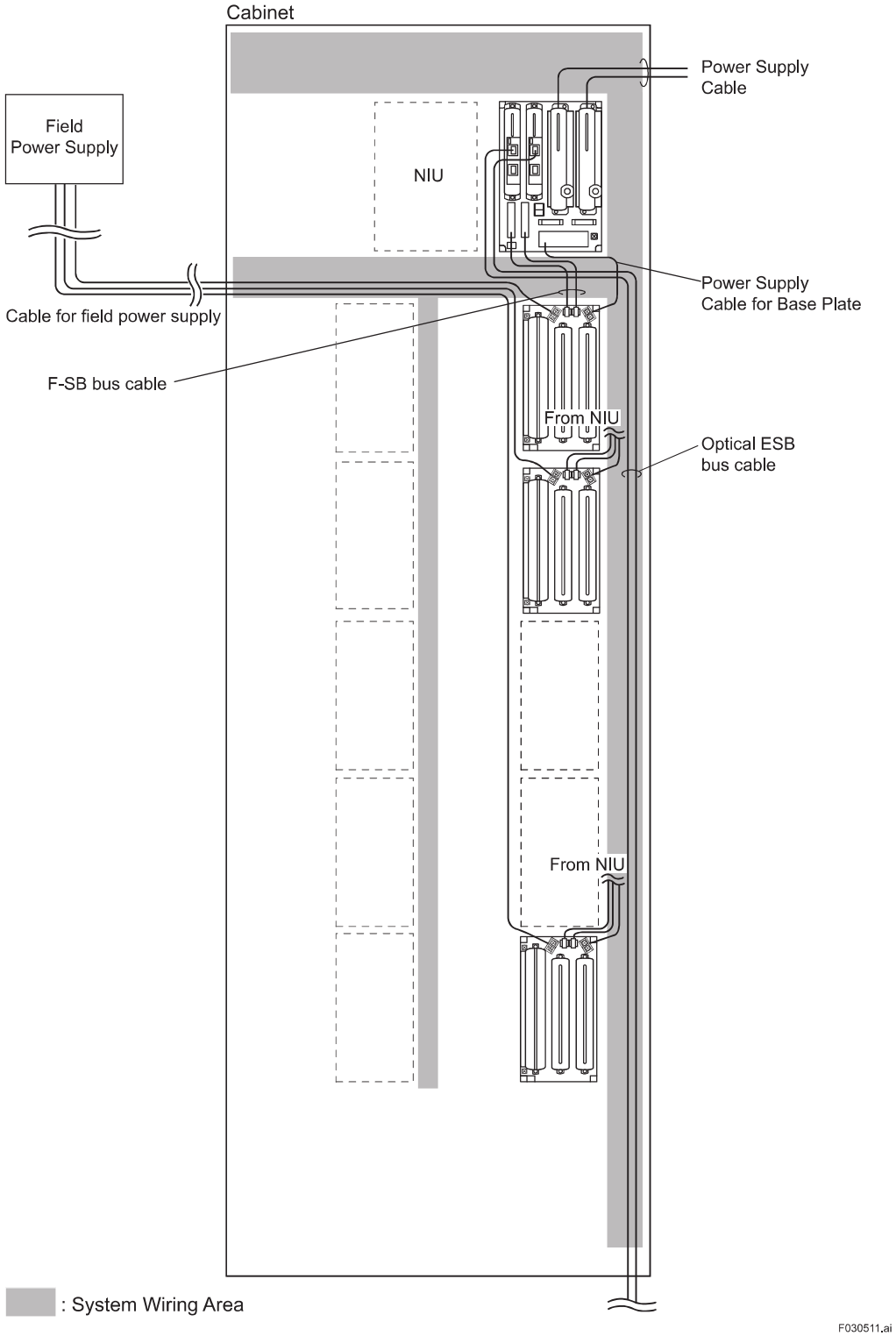
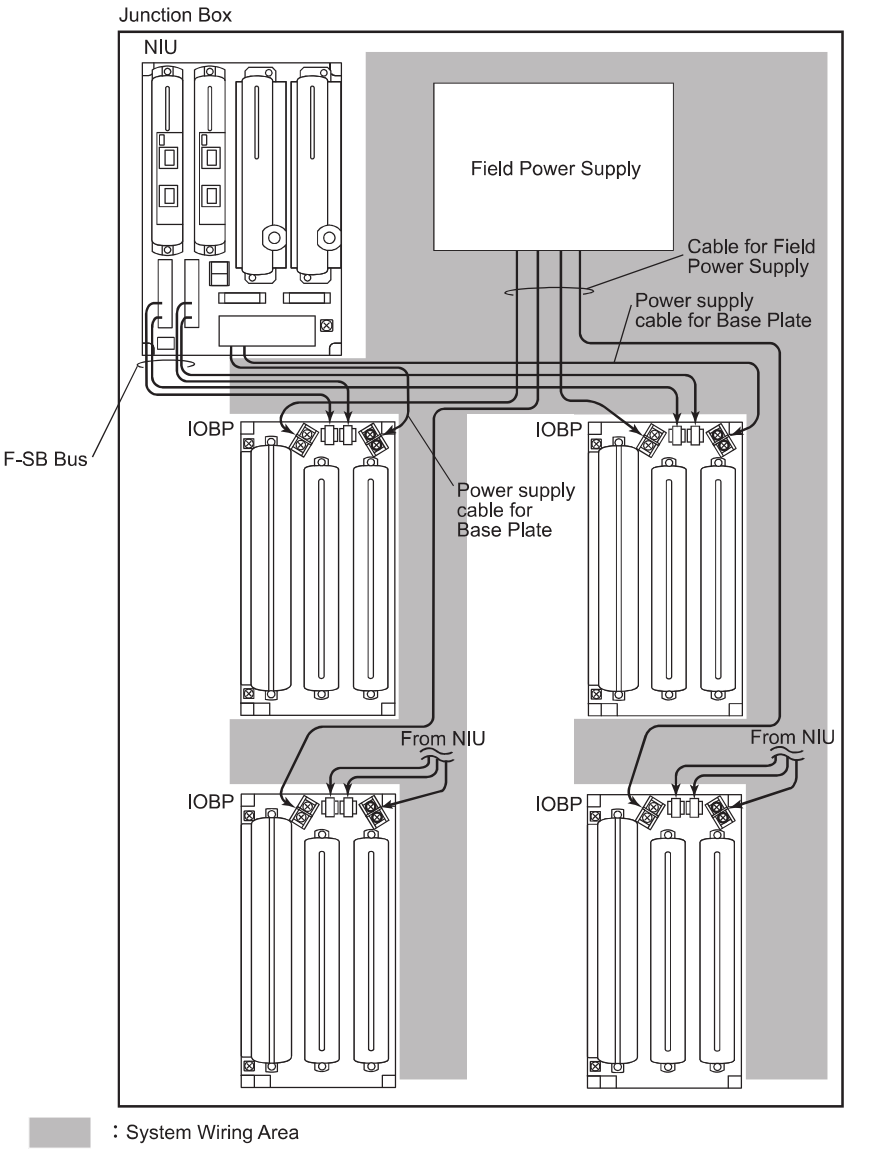


Figure Example of Node Interface Unit and I/O Unit Cable Wiring (Cabinet)

Example of Node Interface Unit and I/O Unit Cable Wiring (Junction Box)



IOBP: N-IO I/O Unit

Figure Example of Node Interface Unit and I/O Unit Cable Wiring (Junction Box)

WARNING

The wiring that will be intrinsic safety circuits must be installed so that they are electrically separated from the wiring of non-intrinsic safety circuits, including the in-cabinet wiring. Install the wiring according to the IEC 60079-14 standards or the requirements for explosion-proof wiring of the country where the system is used.

Connecting external alarm input terminal with Node Interface Unit

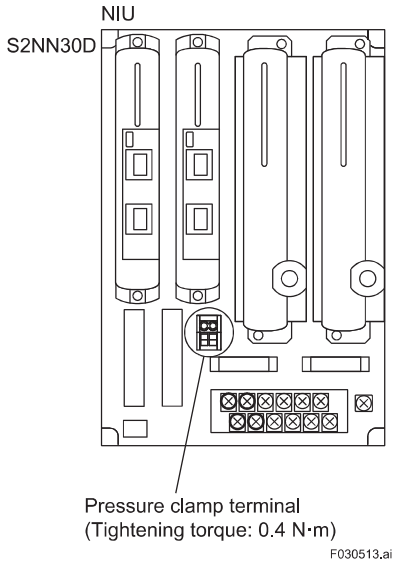


Figure Connecting external alarm input terminal with Node Interface Unit

3.6 Connecting Signal Cables to I/O Modules (for FIO)

3.6.1 Combination of I/O Modules and Terminal Blocks

A pressure clamp terminal block or signal cable interface adapter is available for field wiring, or MIL cables provided by the user may be used.

SEE ALSO For the terminal arrangement of the pressure clamp terminals and terminal board, and the pin arrangement of the MIL connector, refer to GS 32Q06J10-31E, GS 32S06J10-21E or GS 32S06J10-01E "Field Device Connection (for ProSafe-RS)."

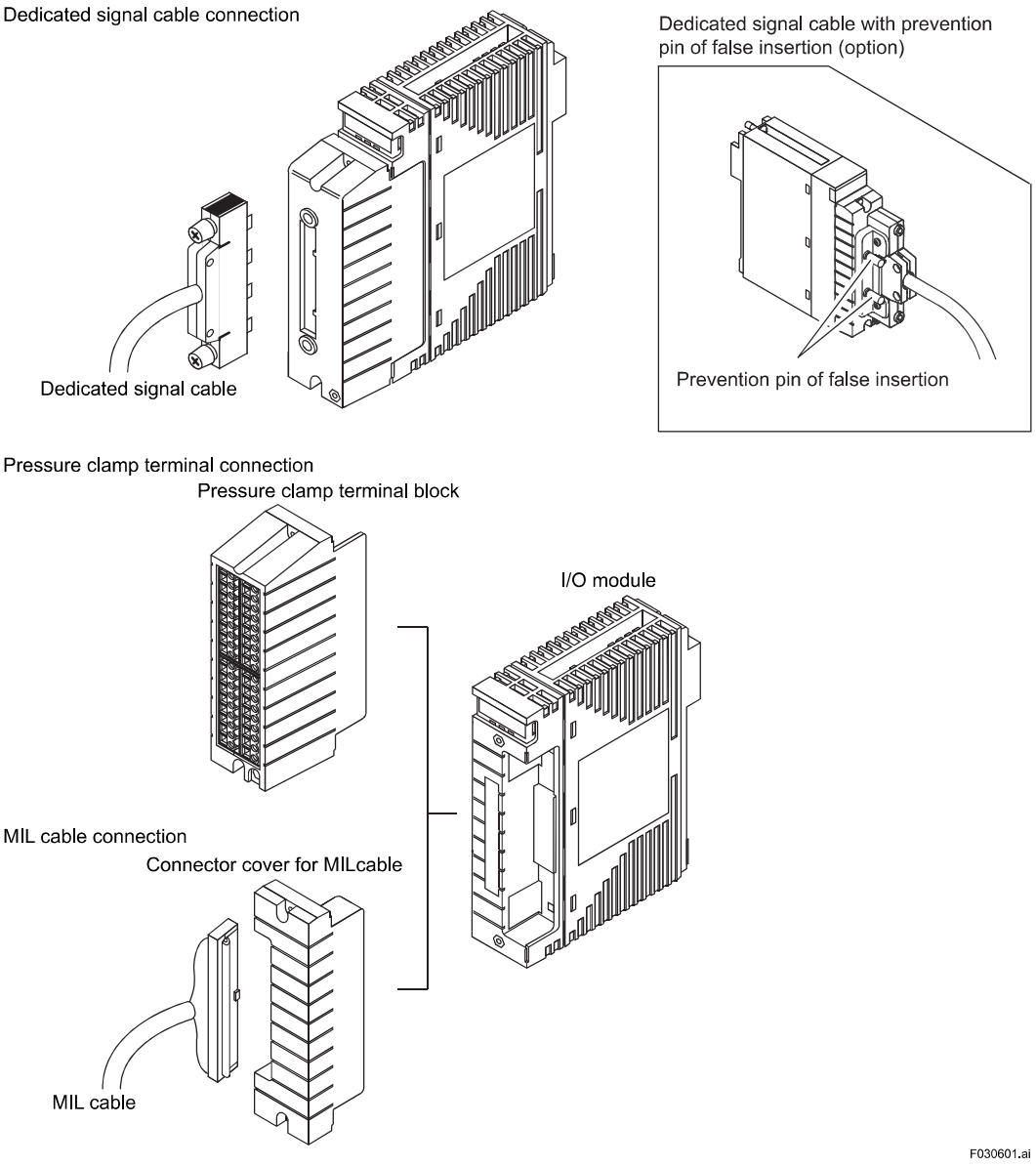


Figure Terminals for Field Wiring

3.6.2 Signal Cable Connections

The following table shows the signal cable connections.

Table Signal Cable Connections for I/O Modules (1/2)

Model	Name	I/O Channels per Module	Signal Connection			
			Pressure Clamp Terminal	MIL Cable	Yokogawa-specific Cable (*2)	
					No option code (*3)	Option code (*4)
Analog Input/Output Module						
SAI143-S53 SAI143-SE3	Analog input module (4 to 20 mA, Module isolation, General-purpose cables (*1))	16	X	X	–	
SAI143-S63 SAI143-SF3	Analog input module (4 to 20 mA, Module isolation, Yokogawa-specific cables (*2))	16	–	–	X (KS1-□□*B)	X (KS1-□□*B/ SAI143)
SAI143-H5□ SAI143-HE□	Analog input module (4 to 20 mA, HART Communication, Module isolation, General-purpose cables (*1))	16	X	X	–	
SAI143-H6□ SAI143-HF□	Analog input module (4 to20 mA, HART Communication, Module isolation, Yokogawa-specific cables (*2))	16	–	–	X (KS1-□□*B)	X (KS1-□□*B/ SAI143)
SAV144-S53 SAV144-SE3	Analog input module (1 to 5 V/1 to 10 V, Module isolation, General-purpose cables (*1))	16	X	X	–	
SAV144-S63 SAV144-SF3	Analog input module (1 to 5 V/1 to 10 V, Module isolation, Yokogawa-specific cables (*2))	16	–	–	X (KS1-□□*B)	X (KS1-□□*B/ SAV144)
SAT145-S□3	TC/mV Input module (Isolated Channels, Yokogawa-specific cables (*2))	16	–	–	X AKB331- M□□□)	X (AKB331- M□□□/SAT14)
SAR145-S□3	RTD Input Module (Isolated Channels, Yokogawa-specific cables (*2))	16	–	–	X AKB611- M□□□)	X (AKB611- M□□□/SAR14)
SAI533-H53 SAI533-HE3	Analog output module (4 to 20 mA, HART Communication Module isolation, General-purpose cables (*1))	8	X	X	–	
SAI533-H63 SAI533-HF3	Analog output module (4 to 20 mA, HART Communication Module isolation, Yokogawa-specific cables (*2))	8	–	–	X (KS1-□□*B)	X (KS1-□□*B/ SAI533)
Digital Input/Output Module						
SDV144-S5□ SDV144-SE□	Digital input module (no-voltage contact, Module isolation, General-purpose cables (*1))	16	X	X	–	
SDV144-S6□ SDV144-SF□	Digital input module (no-voltage contact, Module isolation, Yokogawa-specific cables (*2))	16	–	–	X (AKB331- M□□□)	X (AKB331- M□□□/ SDV144)
SDV521-S□□	Digital output module (24 V DC/2 A, Module isolation, Yokogawa-specific cables (*2))	4	–	–	X (AKB651- M□□□)	X (AKB651- M□□□/ SDV521)
SDV526-S33	Digital output module (100-120 V AC, Module isolation, Yokogawa-specific cables (*2))	4	–	–	X (AKB652- M□□□)	X (AKB652- M□□□/SDV526)
SDV531-S53 SDV531-SE3 SDV531-L5□ SDV531-LE□	Digital output module (24 V DC, Module isolation, General-purpose cables (*1))	8	X	X	–	

X: Can be connected. –: Cannot be connected.

*1: General-purpose cables are pressure clamp terminals and MIL cables.
*2: Yokogawa-specific cables are special cables for connecting input/output modules to terminal boards.
*3: If no option code is selected, a wrong connection to I/O modules with different signals cannot be avoided.
*4: If option codes associated with I/O modules are selected, a wrong connection to I/O modules with different signals can be avoided.

Table Signal Cable Connections for I/O Modules (2/2)

Model	Name	I/O Channels per Module	Signal Connection			
			Pressure Clamp Terminal	MIL Cable	Yokogawa-specific Cable (*2)	
					No option code (*3)	Option code (*4)
Digital Input/Output Module						
SDV531-S63 SDV531-SF3	Digital output module (24 V DC, Module isolation, Yokogawa-specific cables (*2))	8	–	–	X (AKB331-M□□□)	–
SDV531-L6□ SDV531-LF□	Digital output module (24 V DC, Module isolation, Yokogawa-specific cables (*2))	8	–	–	X (AKB331-M□□□) (AKB651-M□□□) (*7)	X (AKB331-M□□□/SDV53L) (AKB651-M□□□/DV53L)
SDV53A-S□3	Digital output module (48 V DC, Module isolation, Yokogawa-specific cables(*2))	8	–	–	X (AKB331-M□□□) (AKB651-M□□□) (*7)	X AKB331-M□□□/SDV53A) (AKB651-M□□□/DV53A)
SDV541-S5□ SDV541-SE□	Digital output module (24 V DC, Module isolation, General-purpose cables (*1))	16	X	X	–	
SDV541-S6□ SDV541-SF□	Digital output module (24 V DC, Module isolation, Yokogawa-specific cables (*2))	16	–	–	X (AKB331-M□□□) (AKB651-M□□□) (*7)	X (AKB331-M□□□/SDV541) (AKB651-M□□□/DV541)
Communications Module						
ALR111	Serial communication module (RS-232C, 2-port) (*6)	Two ports	–	–	X (D-Sub 9-pin connector) (*5)	
ALR121	Serial communication module (RS-422/RS-485, 2-port) (*6)	Two ports	–	–	X (M4-terminal block, 10 poles) (*5)	
ALE111	Ethernet communication module	One port	–	–	X (RJ-45) (*8)	
S2LP131	Fire and gas communication module	One port	–	–	X (RJ-45) (*9) (*10)	

X: Can be connected. –: Cannot be connected.
*1: General-purpose cables are pressure clamp terminals and MIL cables.
*2: Yokogawa-specific cables are special cables for connecting input/output modules to terminal boards.
*3: If no option code is selected, a wrong connection to I/O modules with different signals cannot be avoided.
*4: If option codes associated with I/O modules are selected, a wrong connection to I/O modules with different signals can be avoided.
*5: A Yokogawa-specific cable can be connected without using a terminal block.
*6: If optical ESB extended distance is longer than 5 km, ALR1□1 module for Modbus Slave cannot be mounted to I/O node.
*7: In case of connecting AKB651 to SDV531-L6□, SDV531-LF□, SDV53A-S□3, SDV541-S6□ and SDV541-SF□, Marine Standards are not certified.
*8: ALE111 is available from ProSafe-RS R3.02.00 or later with S2SC70□, SSC60□, SSC50□ or SSC57□.
*9: S2LP131 is available from R4.05.00 or later with S2SC70□.
*10: The cables and connectors must comply with PROFINET standards.

CAUTION

When connecting a Yokogawa-specific cable to an module, ensure to keep the minimum bending radius of the cable.

The minimum bending radius of the Yokogawa-specific cable is six-fold of the diameter of the cable.

3.6.3 Connecting Signal Cables to I/O Modules

Pressure Clamp Terminal

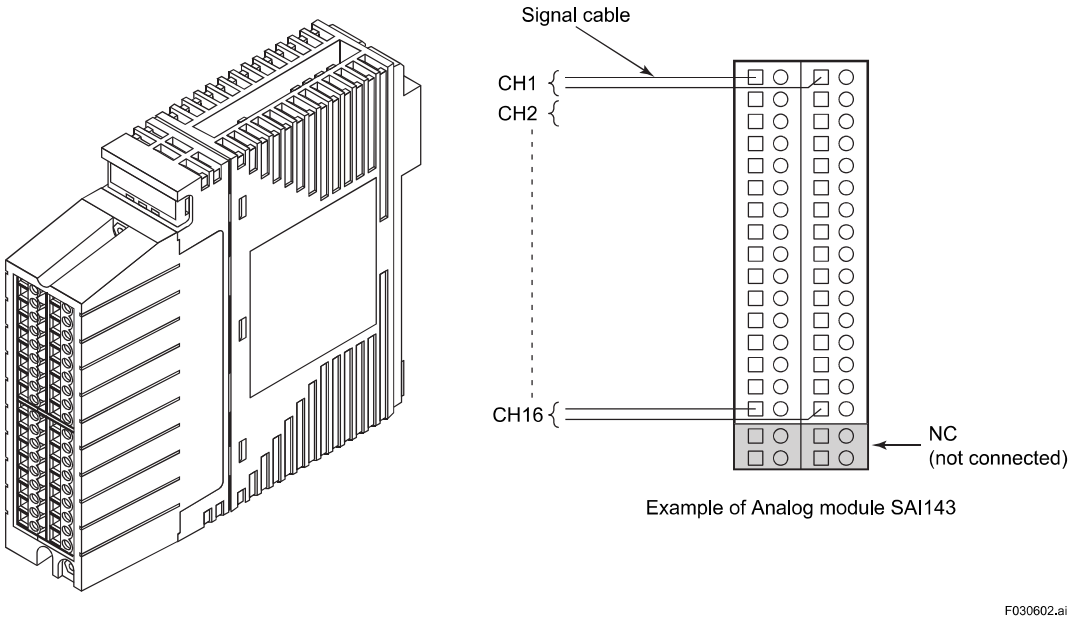


Figure I/O Module with Pressure Clamp Terminal

Dual-redundant Pressure Clamp Terminal

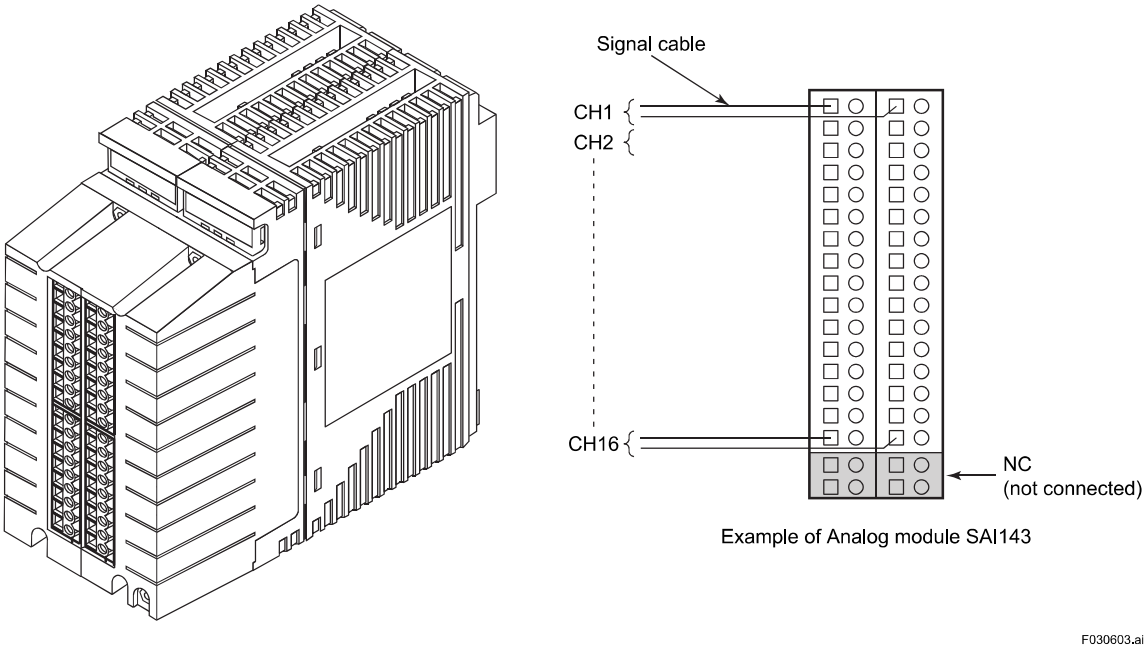


Figure I/O Module with Dual-redundant Pressure Clamp Terminal

Signal Cable Interface Adapter

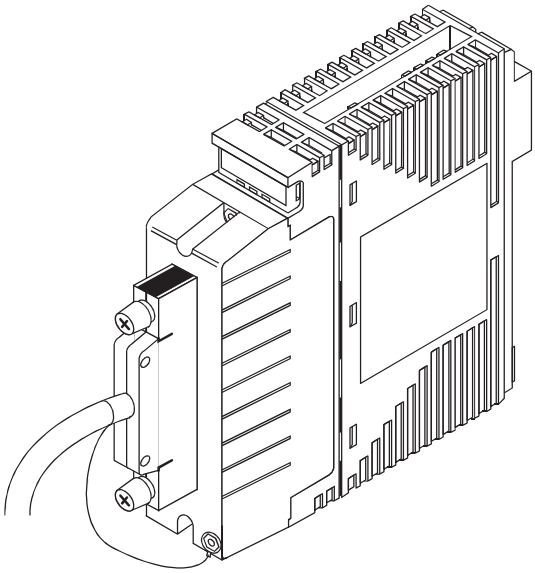


Figure I/O Module with Signal Cable Interface Adapter

The I/O modules are arranged in a dual-redundant configuration on the terminal board.

Connecting Signal Cables to Analog Input Modules

Signal cables are connected to different terminals according to the devices to be connected as shown below.

Table Analog Input Module Signal Names and Types of Input

Module	Signal Name	Type of Input	
		Connection : 2 wire (Setting : 2-wire input)	Connection : 3 wire/4wire(*2) (Setting : 4-wire input)
SAI143 (*1)	IN ☐ A	Two-wire transmitter input +	Current input -
	IN ☐ B	Two-wire transmitter input -	Current input +

☐ : Channel number
*1 : If the SAI143 module power are off or abnormal, the current input loop remains open. Do not use current signals with other receiving devices.
*2: Transmitter power supply is required separately.

Connecting I/O Module to Terminal Board

The I/O module with signal cable interface adapter can be connected to the terminal board using a Yokogawa-specific cable. Field signals are connected through the terminal board.

Example of Connection to SEA4D

SEA4D terminal board allows SAI143, SAV144 or SAI533 modules in both single and dual-redundant configurations.

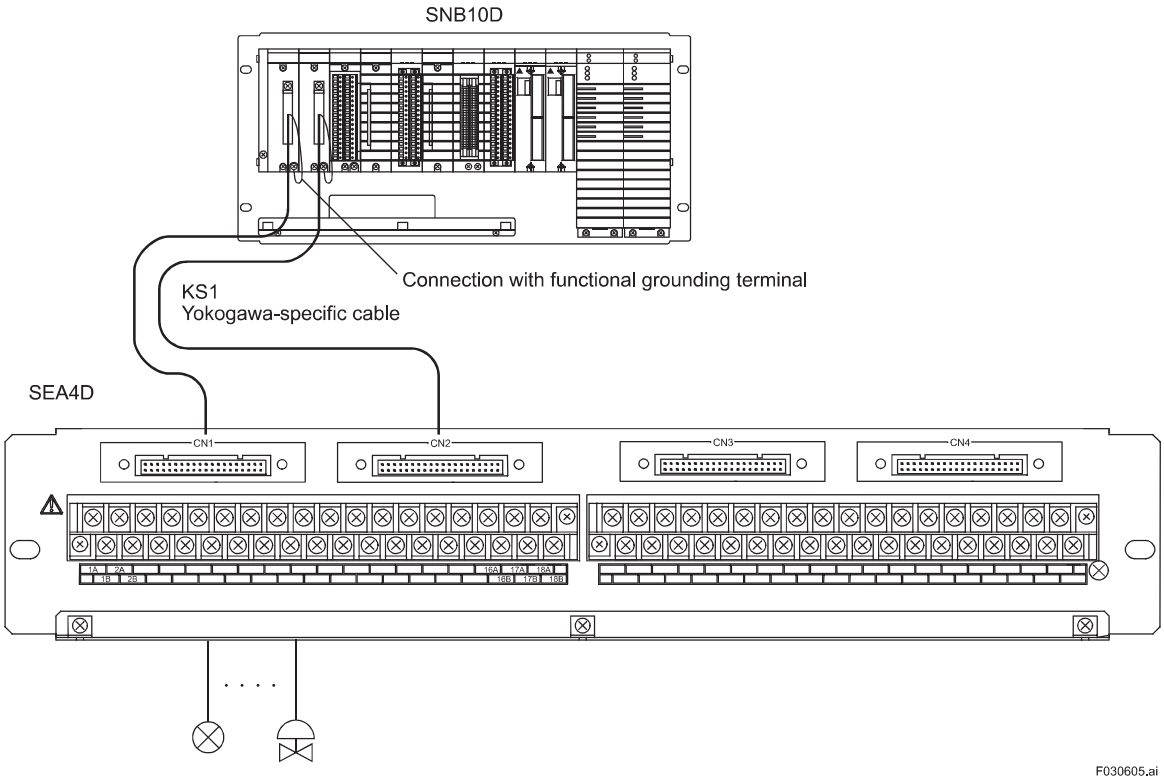


Figure Example of Terminal Board Connection with Dual-redundant I/O Module

SEE ALSO For the signal cable interface adapter model and the cable model for I/O modules, refer to GS 32Q06J10-31E, GS 32S06J10-21E or GS 32S06J10-01E “Field Device Connection (for ProSafe-RS).”

Example of Connection to SBA4D

SBA4D terminal board allows SAI143, SAV144 or SAI533 modules in both single and dual-redundant configurations.

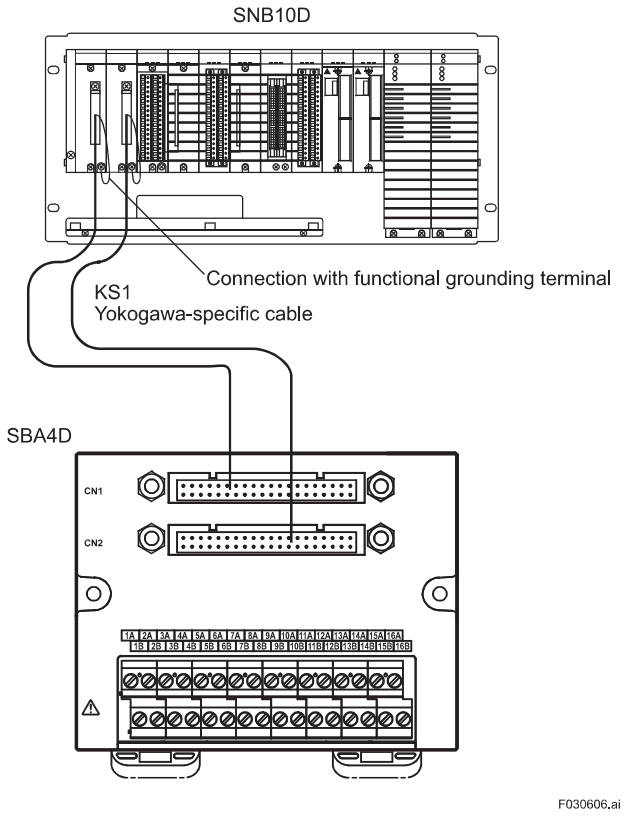


Figure Connecting Analog I/O Modules to SBA4D Terminal Board (for Dual-redundant Use)

Example of Connection to S1BB4D

S1BB4D terminal board allows SAI143 module in both single and dual-redundant configurations.

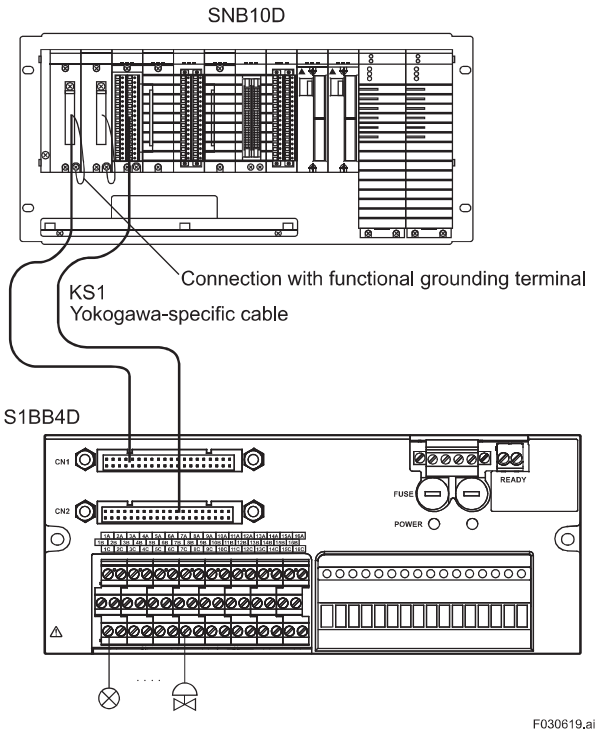


Figure Connecting Analog I/O Modules to S1BB4D Terminal Board (for Dual-redundant Use)

Example of Connection to SBT4D

SBT4D terminal board allows SAT145 modules in both single and dual-redundant configurations.

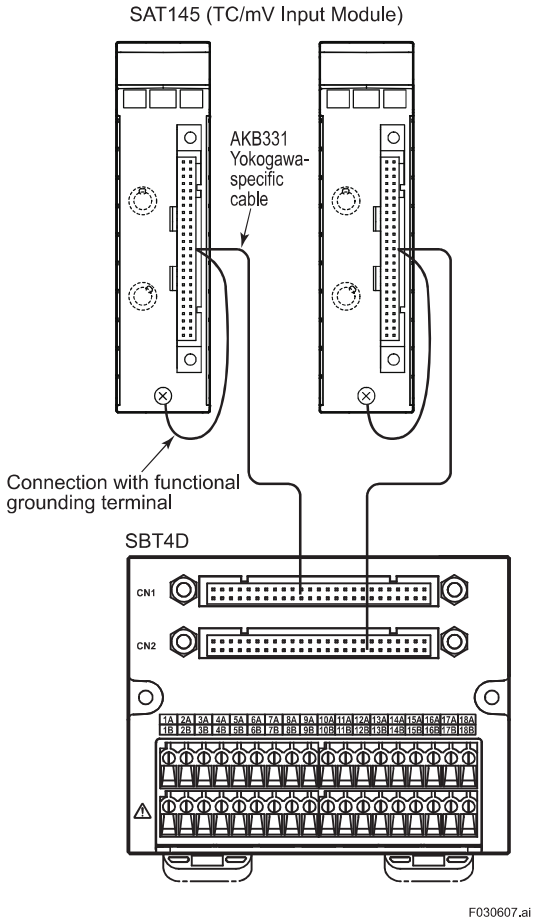


Figure Connecting TC/mV Input Modules to SBT4D Terminal Board (for Dual-redundant Use)

Example of Connection to SBR4D

SBR4D terminal board allows SAR145 modules in both single and dual-redundant configurations.

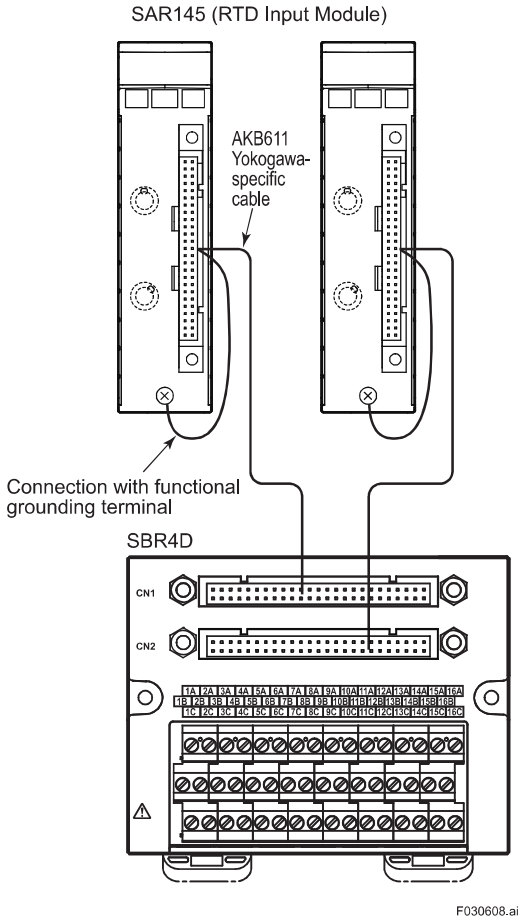


Figure Connecting RTD Input Modules to SBR4D Terminal Board (for Dual-redundant Use)

Example of Connection to SED2D

SED2D terminal board allows SDV521 modules in both single and dual-redundant configurations.

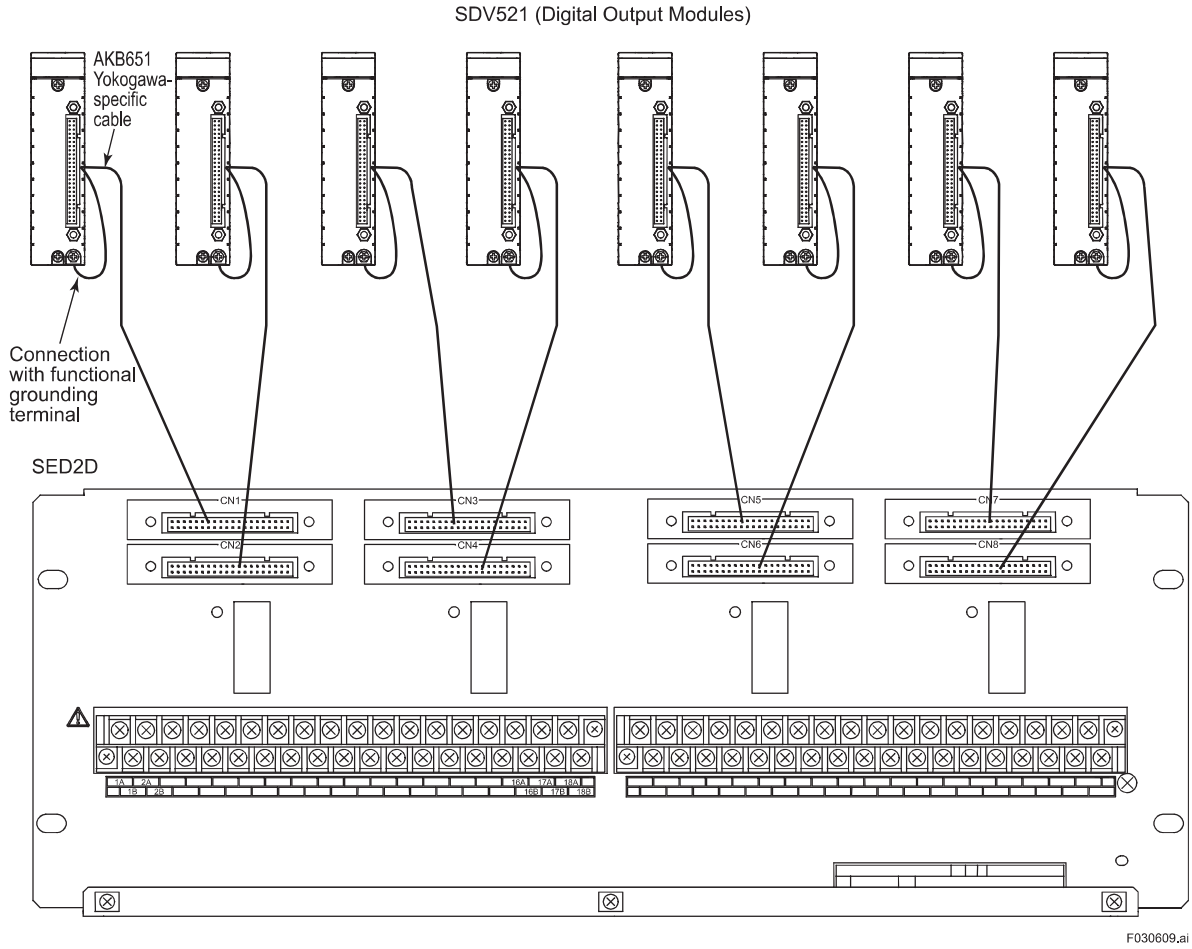


Figure Connecting Digital Output Modules to SED2D Terminal Board (for Dual-redundant Use)

Example of Connection to SBD2D

SBD2D terminal board allows SDV521 modules in both single and dual-redundant configurations.

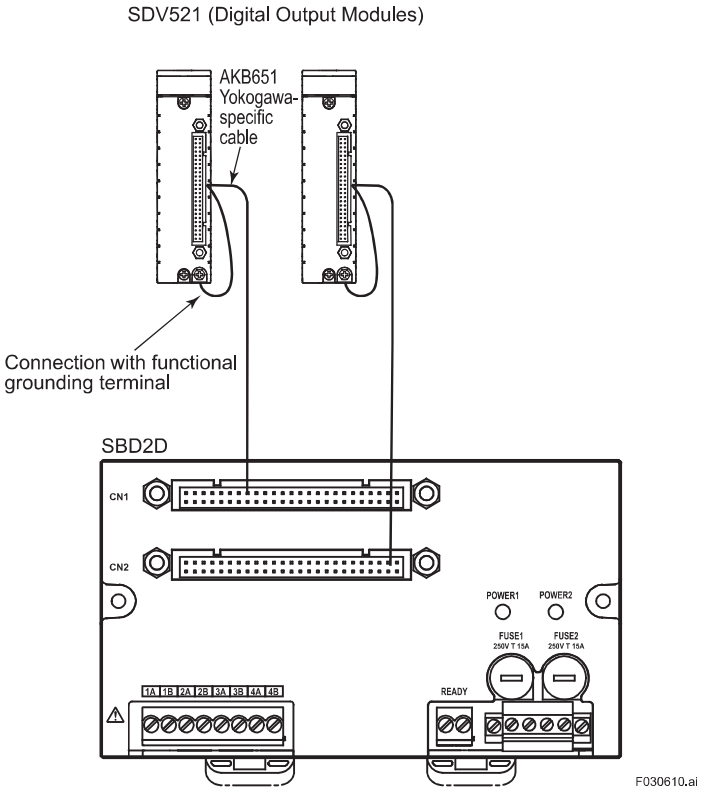


Figure Connecting Digital Output Modules to SBD2D Terminal Board (for Dual-redundant Use)

Example of Connection to SED3D

SED3D terminal board allows SDV53A modules in both single and dual-redundant configurations.

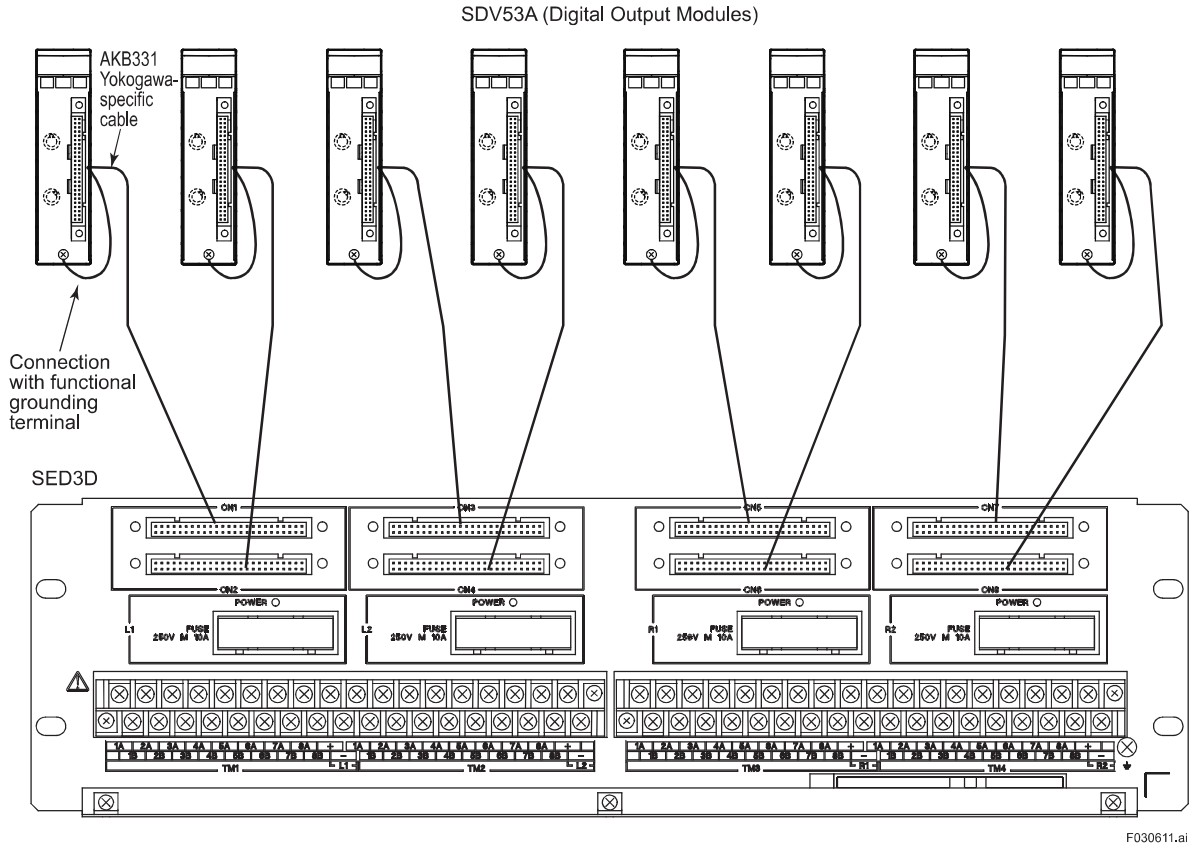


Figure Connecting Digital Output Modules to SED3D Terminal Board (for Dual-redundant Use)

Example of Connection to SBD3D

SBD3D terminal board allows SDV53A or SDV531 modules in both single and dual-redundant configurations.

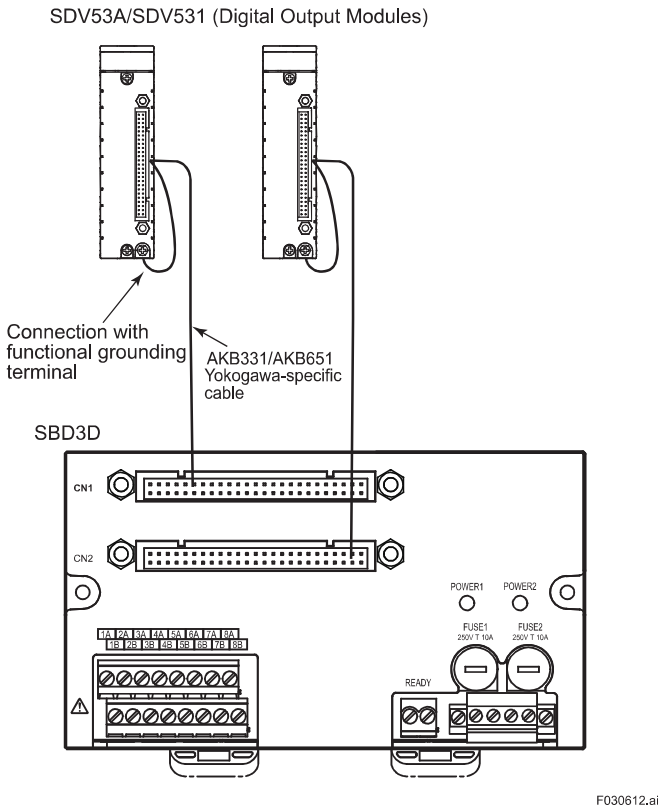


Figure Connecting Digital Output Modules to SBD3D Terminal Board (for Dual-redundant Use)

Example of Connection to SED4D

SED4D terminal board allows SDV144, SDV531 or SDV541 modules in both single and dual-redundant configurations.

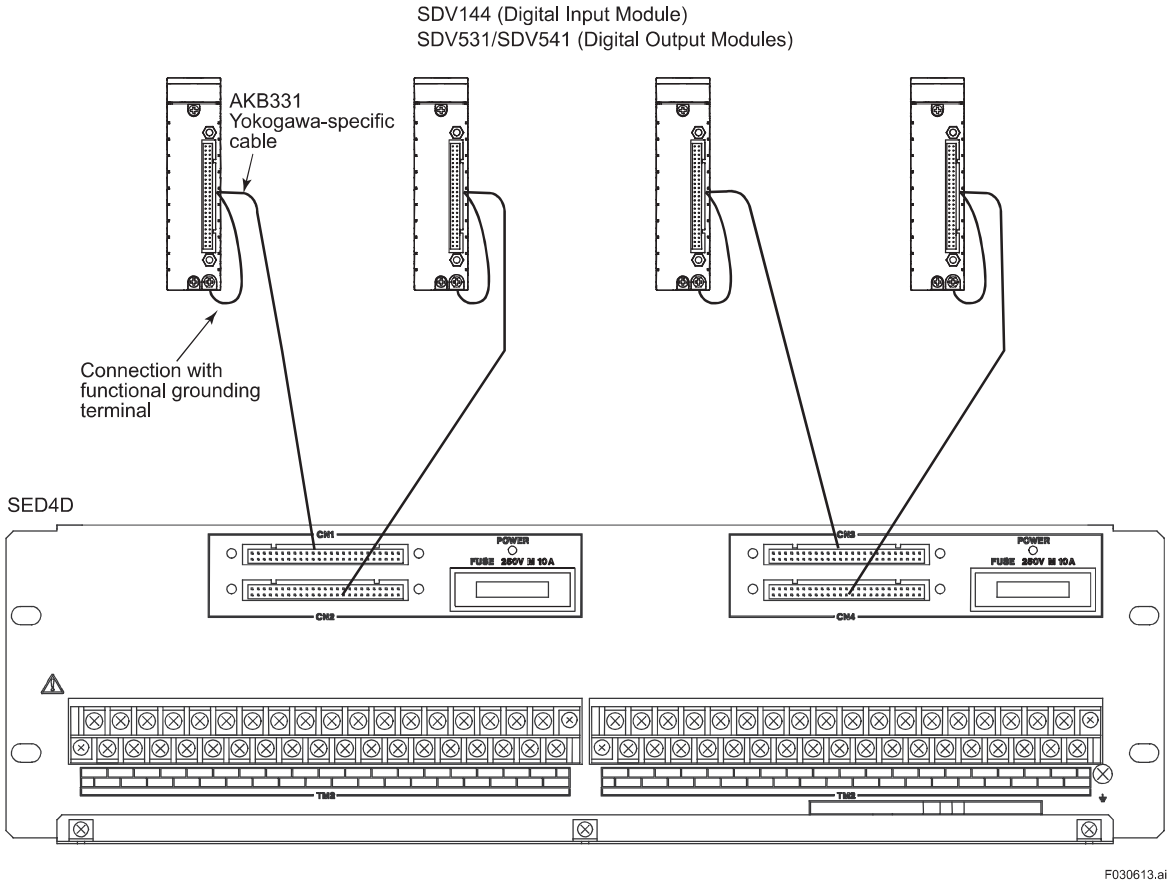


Figure Connecting Digital Input/Output Modules to SED4D Terminal Board (for Dual-redundant Use)

Example of Connection to SBD4D

SBD4D terminal board allows SDV144 or SDV541 modules in both single and dual-redundant configurations.

SDV144 (Digital Input Module) AKB331 Yokogawa-specific cable
SDV541 (Digital Output Module) AKB331/AKB651 Yokogawa-specific cable

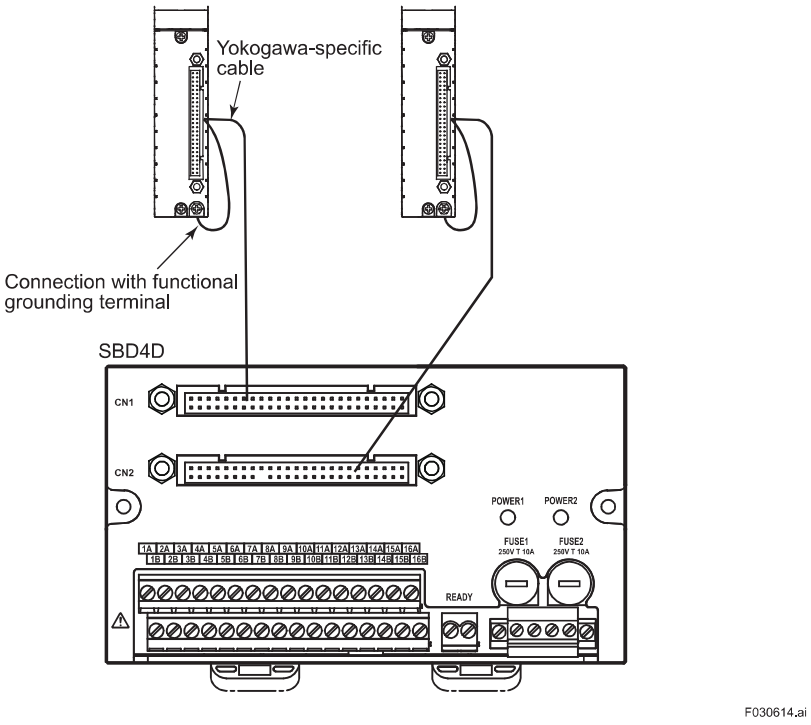


Figure Connecting Digital I/O Modules to SBD4D Terminal Board (for Dual-redundant Use)

Example of Connection to SWD2D

SWD2D terminal board allows SDV526 modules in both single and dual-redundant configurations.

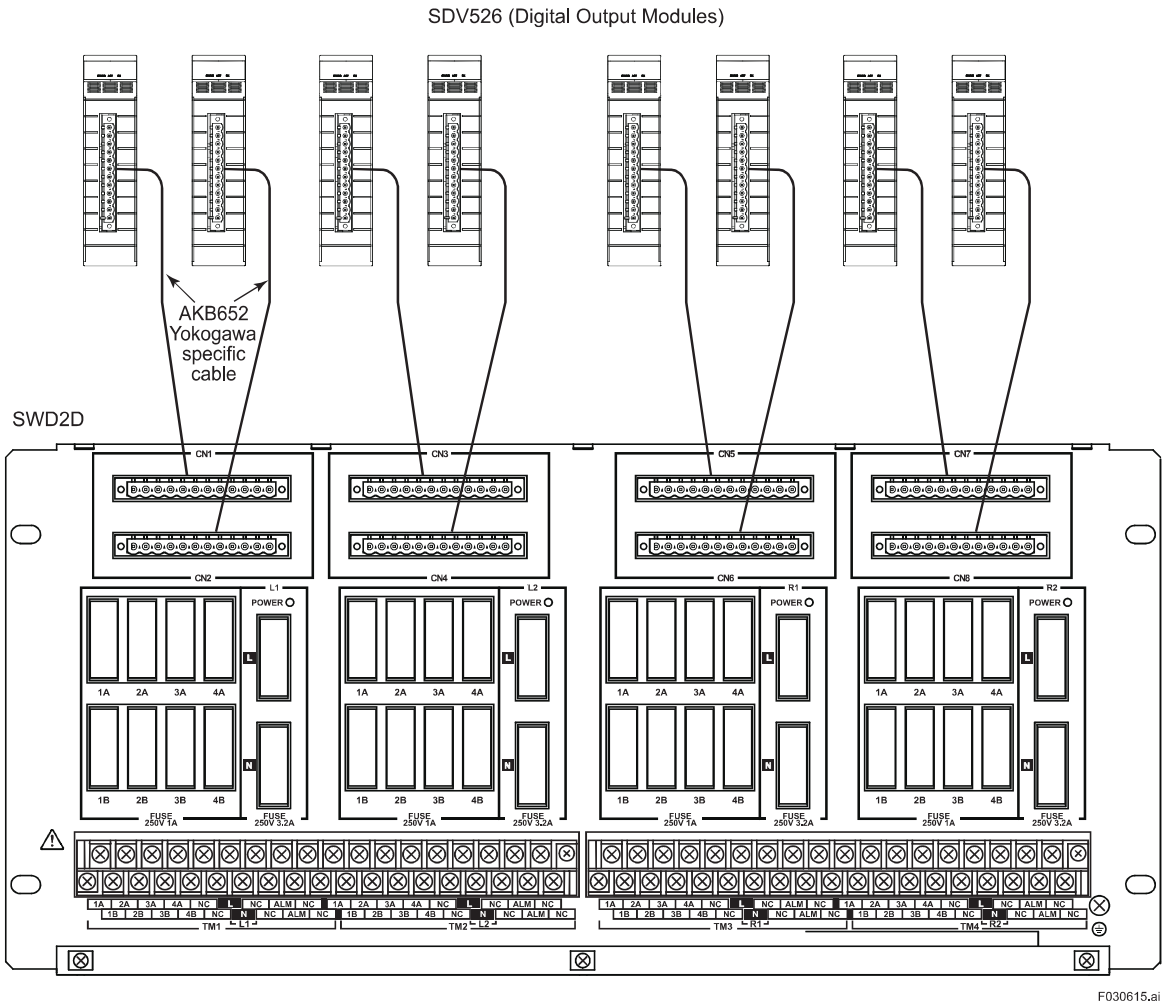


Figure Connecting Digital Output Modules to SWD2D Terminal Board (for Dual-redundant Use)

Connecting Digital Output Modules to Relay Boards

Example of Connection to SRM53D Relay Board

The SRM53D relay board allows SDV531 modules to be dual-redundant.

The SDV144 digital input modules can read back relay output statuses (up to 16 points) (*1).

The SDV144 digital input modules can also be dual-redundant.

*1: 16-point relay output statuses, including 1 to 8 points of CN1 (CN2 for dual-redundant use) and 9 to 16 points of CN5 (CN6 for dual-redundant use), can be read over simultaneously.

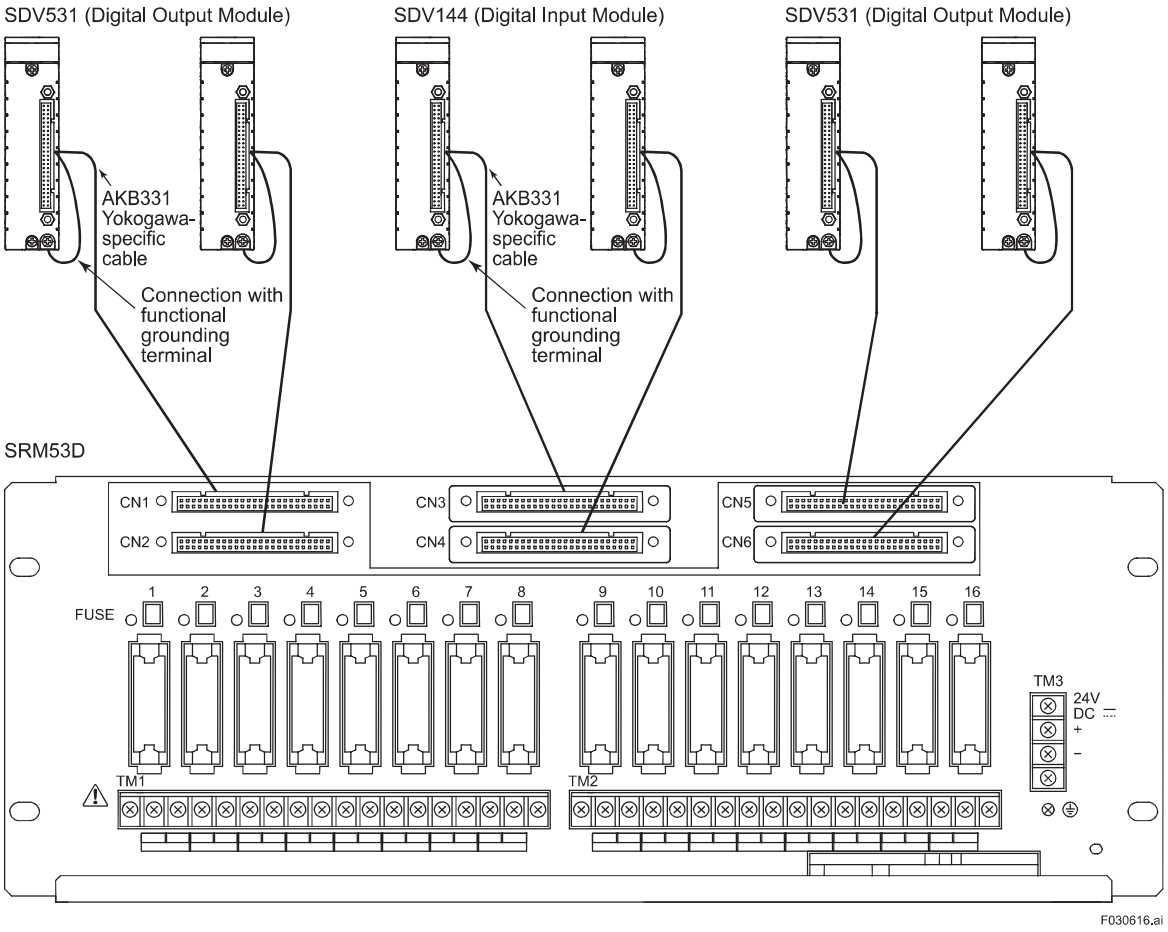


Figure Connecting Digital I/O Modules to SRM53D (for Dual-redundant Use)

Example of Connection to SRM54D Relay Board

The SRM54D relay board allows SDV541 modules to be dual-redundant. The SDV144 digital input module can read back relay output statuses. The SDV144 digital input modules can also be dual-redundant.

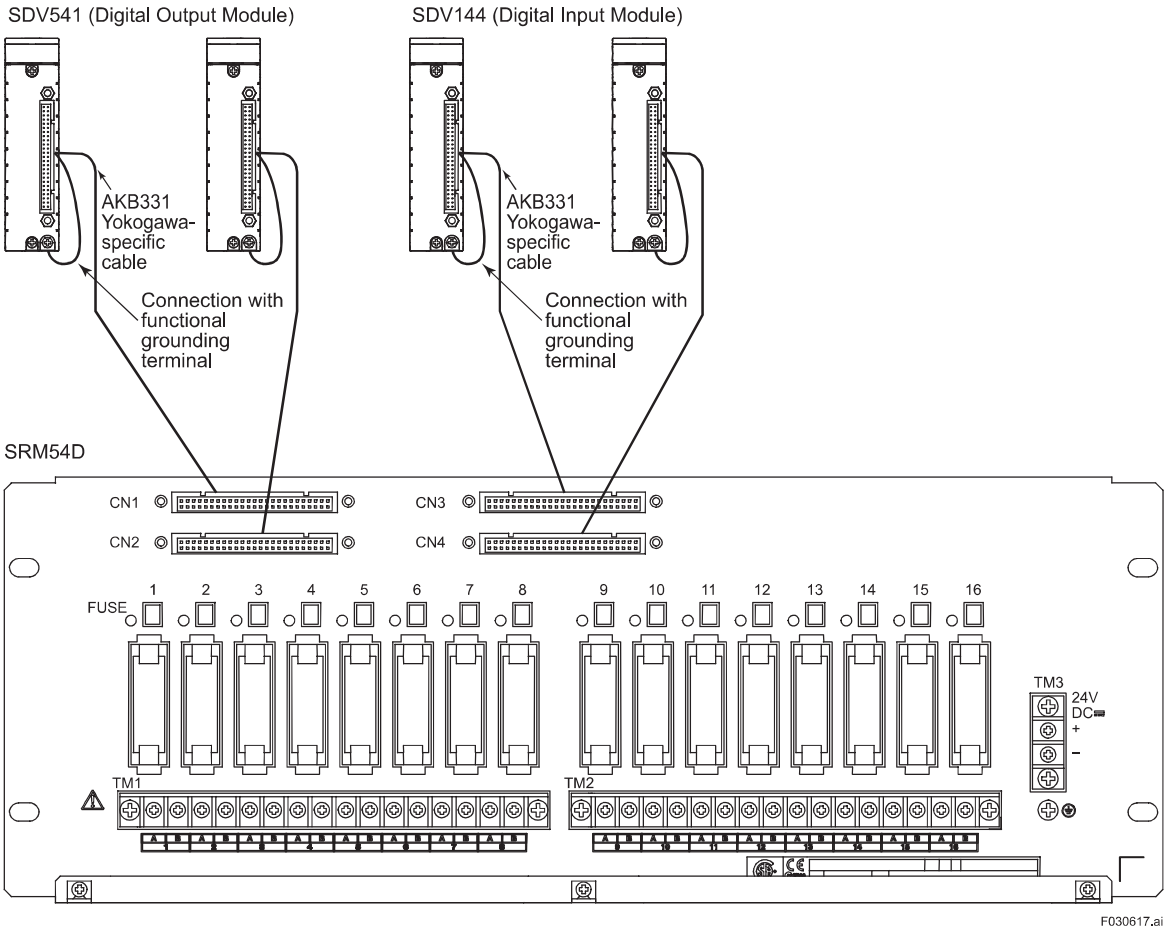


Figure Connecting Digital I/O Modules to SRM54D Relay Board (for Dual-redundant Use)

Example of Connection to SBM54D Relay Board

The SBM54D relay board allows SDV541 modules to be dual-redundant.

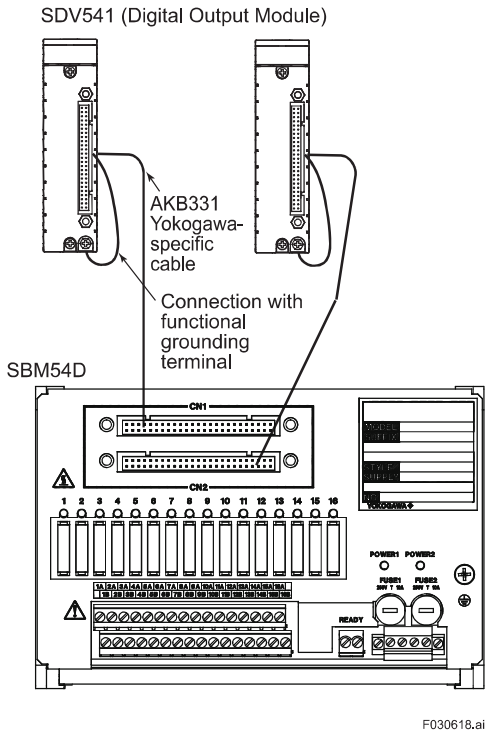


Figure Connecting Digital Output Modules to SBM54D Relay Board (for Dual-redundant Use)

Connecting Wiring Check Adapters

Connect the wiring check adapters to detect disconnected or short-circuited field wiring between the digital input module and field equipment. These adapters should be connected at the field equipment side. The two types of these adapters are:

- SCB100: Disconnection detection while accepting an OFF signal
  If this type of adapter is connected in parallel with a sensor switch, a disconnection occurring while accepting an OFF signal can be detected.
- SCB110: Short-circuit detection
  If this type of adapter is connected in series with a sensor switch, a short-circuit in the power line, occurring while accepting an ON signal, or a short-circuit with other channels can be detected. In addition to the above wiring check adapters, input module's diagnostic functions should be able to detect disconnections or short-circuits.

SEE ALSO For more information about diagnostic features of the input modules, see the following:
Appendix 1.3.4 "Setting for the DI channel" of the Engineering Guide Vol. 1 (IM 32P01C10-01EN).

Shape of Wiring Check Adapters

The following figure shows the shape of the SCB100 and SCB110.

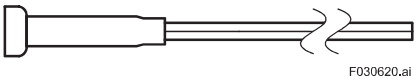


Figure External View of SCB100 and SCB110

Connecting Wiring Check Devices

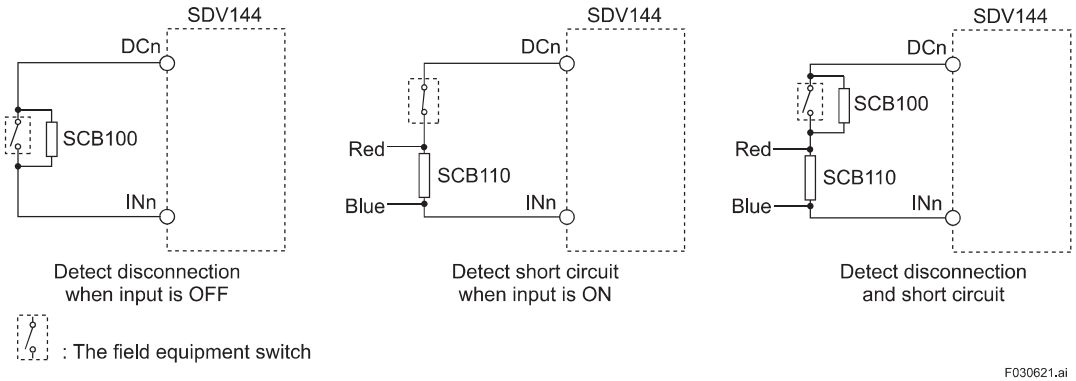


Figure Connecting Wiring Check Adapters

IMPORTANT

- Connect the SCB110 with correct polarity. If it is connected incorrectly, no detection can be made.
- To detect short-circuits or disconnections in the field wiring effectively, locate the adapters in the vicinity of the field equipment. Also install these adapters in a location out of direct sunlight and sheltered from rain.
- Be careful not to bend a covered part.

3.7 Signal Connections of N-IO I/O Unit

This section describes connecting to the N-IO I/O unit.

3.7.1 N-IO I/O Unit Types

I/O Modules that can be used with Base Plate

The following table shows I/O Modules installable with Base Plate.

Table I/O Modules Installable with Base Plate

Base plate model	Description	Base Plate		
		S2BN1D	S2BN4D	S2BN5D
S2MMM843	Analog Digital I/O Module	X	X	X
S2MDV843	Digital I/O Module	X	X	X

X: Mountable

3.7.2 Base Plate

Terminal type that can be select with Base Plate

The following table shows terminal types can be select with S2BN1D Base Plate.

Table Terminal type Compatible with S2BN1D Base Plate

Base plate model	Suffix code	Terminal type
S2BN1D (Base Plate with disconnecting terminal)	-□1□□□	Pressure clamp terminal
	-□2□□□	Spring clamp terminal
	-□9□□□	Cable connector (*1)

*1: Connecting the field signal to the pressure cramp terminal on the terminal board (A2BM4) via a dedicated cable.

Connecting Signal Cables with S2BN1D

S2BN1D

Terminal number	Signal type
□A	Analog Digital I/O (AI_□/AO_□/DI_□/DO_□)
□B	Common (COM)

□: Channel number

A2BM4

Terminal number	Signal type
□A	Analog Digital I/O (AI_□/AO_□/DI_□/DO_□)
□B	Common (COM)
□C	Field power supply (F24V) or unused (*1)

□: Channel number
*1: Field power supply (F24 V) is for Analog input function (3-wire). Otherwise, terminal-C is unused.

Base Plate Terminal Numbers (Spring Clamp Terminals)

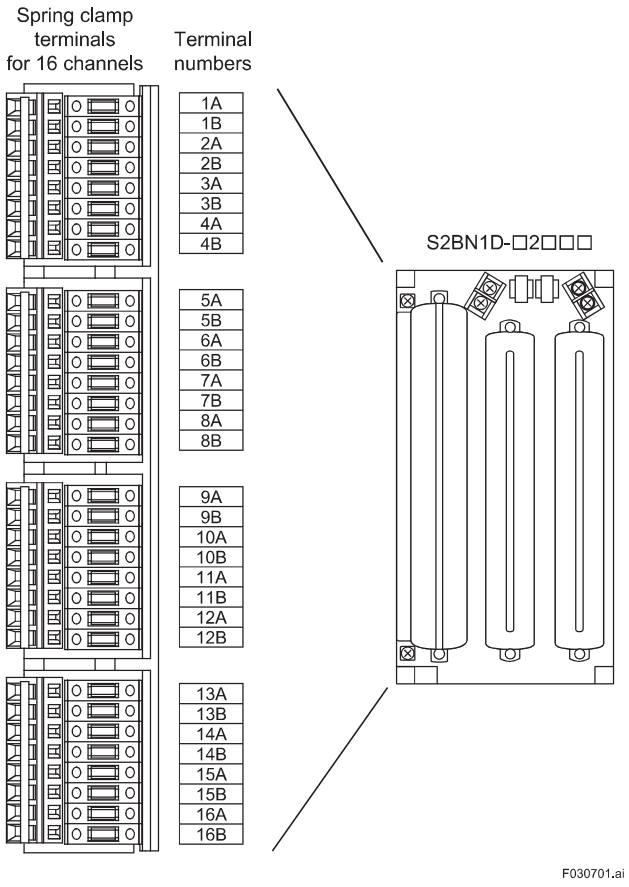


Figure S2BN1D-□2□□□ Base Plate for Adaptor

Base Plate Terminal Numbers (Pressure Clamp Terminals)

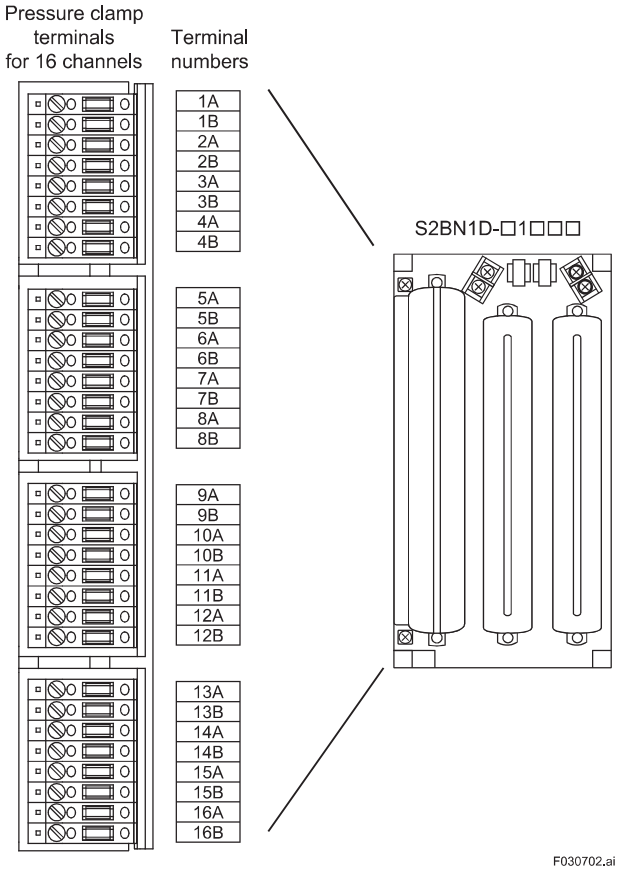
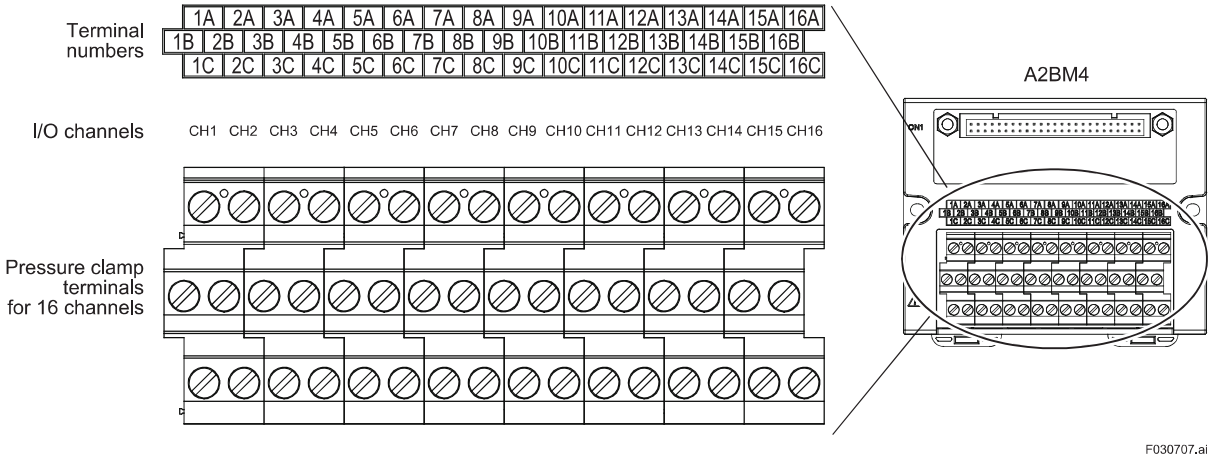


Figure S2BN1D-□1□□□ Base Plate

Terminal board Terminal Numbers (pressure Clamp Terminals)



Parallel connection with adjacent channels (S2BN1D, A2BM4)

The maximum load current per channel is 0.66 A. A load current device with more than 0.66 A can be connected by using parallel connection with adjacent channels.

- The 2 channels parallel connection allows a maximum load current of 1.3 A.
- The 3 channels parallel connection allows a maximum load current of 2.0 A.

For the parallel connection, connect the signal cable to the external terminal block from the terminal block of the base plate (S2BN1D) or terminal board (A2BM4). The following figure shows an example of parallel connection.

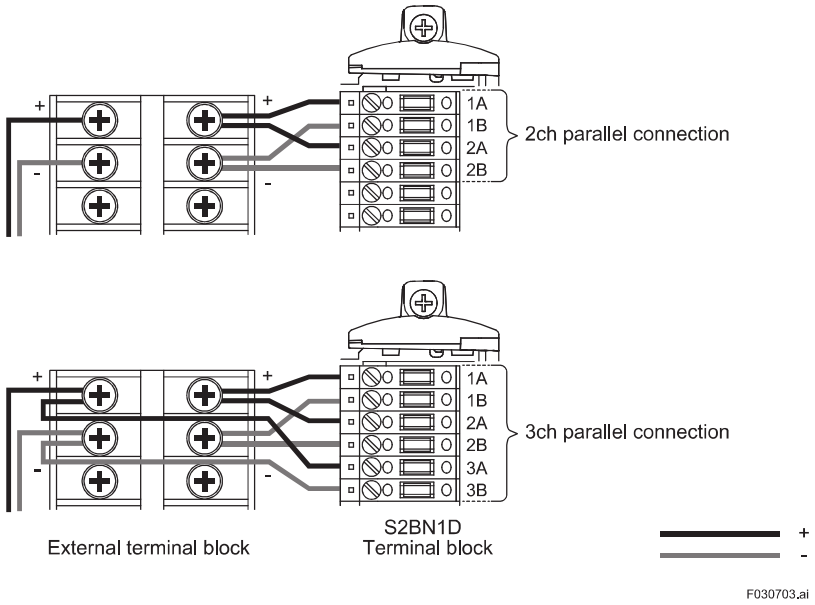


Figure Parallel connection for S2BN1D

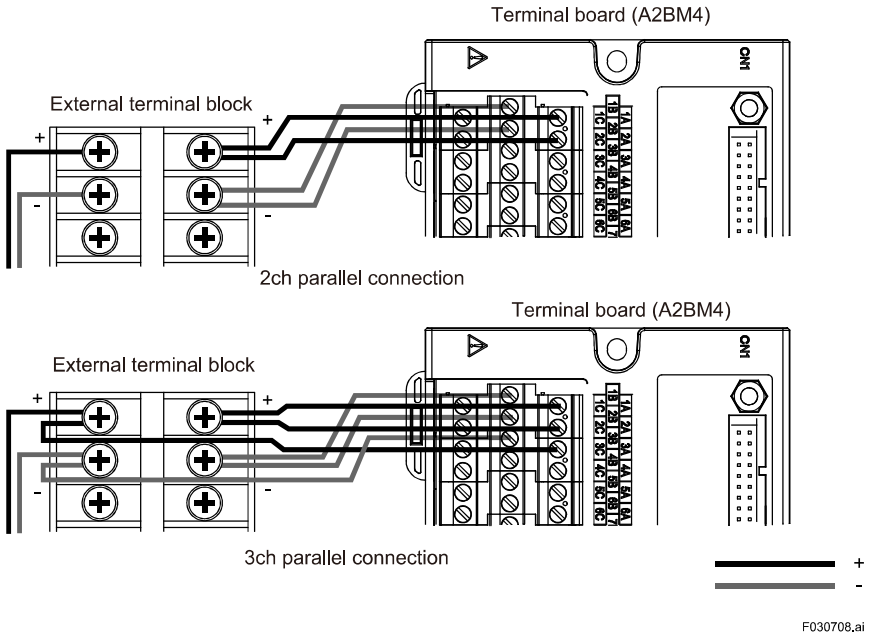


Figure Parallel connection for A2BM4

Connecting Wiring Check Adapters

Connect the wiring check adapters to detect disconnected or short-circuited field wiring between the digital input channel and field equipment. These adapters should be connected at the field equipment side. The two types of these adapters are:

- SCB100: Disconnection detection while accepting an OFF signal
  If this type of adapter is connected in parallel with a sensor switch, a disconnection occurring while accepting an OFF signal can be detected.
- SCB110: Short-circuit detection
  If this type of adapter is connected in series with a sensor switch, a short-circuit in the power line, occurring while accepting an ON signal, or a short-circuit with other channels can be detected. In addition to the above wiring check adapters, input module's diagnostic functions should be able to detect disconnections or short-circuits.

SEE ALSO For more information about diagnostic features of the input modules, see the following:
Appendix 1.3.4 "Setting for the DI channel" of the Engineering Guide Vol. 1 (IM 32P01C10-01EN).

Shape of Wiring Check Adapters

The following figure shows the shape of the SCB100 and SCB110.

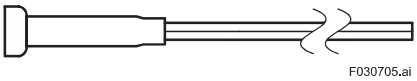


Figure External View of SCB100 and SCB110

Example of Connecting Wiring Check Devices

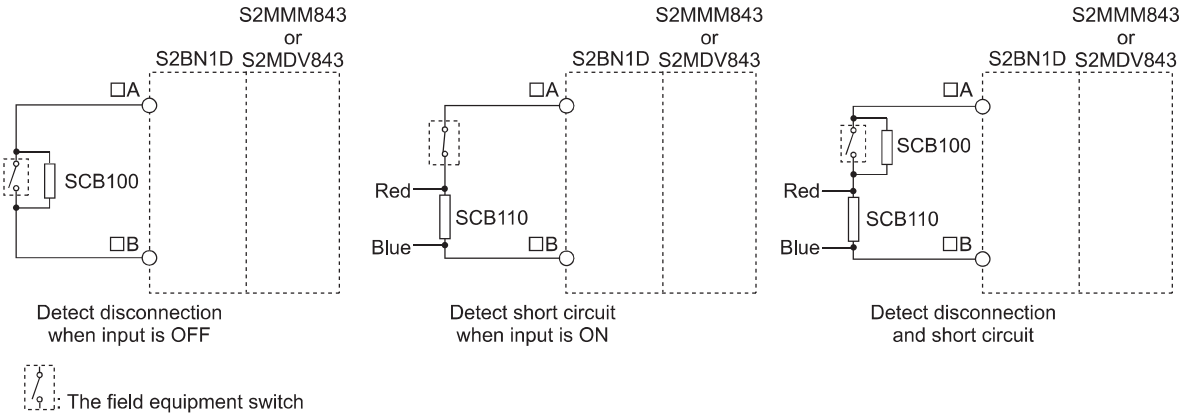


Figure Connecting Wiring Check Adapters

IMPORTANT

- Connect the SCB110 with correct polarity. If it is connected incorrectly, no detection can be made.
- To detect short-circuits or disconnections in the field wiring effectively, locate the adapters in the vicinity of the field equipment. Also install these adapters in a location out of direct sunlight and sheltered from rain.
- Be careful not to bend a covered part.

3.7.3 Base Plate for Barrier

Base Plate for Barrier Types and Terminal Types

The following table shows relation between Base Plate for Barrier Types and Terminal Types.

Table Base Plate for Barrier Types and Terminal Types

Base plate model	Suffix code	Field wiring direction	Terminal type	Terminal position
S2BN4D Base Plate for Barrier (MTL)	-□□□C□	Left	Pressure clamp terminal	On barrier module
	-□□□D□	Right		
S2BN5D Base Plate for Barrier (P+F)	-□□□C□	Left	Spring clamp terminal	On base plate
	-□□□D□	Right		

Installable Barriers with Base Plate for Barrier

The following table shows Modules installable with Base Plate for Barrier.

Table Modules Installable with Base Plate for Barrier

Base plate model	Model of installable barrier
S2BN4D Base Plate for Barrier (MTL)	Refer to the General Specifications (GS).
S2BN5D Base Plate for Barrier (P+F)	Refer to the General Specifications (GS).

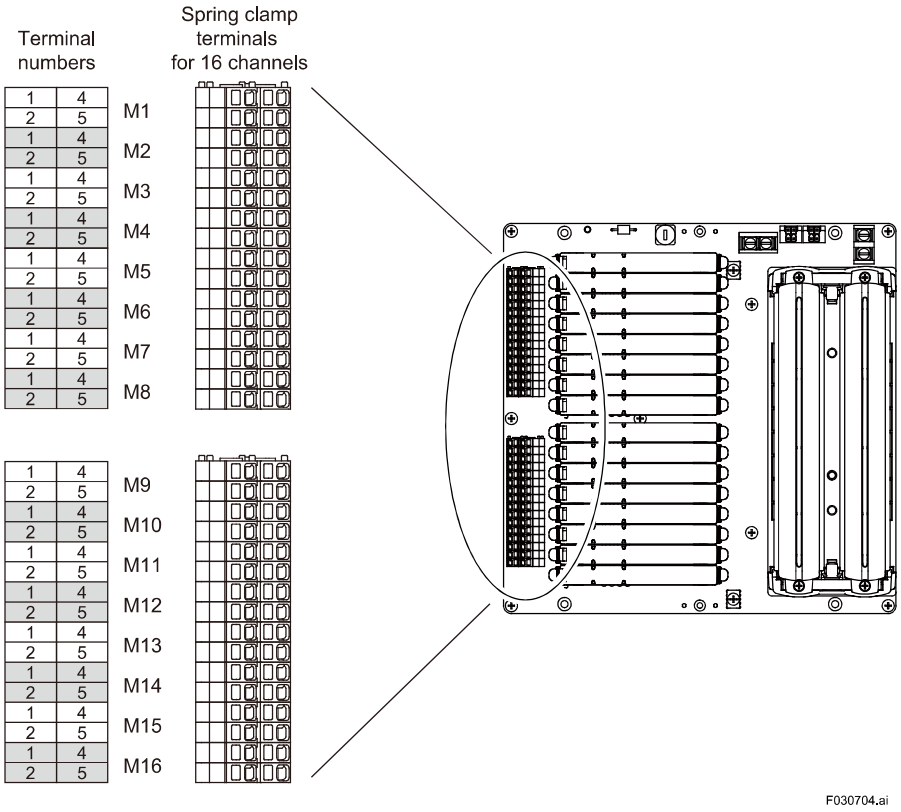
Base Plate for Barrier Terminal Numbers

S2BN4D (Pressure Clamp Terminals)

The S2BN4D Base Plate for Barrier do not have signal terminals because signal terminals are provided on intrinsic safety barriers.

Information about the terminal numbers of the signal terminals provided on the intrinsic safety barriers, refer to the manufacture's catalog.

S2BN5D Base Plate for Barrier (Spring Clamp Terminals)



Connecting Signal Cables with Base Plate for Barrier (S2BN5D)

The signal connections of the base plate for Barrier (model: S2BN5D) differ depending on the signal type. The following table shows the terminal numbers and signal types.

Table Terminal Numbers and Signal Types (S2BN5D)

Intrinsic safety barriers	Terminal number	Signal type (*1)					
		Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
For analog input	1	Two-wire transmitter input +	Current input +	—	—	—	—
	2	—	—	—	—	—	—
	4	Two-wire transmitter input −	—	—	—	—	—
	5	—	Current input −	—	—	—	—
For analog output	1	Analog output +	—	—	—	—	—
	2	—	—	—	—	—	—
	4	Analog output −	—	—	—	—	—
	5	—	—	—	—	—	—
For digital input	1	Digital input+	—	—	—	—	—
	2	—	—	—	—	—	—
	4	Digital input −	—	—	—	—	—
	5	—	—	—	—	—	—
For digital output	1	Digital output +	—	—	—	—	—
	2	—	—	—	—	—	—
	4	Digital output −	—	—	—	—	—
	5	—	—	—	—	—	—
For temperature input	1	RJC connection	—	RTD four-wire type current source +	RTD three-wire type current source +	RTD two-wire type current source +	Skid resistance current source +
	2	Thermocouple input +	Voltage input +	RTD four-wire type input +	—	—	—
	4	RJC connection	—	RTD four-wire type current source -	RTD three-wire type current source -	RTD two-wire type current source -	Skid resistance current source -
	5	Thermocouple input -	Voltage input -	RTD four-wire type input -	RTD three-wire type input -	—	Skid resistance input -

*1: "—" denotes that the terminal is not used. Do not connect any signal to it.

3.8 Connecting Bus Cable

There are three types of control network bus named as Vnet/IP, and Vnet/IP-Upstream for the ProSafe-RS system.
Vnet/IP or Vnet/IP-Upstream is used for S2SC70S/S2SC70D, SSC60S/SSC60D, SSC50S/SSC50D, and SSC57S/SSC57D. Vnet/IP-Upstream is the same connection as Vnet/IP.
This section describes each control network bus cabling and ESB bus cabling related to the control network bus.

3.8.1 Vnet/IP network

Information on Vnet/IP interface connection and an example of SENG and SCS connection are shown below:

● Vnet/IP Interface

- Topology : tree connection
- Configuration : dual redundancy only
- Connector : RJ45 connector
- Intra-domain connection : L2SW used
- Inter-domain connection : L3SW used
- Recommended cable : UTP cable of CAT5e or above (optical cable for outdoor use)

● SENG and SCS Connection

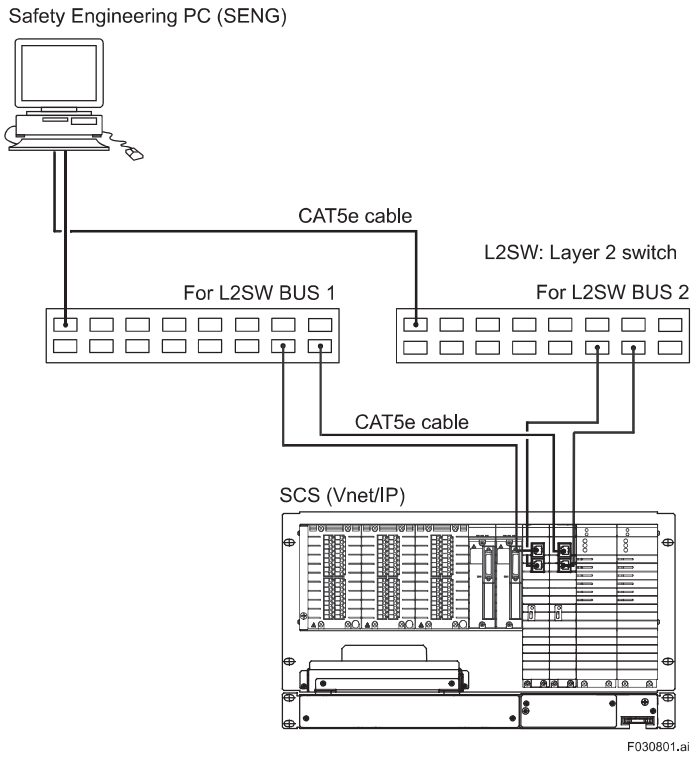


Figure Example of SENG and SCS Connection

Example of Connection between V net Router and SCS

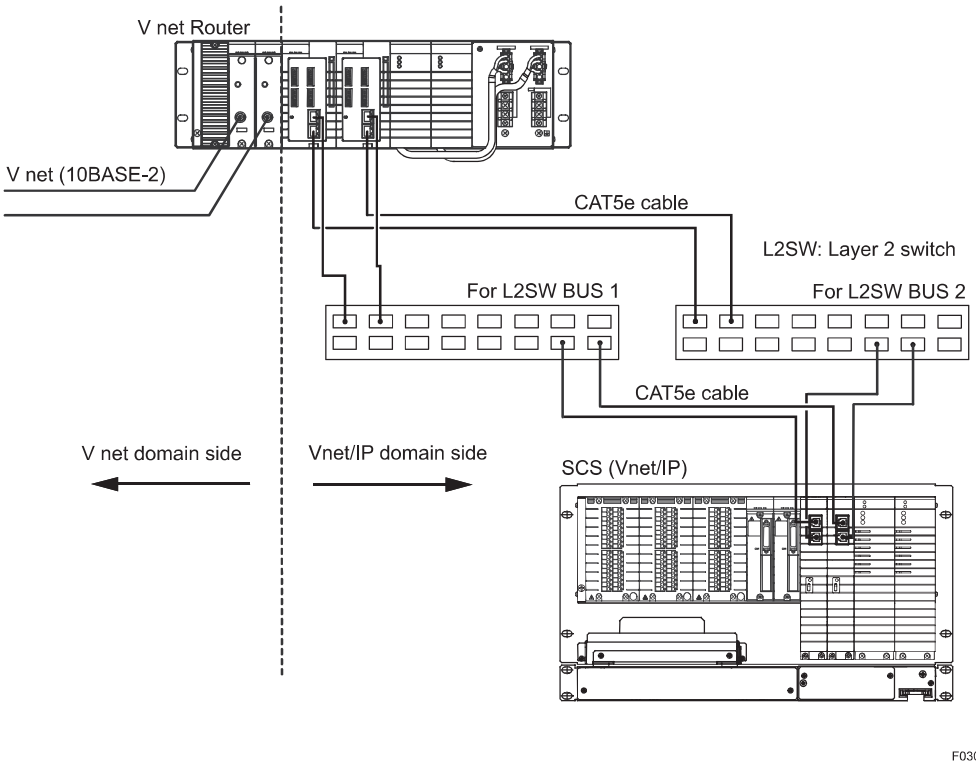


Figure Example of Connection between V net Router and SCS

Example of Connection between AW810D and SCS

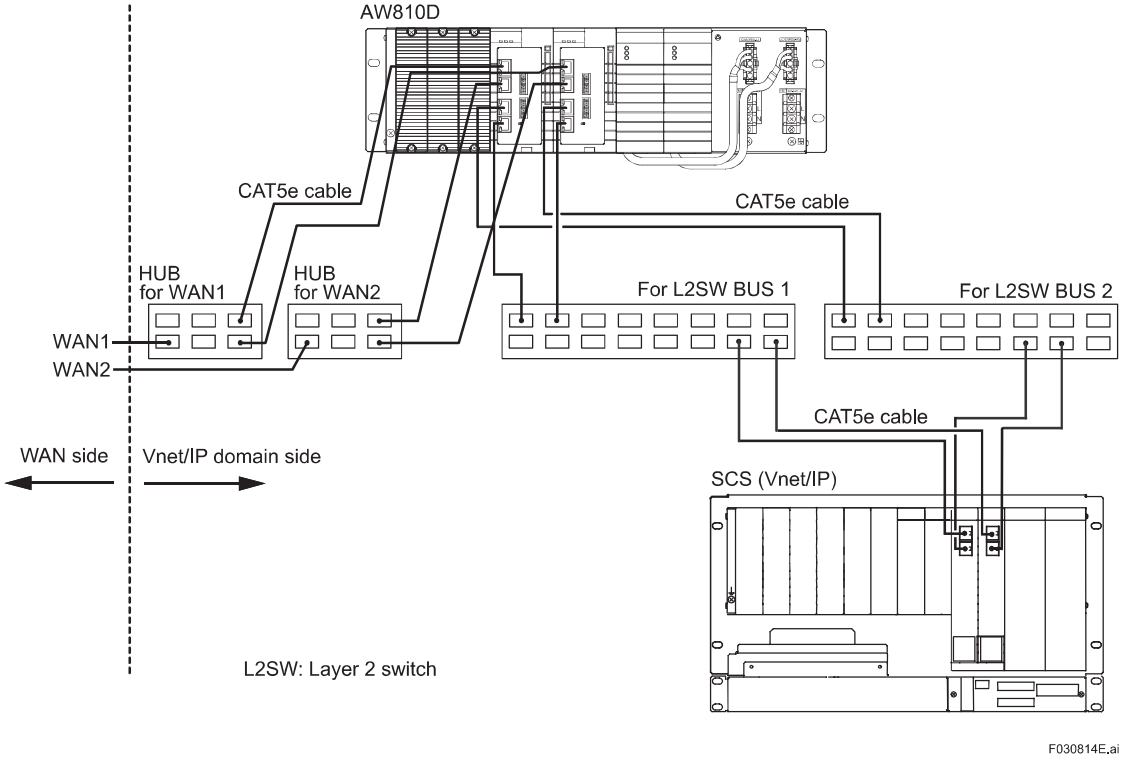


Figure Example of Connection between AW810D and SCS

Differentiation between BUS 1 and BUS 2

Use different colors, etc., to differentiate between BUS 1 and BUS 2.

Destination Display

Attach a display tag at the tip of cables to indicate the station number, switch number, and port number of the destination.

Cable Fixing

Fix cables securely so that their connectors are not exposed to undue stress.

Handling of Vnet/IP Cables Connected to the Processor Module (S2CP471/ SCP461/SCP451)

- Turn the power on after connecting the cables to the processor module.
- When removing the processor module on-line, remove it with the cable connected to it.
- Before installing the processor module on-line, connect a cable to it.

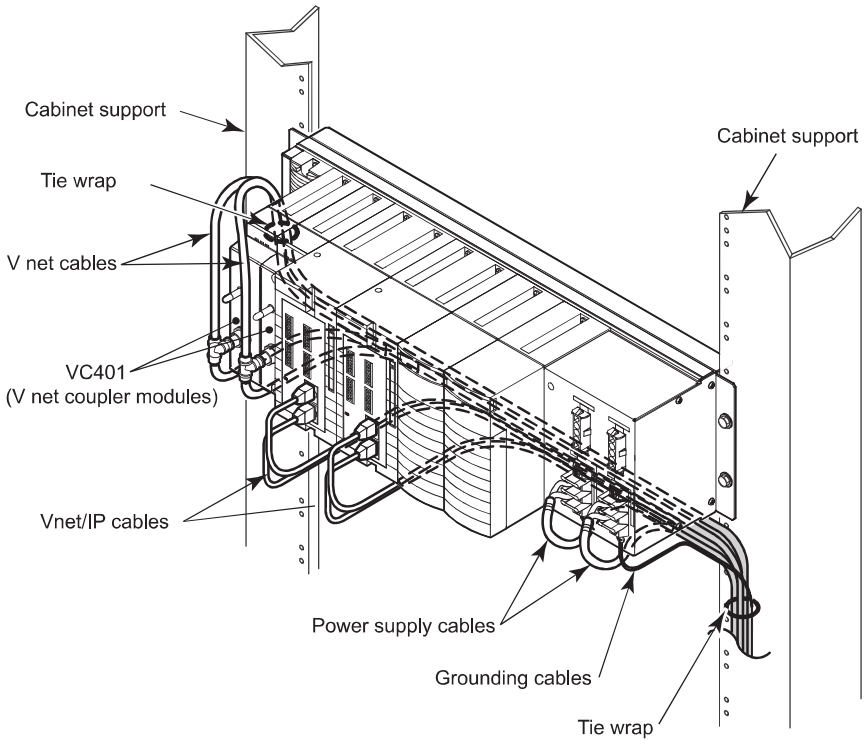
Handling communication module for V net router (VI451) of Duplexed V net router (AVR10D) and connecting cable

- Switch on after connecting a cable to VI451.
- Remove VI451 on line with a cable connected to VI451.
- Attach VI451 on line after connecting cable to VI451.

Handling VI702 and connecting cable

- Do not power on PC until a cable is attached.
- Power off PC first to remove a cable.

Cabling for AVR10D System



Use a tie wrap to fix the V net cable onto the support on the side of the VC401.

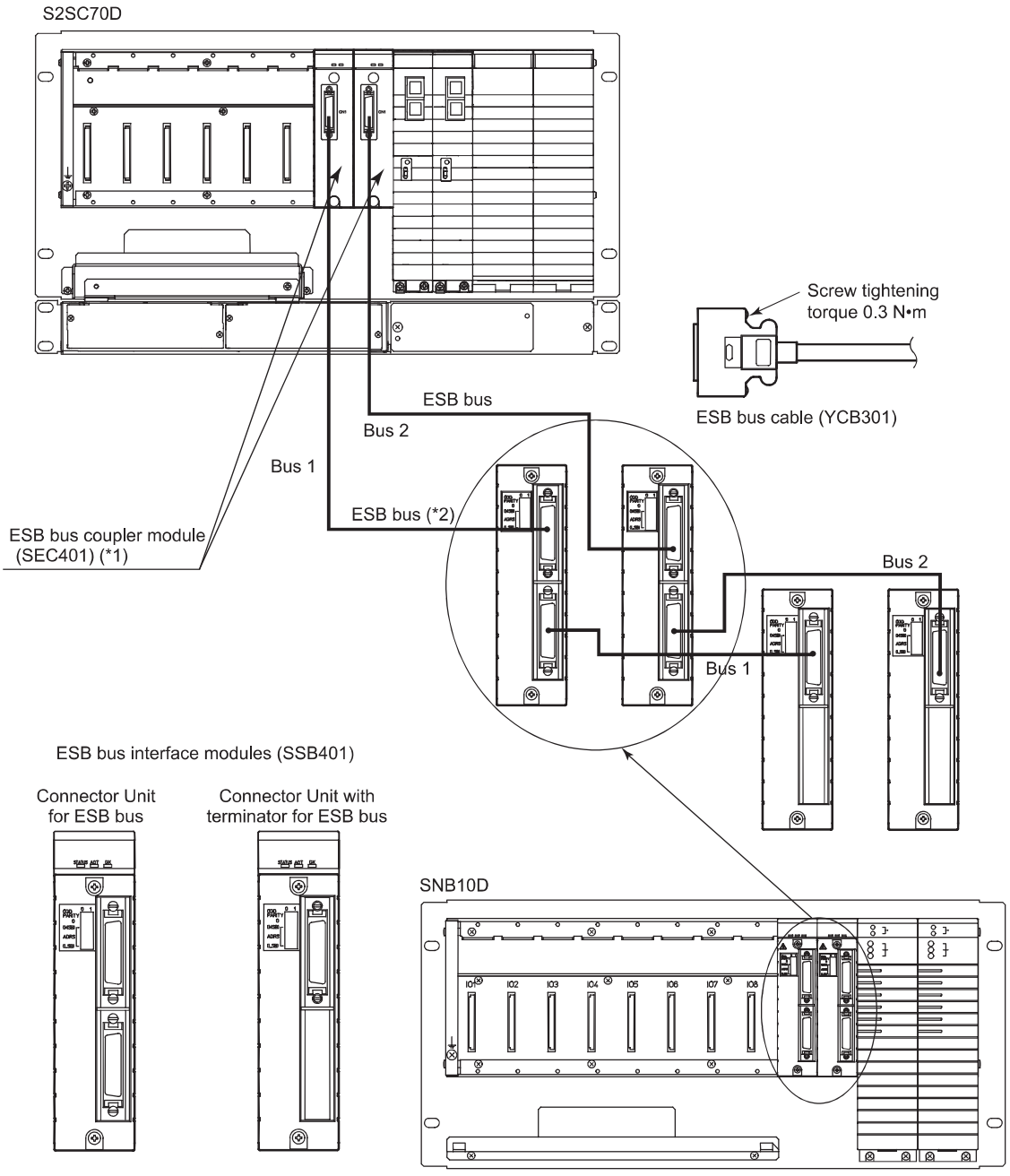
F030803.ai

Figure Cabling Diagram for the AVR10D System

3.8.2 ESB Bus

Either the ESB bus branching connector or the branching connector that has a built-in ESB bus terminator must be mounted to SSB401 installed in the SNB10D safety node unit. If a node unit is connected next, select the ESB bus branching connector. If the node unit is the last one, select the branching connector that has a built-in ESB bus terminator.

The following is an example of connecting an ESB bus using SEC401 ESB bus coupler module. SEC401 can be installed in S2SC70☐, SSC60☐, SSC50☐, and SSC57☐.



*1: Total number of SNB10D safety node units must be 9 or less when SEC401 is used.
*2: Length of ESB buses must be 10 m or shorter from SEC401.

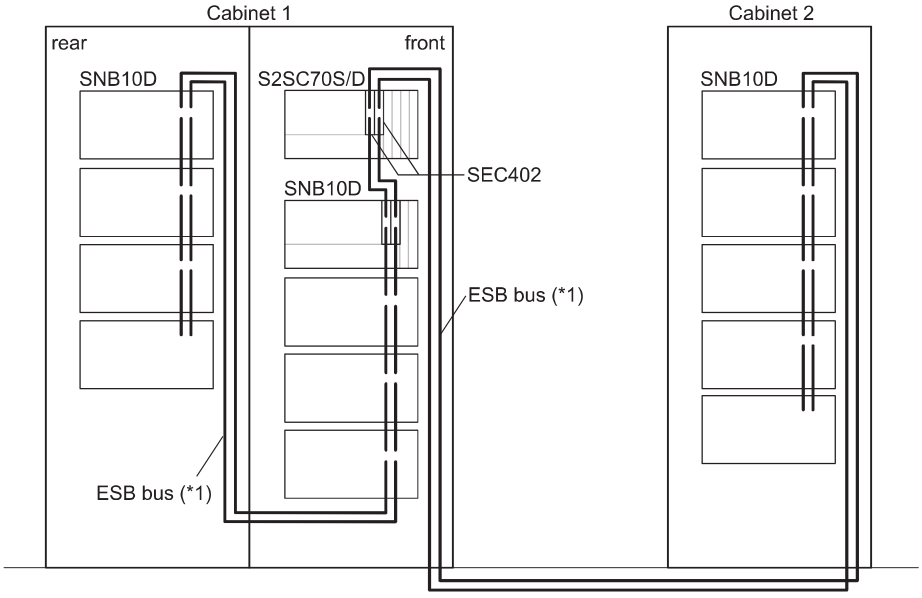
F030804.ai

Figure ESB bus Connection (S2SC70D)

Using SEC402 ESB bus coupler module, up to 13 SNB10D safety node units (*1) can be connected to S2SC70☐/SSC60☐ safety control unit. SEC402 has two ports to connect ESB bus cables. Up to 9 SNB10D units can be connected to each of the upper and lower port, and up to 13 SNB10D units can be connected to SEC402 as a total of the upper and lower ports. SEC402 can work normally even when node units are only connected to either of the two ports, leaving the other port vacant and not terminated. ESB Bus communication is available at this condition.

*1: To connect 10 or more SNB10Ds, CFS1350 Node Expansion Package is required.

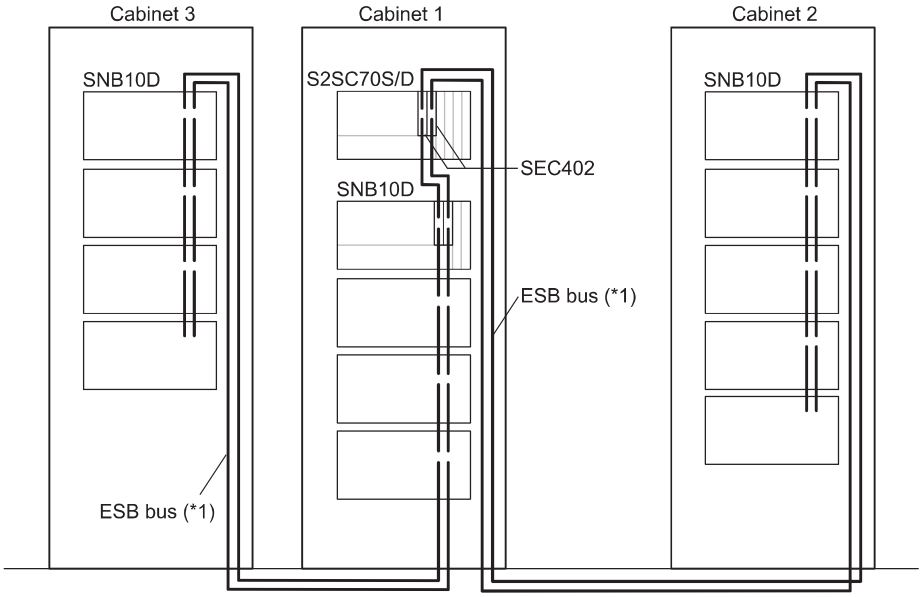
The following are examples of ESB bus connection using SEC402.



*1: Length of ESB buses must be 10 m or shorter each from the upper and lower port of SEC402.

F030805.ai

Figure ESB bus Connection when Two Cabinets are Used



*1: Length of ESB buses must be 10 m or shorter each from the upper and lower port of SEC402.

F030806.ai

Figure ESB bus Connection when Three Cabinets are Used

3.8.3 N-ESB Bus

The following figure shows a connection example of the N-ESB bus.

Connect UTP straight Cable of Cat5e (two) from N-ESB bus Coupler Module (S2EN402, S2EN404) to N-ESB bus Module (S2EN501).

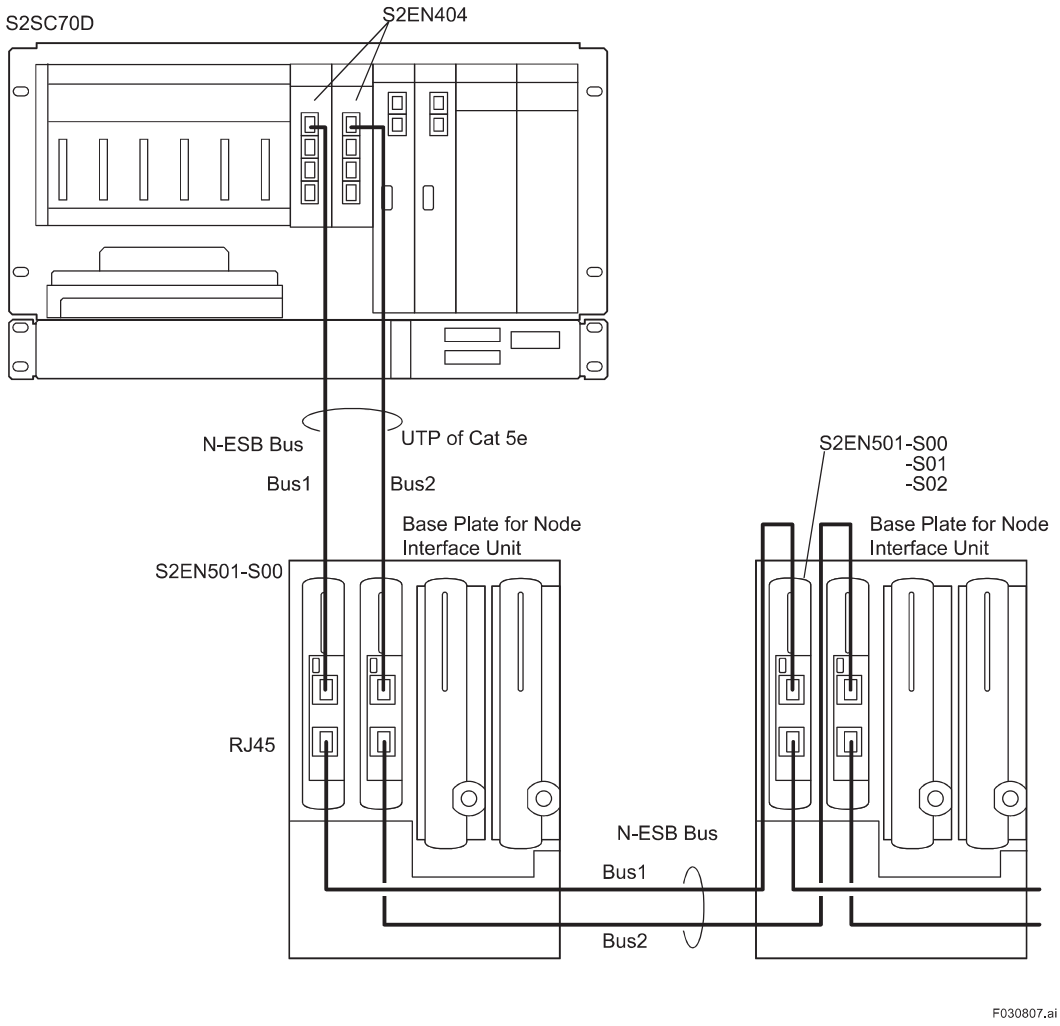


Figure Example of N-ESB Bus Connection

IMPORTANT

An N-ESB bus cable for the ProSafe-RS can be routed only in the cabinet or within the cabinets bayed together. An optical ESB bus cable must be used instead of an N-ESB bus cable when a cable is routed outside of the cabinet.

3.8.4 Optical ESB Bus

S2EN40☐

The following figure shows a connection example of the optical ESB Bus of the N-IO system.

Use a N-ESB Bus Module (S2EN501) equipped with an optical module to connect between an NIU and NIU.

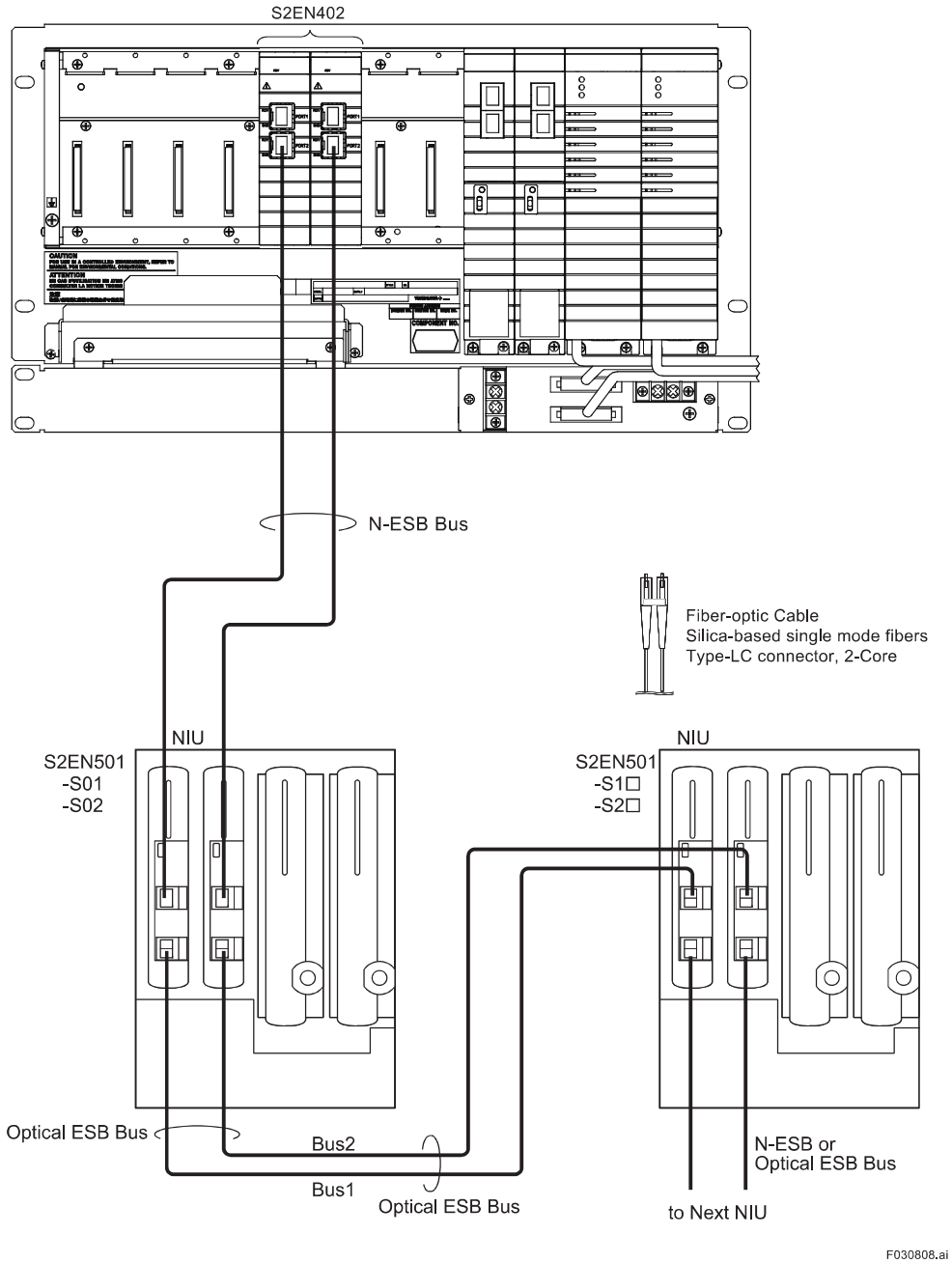


Figure Optical ESB Bus (N-IO) Connection (When Chain Connection)

Optical ESB Bus Repeaters use fiber-optic cables to connect an SNT401/SNT411 Optical ESB Bus Repeater Master Module and an SNT501/SNT511 Optical ESB Bus Repeater Slave Module to each other.
When S2SC70☐, SSC60☐, SSC50☐ or SSC57☐ is used for the safety control unit, SNT401, SNT411, SNT501 and SNT511 are available.

You can connect these devices in the structures of star and chain type connections.

In one method, optical ESB bus repeater module unit (SNT10D) is used and in the other, it is not.

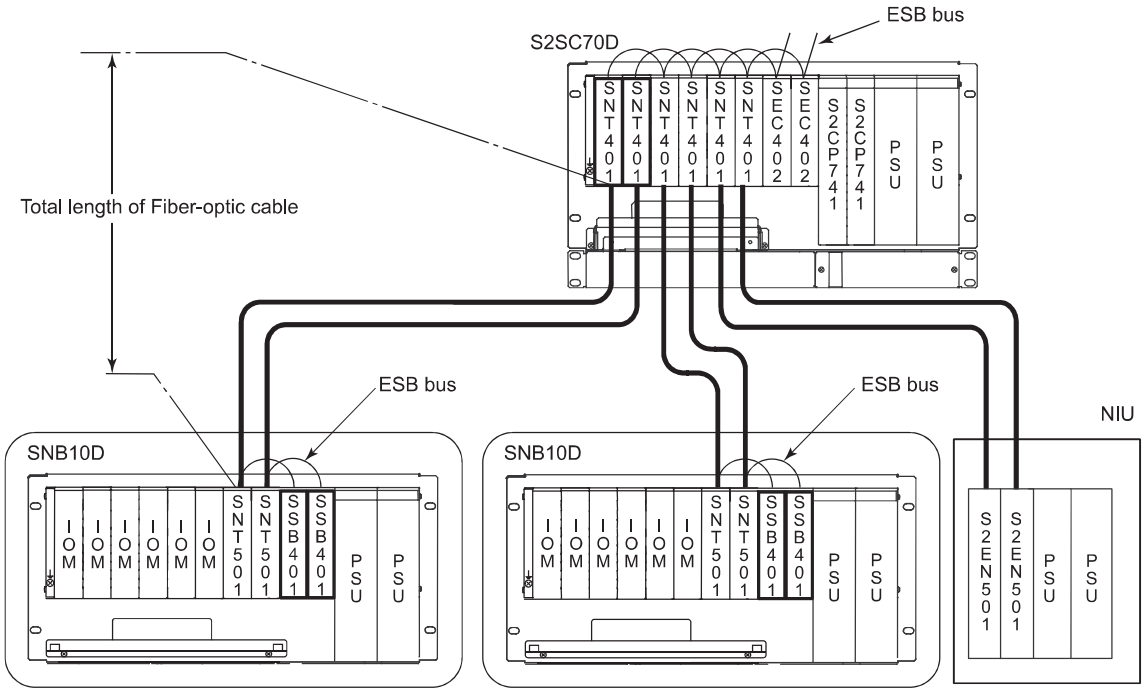
Examples of connecting optical ESB bus repeater modules are shown below using SNT401 and SNT501. The same connection can be applied to SNT411 and SNT511.

Star Type Connection

Star type connection is possible when connecting SNT401/SNT411 installed on S2SC70☐/ SSC60☐/SSC50☐/SSC57☐ (safety control unit) or SNT10D (unit for Optical ESB bus repeater module) to SNT501/SNT511 installed on SNB10D (safety node unit).

Fiber-optic cable for ESB bus can be star-connected to SNT501/SNT511.

Example of not using SNT10D



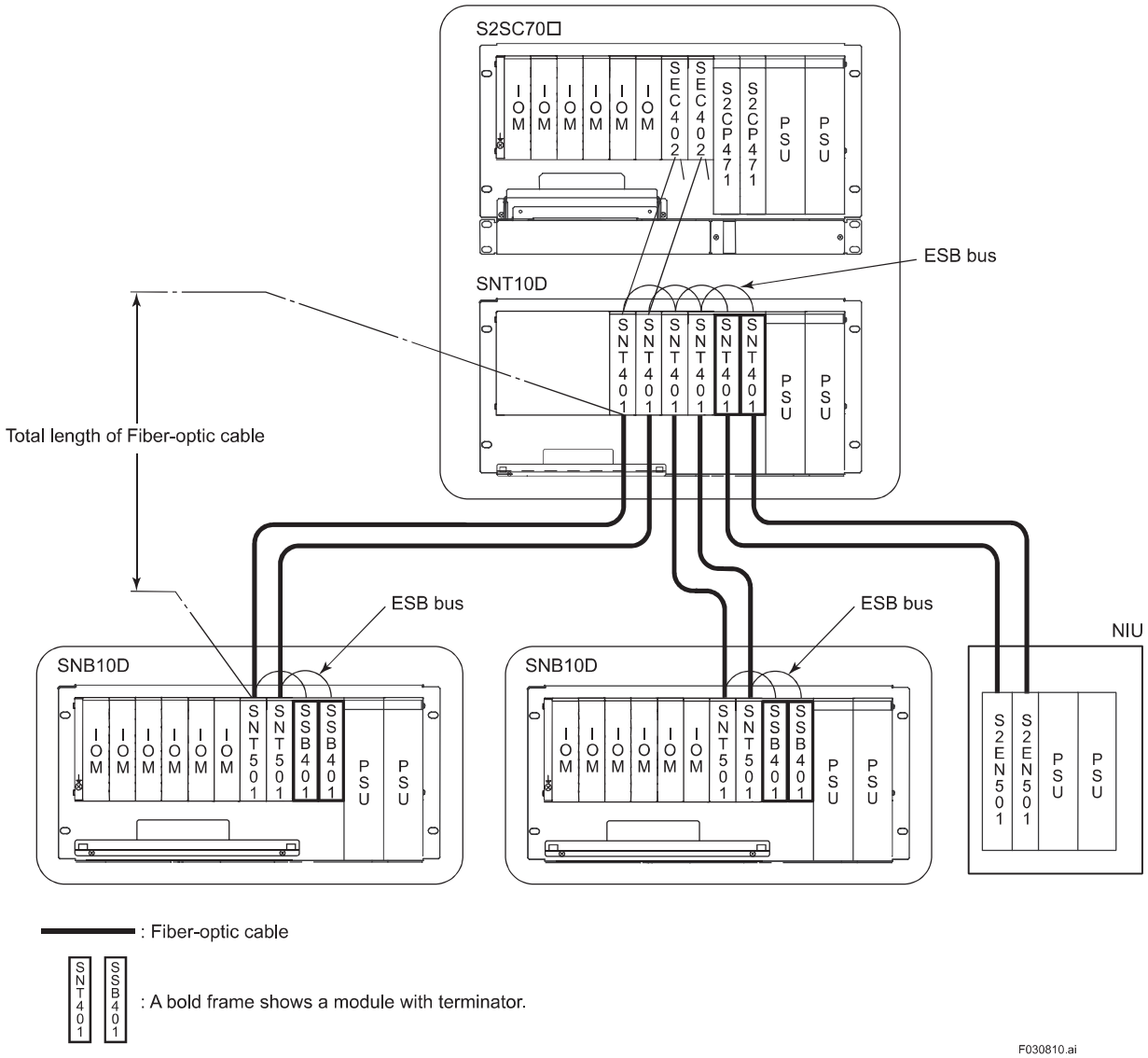
: Fiber-optic cable

: A bold frame shows a module with terminator.

F030809.ai

Figure Star Type Connection: Not Using SNT10D

Example of using SNT10D



Note: Max. five SNB10Ds are connectable to one SNT10D.

Figure Star Type Connection: Using SNT10D

Chain Type Connection

There are two structures of chain type connections: one uses the SNT10D Unit for Optical Bus Repeater Modules and the other does not use any SNT10D Unit for Optical Bus Repeater Modules.

Where No SNT10D Unit Is Used

The SNT401/SNT411 modules installed on the S2SC70☐/SSC60☐/SSC50☐/SSC57☐ Safety Control Unit as well as on the SNB10D Safety Node Unit can be chain-connected respectively to SNT501/SNT511 modules installed on the SNB10D Unit. In such a case, the number of I/O modules that can be installed on S2SC70☐/SSC60☐/SSC50☐/SSC57☐ and SNB10D is up to four and six respectively. If you have a plan to connect an SNB10D and your SNB10D with fiber-optic cables in the future, it is recommended that you reserve sufficient slots in your SNB10D for optical ESB bus repeater modules.

Example of not using SNT10D

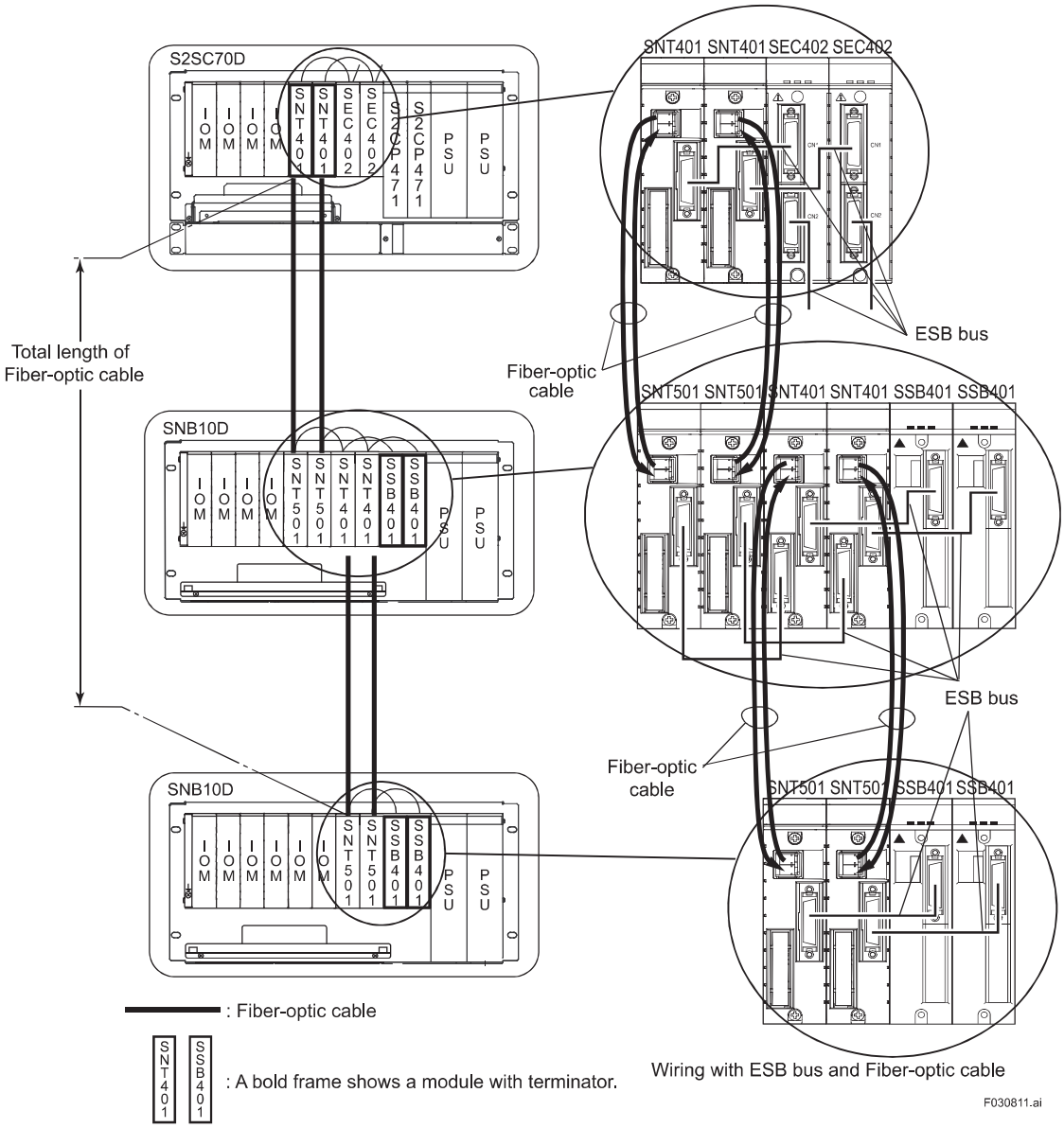


Figure Chain Type Connections: Not Using SNT10D

Where an SNT10D Unit Is Used

The SNT10D is used for S2SC70☐, SSC60☐, SSC50☐, SSC57☐, and SNB10D to allow the SNT401/SNT411 and SNT501/SNT511 modules to be chain-connected to each other. In such a case, the number of I/O modules that can be installed on each unit is six to eight. This can result in the same installation as in ESB-bus cable connections on the ESB bus.

Example of using SNT10D

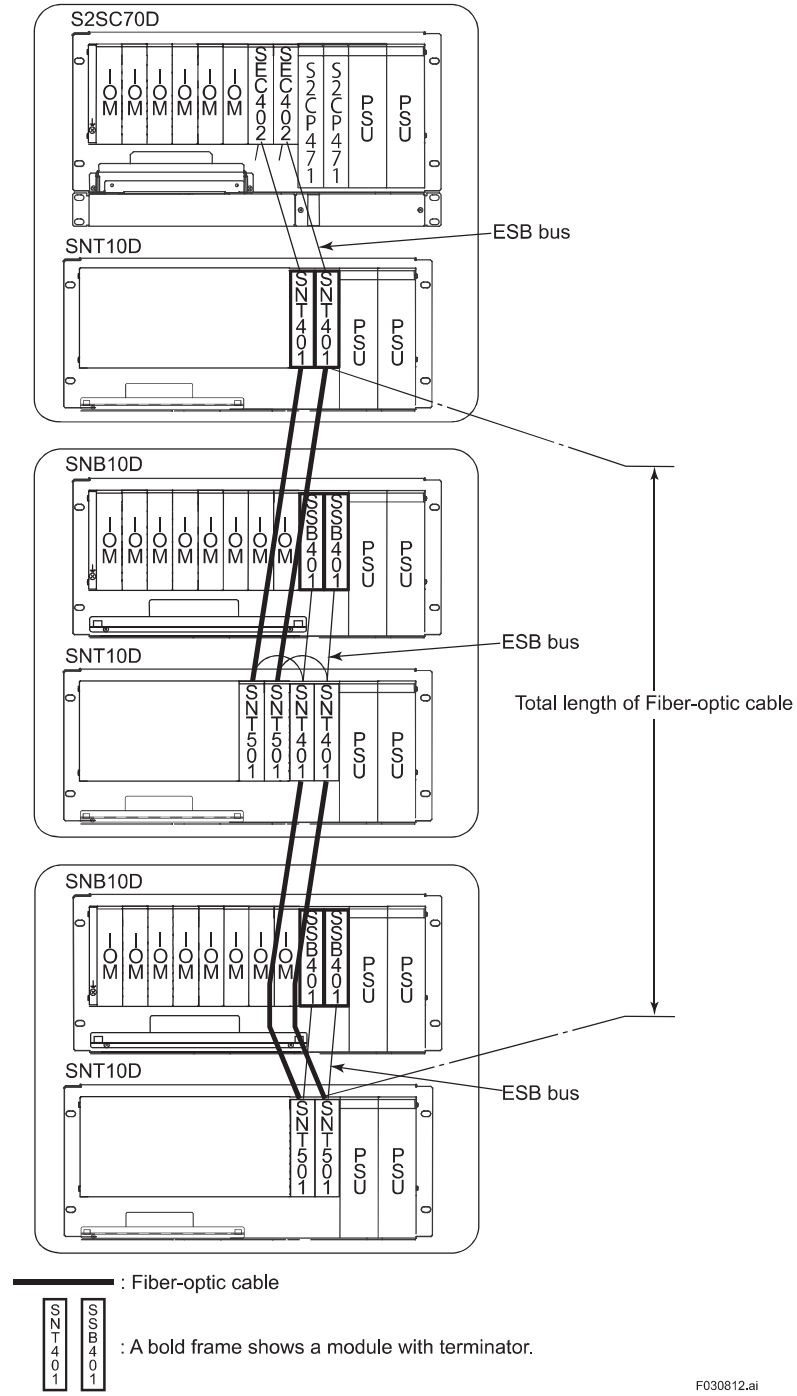


Figure Chain Type Connections: Using SNT10D

Fiber-optic Cable for Optical ESB

Specifications of Fiber-optic Cables Used in Optical ESB Bus Repeater Modules

The table below shows the specifications of the fiber-optic cables used in optical ESB bus repeater modules.

Table Specifications of Fiber-optic Cables Used in Optical ESB Bus Repeater Modules

Item	Specification
Connector	Type LC connector (IEC 61754-20-compliant product)
Cable	Silica-based single-mode fibers (JIS C6835 SSMA-9.3/125, IEC 60793-2-50B1.1)
Number of cores used	Two

Fiber-optic cables with the temperature rating of an ambient temperature plus 20 °C or more must be used.

Lay fiber-optic cables according to the manufacturer's cable handling precautions such as allowable bending radius.

Secure and wire the fiber-optic cables so as not to put extra stress on the cable trays in the units listed below:

- Safety control unit
- Safety node unit
- Unit for optical bus repeater module

3.8.5 F-SB Bus (for N-IO Node)

The following figure shows a conne.

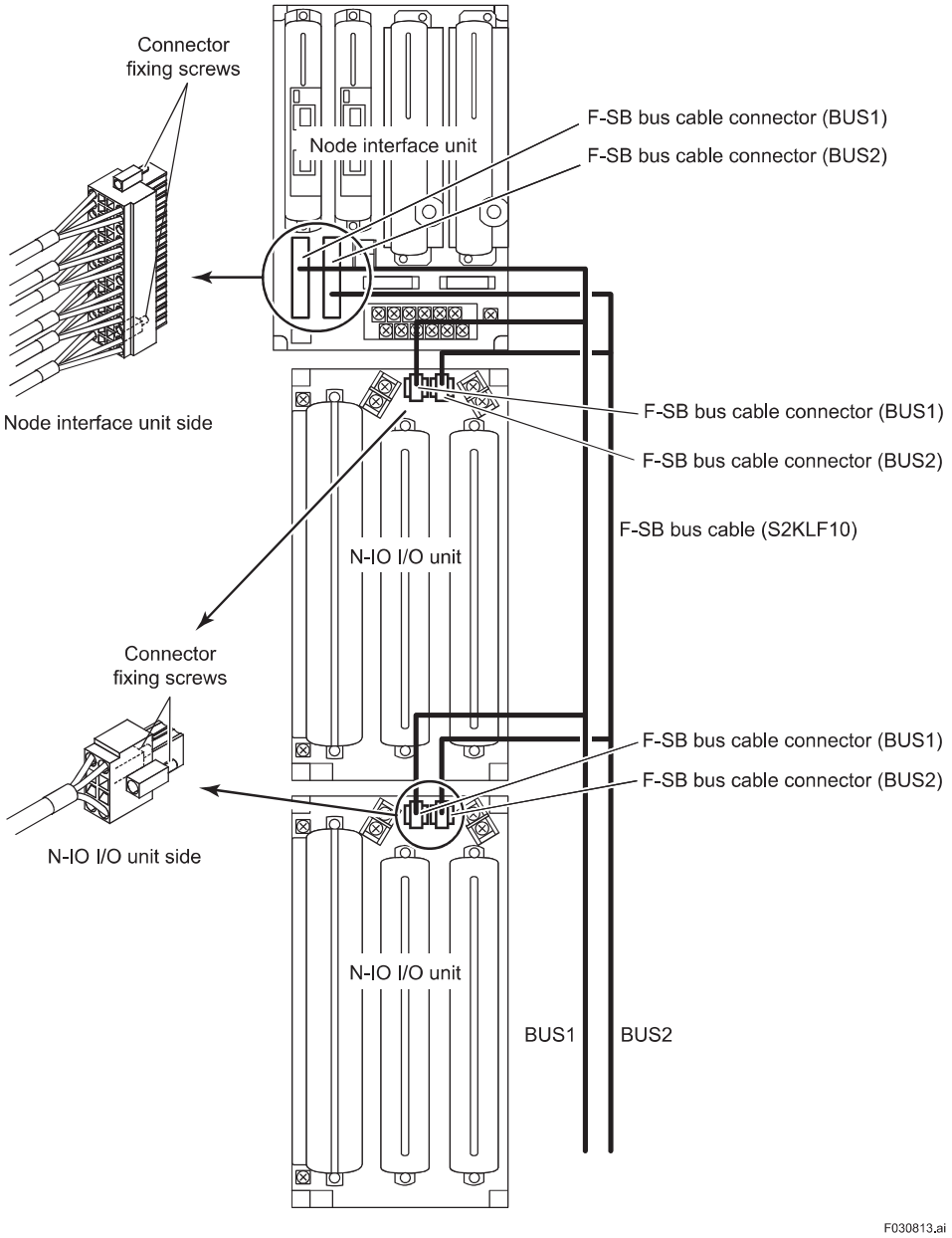


Figure F-SB Bus Connection

CAUTION

NIU and N-IO I/O Units can be installed in only the same cabinet.

When connecting a F-SB bus cable to N-IO node, ensure to keep the minimum bending radius of the cable.

The minimum bending radius of the F-SB bus cable is six-fold of the diameter of the cable.

4. Installation Specifications

This section summarizes power consumption, in-rush current, fuse (breaker) ratings, durability of parts, and other data for the installation of the ProSafe-RS system.

Electrical Specifications

Power consumption (current) and other electrical data are shown below.

Table Electrical Specifications (1/2)

Equipment	Input voltage range		Maximum power consumption/current dissipation (*1), VA, A	Heating value, J/h (*2)
	Voltage, V AC	Frequency, Hz		
SSC60S-S Safety Control Unit (for Vnet/IP)	100-120	50 or 60 ± 3	200 VA	432 x 10^3 (120 W)
	220-240		230 VA	
	24 V DC		5.5 A	
SSC60S-F Safety Control Unit (for Vnet/IP)	100-120	50 or 60 ± 3	240 VA	540 x 10^3 (150 W)
	220-240		290 VA	
	24 V DC		7.0 A	
SSC60D-S Duplex Safety Control Unit (for Vnet/IP)	100-120	50 or 60 ± 3	200 VA	432 x 10^3 (120 W)
	220-240		230 VA	
	24 V DC		5.5 A	
SSC60D-F Duplex Safety Control Unit (for Vnet/IP)	100-120	50 or 60 ± 3	240 VA	540 x 10^3 (150 W)
	220-240		290 VA	
	24 V DC		7.0 A	
SSC50S-S Safety Control Unit (for Vnet/IP)	100-120	50 or 60 ± 3	200 VA	432 x 10^3 (120 W)
	220-240		230 VA	
	24 V DC		5.5 A	
SSC50S-F Safety Control Unit (for Vnet/IP)	100-120	50 or 60 ± 3	240 VA	540 x 10^3 (150 W)
	220-240		290 VA	
	24 V DC		7.0 A	
SSC50D-S Duplex Safety Control Unit (for Vnet/IP)	100-120	50 or 60 ± 3	200 VA	432 x 10^3 (120 W)
	220-240		230 VA	
	24 V DC		5.5 A	
SSC50D-F Duplex Safety Control Unit (for Vnet/IP)	100-120	50 or 60 ± 3	240 VA	540 x 10^3 (150 W)
	220-240		290 VA	
	24 V DC		7.0 A	
SSC57S-S Safety Control Unit (for Vnet/IP-Upstream)	100-120	50 or 60 ± 3	200 VA	432 x 10^3 (120 W)
	220-240		230 VA	
	24 V DC		5.5 A	
SSC57S-F Safety Control Unit (for Vnet/IP-Upstream)	100-120	50 or 60 ± 3	240 VA	540 x 10^3 (150 W)
	220-240		290 VA	
	24 V DC		7.0 A	
SSC57D-S Duplex Safety Control Unit (for Vnet/IP-Upstream)	100-120	50 or 60 ± 3	200 VA	432 x 10^3 (120 W)
	220-240		230 VA	
	24 V DC		5.5 A	
SSC57D-F Duplex Safety Control Unit (for Vnet/IP-Upstream)	100-120	50 or 60 ± 3	240 VA	540 x 10^3 (150 W)
	220-240		290 VA	
	24 V DC		7.0 A	

*1: The power consumption in steady operation is indicated in VA (AC) or A (DC). When the power consumption varies according to the installed number of equipment, the power consumption by the maximum number of units installed is listed.

*2: The heating value in steady operation is indicated in Joule/hour. When the heating value varies according to the installed number of equipment, the heating value by the maximum number of units installed is listed.

Table Electrical Specifications (2/2)

Equipment	Input voltage range		Maximum power consumption/current dissipation (*1), VA, A	Heating value, J/h (*2)
	Voltage, V AC	Frequency, Hz		
S2SC70S-S Safety Control Unit	100-120	50 or 60 ± 3	200 VA	432 x 10^3 (120 W)
	220-240		230 VA	
	24 V DC		5.5 A	
S2SC70S-F Safety Control Unit	100-120	50 or 60 ± 3	240 VA	540 x 10^3 (150 W)
	220-240		290 VA	
	24 V DC		7.0 A	
S2SC70D-S Duplex Safety Control Unit	100-120	50 or 60 ± 3	200 VA	432 x 10^3 (120 W)
	220-240		230 VA	
	24 V DC		5.5 A	
S2SC70D-F Duplex Safety Control Unit	100-120	50 or 60 ± 3	240 VA	540 x 10^3 (150 W)
	220-240		290 VA	
	24 V DC		7.0 A	
SNB10D Safety Node Unit (with maximum number of I/O Modules Installed)	100-120	50 or 60 ± 3	200 VA	432 x 10^3 (120 W)
	220-240		230 VA	
	24 V DC		5.5 A	
SNT10D Unit for Optical Bus Repeater Module	100-120	50 or 60 ± 3	200 VA	432 x 10^3 (120 W)
	220-240		230 VA	
	24 V DC		5.5 A	
AVR10D Duplexed V net router	100-120	50 or 60 ± 3	80 VA	158 x 10^3 (44 W)
	220-240		110 VA	
	24 V DC		1.7 A	
AW810D Wide Area Communication Router	100-120	50 or 60 ± 3	80 VA	158 x 10^3 (44 W)
	220-240		110 VA	
	24 V DC		1.7 A	
S2NN30D Node Interface Unit	100-240	50 or 60 ± 3	190 VA	90 x 10^3 (25 W)
	24 V DC		150 W	
S2BN1D Base Plate	24 V DC		24 W	51 x 10^3 (14 W)
S2BN4D Base Plate for Barrier (MTL) System Power	24 V DC		24 W	51 x 10^3 (14 W)
S2BN4D Base Plate for Barrier (MTL) Barrier Power	24 V DC		38.4 W	83 x 10^3 (23 W)
S2BN5D Base Plate for Barrier (P+F) System Power	24 V DC		24 W	51 x 10^3 (14 W)
S2BN5D Base Plate for Barrier (P+F) Barrier Power	24 V DC		28.8 W	58 x 10^3 (16 W)

*1: The power consumption in steady operation is indicated in VA (AC) or A (DC). When the power consumption varies according to the installed number of equipment, the power consumption by the maximum number of units installed is listed.

*2: The heating value in steady operation is indicated in Joule/hour. When the heating value varies according to the installed number of equipment, the heating value by the maximum number of units installed is listed.

In-Rush Current for Each Component

Actual in-rush current data measured for each ProSafe-RS component is listed below.

Table System Equipment Power-On In-Rush Current

Equipment	In-rush current (A) 100 V AC		In-rush current (A) 220 V AC		In-rush current (A) 24 V DC	
	Primary	Secondary	Primary	Secondary	Primary	Secondary
SSC60S-S Safety Control Unit	62	5	124	5	30	23
SSC60S-F Safety Control Unit (Wide range temperature type)	82	9	168	8	40	23
SSC60D-S Duplexed Safety Control Unit	62	5	124	5	30	23
SSC60D-F Duplexed Safety Control Unit (Wide range temperature type)	82	9	168	8	30	23
SSC50S-S Safety Control Unit	62	5	124	5	30	23
SSC50S-F Safety Control Unit (Wide range temperature type)	82	9	168	8	40	23
SSC50D-S Duplexed Safety Control Unit	62	5	124	5	30	23
SSC50D-F Duplexed Safety Control Unit (Wide range temperature type)	82	9	168	8	30	23
SSC57S-S Safety Control Unit	62	5	124	5	30	23
SSC57S-F Safety Control Unit (Wide range temperature type)	82	9	168	8	40	23
SSC57D-S Duplexed Safety Control Unit	62	5	124	5	30	23
SSC57D-F Duplexed Safety Control Unit (Wide range temperature type)	82	9	168	8	30	23
S2SC70S-S Safety Control Unit	62	5	124	5	30	23
S2SC70S-F Safety Control Unit (Wide range temperature type)	82	9	168	8	40	23
S2SC70D-S Duplexed Safety Control Unit	62	5	124	5	30	23
S2SC70D-F Duplexed Safety Control Unit (Wide range temperature type)	82	9	168	8	30	23
SNB10D Safety Node Unit	62	5	124	5	30	23
SNT10D Unit for Optical Bus Repeater Module	62	5	124	5	30	23
AVR10D Duplexed V net router	47	1	48	0.5	10	2
AW810D Wide Area Communication Router	47	1	48	0.5	10	2
S2NN30D Node Interface Unit	40	—	80	—	60	—

Input current peak values and waveforms, influenced by input impedance, vary with system configurations, line sharing with other systems, and other factors. The rush current data shown above have been measured under the predetermined conditions (see below). Please note that the values are subject to change.

The power input circuit, with an in-rush current limiting circuit, restrains primary in-rush current, turning any current exceeding the limits to secondary and successive rush current.

Measurement Conditions

Input voltage: 132/264 V AC, 50 Hz, and 24 V DC

Line impedance: Approx. 0.4 ohms (external line impedance and internal impedance)

Turn-on timing: At 50 Hz, 90º or 5 ms after the AC zero-crossing point (60 Hz data are almost the same as the 50 Hz data shown above.)

Note

- The timing of the maximum primary/secondary in-rush current varies with devices.
- The restart in-rush current after a momentary power failure exceeds the above data and its timing is also different.
- For a system composed of multiple pieces of equipment, the in-rush current is normally smaller than the total of the in-rush currents by individual pieces of equipment.

Maximum Current Consumption of FIO Modules

Table Maximum Current Consumption of I/O Modules

Model	Name	Maximum current consumption (mA) 5 V DC	Maximum current consumption (mA) 24 V DC
Analog Input/Output Module			
SAI143-S	Analog input module (4 to 20 mA, 16 channels, Module isolation)	320	550
SAI143-H	Analog input module (4 to 20 mA, 16 channels, Module isolation, HART communication)	320	550
SAV144	Analog input module (1 to 5 V/1 to 10 V, 16 channels, Module isolation)	300	140
SAI533	Analog output module (4 to 20 mA, 8 channels, Module isolation, HART communication)	320	300
SAT145	TC/mV input module (16 channels, Isolated Channels)	400	200
SAR145	RTD input module (16 channels, Isolated Channels)	500	200
Digital Input/Output Module			
SDV144	Digital input module (non-voltage contact, 16 channels, Module isolation)	290	140
SDV521	Digital output module (24 V DC/2 A, 4 channels, Module isolation)	280	140
SDV526	Digital output module (100-120 V AC, 4 channels, Module isolation)	500	50
SDV531	Digital output module (24 V DC, 8 channels, Module isolation)	280	140
SDV53A	Digital output module (48 V DC, 8 channels, Module isolation)	290	150
SDV541	Digital output module (24 V DC, 16 channels, Module isolation)	300	150
ESB Bus Interface Module			
SNT401	Optical ESB Bus Repeater Master Module	500	0
SNT501	Optical ESB Bus Repeater Slave Module	500	0
SNT411	Optical ESB Bus Repeater Master Module 5 km - 50 km	500	-
SNT511	Optical ESB Bus Repeater Slave Module 5 km - 50 km	500	-
Communication Module			
ALR111	Serial communication module (RS-232C, 2-port)	500	-
ALR121	Serial communication module (RS-422/RS-485, 2-port)	500	-
ALE111	Ethernet communication module (1-port) (*1)	500	-
S2LP131	Fire and gas communication module (1-port) (*2)	800	-
Bus Interface Module			
SEC402	ESB Bus Coupler Module (2-Port)	500	-
SEC401	ESB Bus Coupler Module	500	-
S2EN402	N-ESB Bus Coupler Module (2-Port)	500	-
S2EN404	N-ESB Bus Coupler Module (4-Port)	500	-

*1: ALE111 is available from ProSafe-RS R3.02.00 or later with S2SC70☐, SSC60☐, SSC50☐ or SSC57☐.
*2: S2LP131 is available from ProSafe-RS R4.05.00 or later with S2SC70☐.

Maximum Current Consumption of N-IO

Mode	Name	Max current consumption 24 V DC (A)
S2BN1D	Base Plate (Field Power Supply)	11 A
S2BN4D	Base Plate for Barrier (Barrier Power Supply)	1.6 A
S2BN5D	Base Plate for Barrier (Barrier Power Supply)	1.8 A

Fuse (Breaker) Specifications

Fuse (breaker) ratings are listed below.

Table Fuse (Breaker) Ratings

Equipment	Built-in fuse rating (A/V)	External breaker rating (A/V) (*1)
SNT10D Unit for Optical Bus Repeater Module (for 100 V or 220 V AC power supply)	6.3/250	15/250
SNT10D Unit for Optical Bus Repeater Module (for 24 V DC power supply)	10/250	20/250
SSC60S/SSC60D Safety Control Unit (for 100 V AC power supply)	6.3/250	15/250
SSC60S/SSC60D Safety Control Unit (for 220 V AC power supply)	6.3/250	15/250
SSC60S/SSC60D Safety Control Unit (for 24 V DC power supply)	10/250	20/250
SSC50S/SSC50D Safety Control Unit (for 100 V AC power supply)	6.3/250	15/250
SSC50S/SSC50D Safety Control Unit (for 220 V AC power supply)	6.3/250	15/250
SSC50S/SSC50D Safety Control Unit (for 24 V DC power supply)	10/250	20/250
SSC57S/SSC57D Safety Control Unit (for 100 V AC power supply)	6.3/250	15/250
SSC57S/SSC57D Safety Control Unit (for 220 V AC power supply)	6.3/250	15/250
SSC57S/SSC57D Safety Control Unit (for 24 V DC power supply)	10/250	20/250
S2SC70S/S2SC70D Safety Control Unit (for 100 V AC power supply)	6.3/250	15/250
S2SC70S/S2SC70D Safety Control Unit (for 220 V AC power supply)	6.3/250	15/250
S2SC70S/S2SC70D Safety Control Unit (for 24 V DC power supply)	10/250	20/250
SNB10D Safety Node Unit (for 100 V or 220 V AC power supply)	6.3/250	15/250
SNB10D Safety Node Unit (for 24 V DC power supply)	10/250	20/250
AVR10D Duplexed V net router (for 100 V or 220 V AC power supply)	3.15/250	10/250
AVR10D Duplexed V net router (for 24 V DC power supply)	6.3/250	15/250
S2NN30D Node Interface Unit (100-240 V AC system)	5/250 (fuse)	15/250
S2NN30D Node interface Unit (24 V DC)	12/250 (fuse)	30/24
S2BN1D Base Plate with disconnecting terminal	—	—
S2BN4D Base Plate for Barrier (MTL): Barrier Power Input (24 V DC)	2.5/250 (fuse)	—
S2BN5D Base Plate for Barrier (P+F): Barrier Power Input (24 V DC)	3.15/250 (fuse)	—

*1: Recommended.

Durability of Parts

Some hardware components require periodical replacement. As a guideline to the intervals between preventive maintenance checks, the following table lists components with life span of less than 10 years. Users should replace the components indicated by a cross mark X during the preventive maintenance check. For other components, users should not attempt to replace them; contact Yokogawa for replacement.

Note: Random failures within the recommended replacement intervals may occur in some parts.

IMPORTANT

Parts reliability and durability depends much on environment in which they are used. Even within a range of environmental requirements, it is still important to be used in “desirable environment” to enhance reliable operation and durability.

For example, when a device whose temperature range is 5-40 degrees centigrade is used always in 35 degrees centigrade, its estimated failure rate is generally almost doubled and durability decreases by almost half, compared to the same device used in 25 degrees centigrade.

If there are corrosive gases; moreover, they promote corrosion of contact parts and printed circuit boards and their durability is shortened, compared to those in cleaner atmosphere. If there is more dust; in addition, we have to shorten the cleaning and replacement cycle for filters.

Control Devices (S2SC70☐, SSC60☐, SSC50☐, SSC57☐, and SNB10D)

Component	Part number	Recommended replacement period	Replacement by user	Remarks
Power Supply Module (100-120 V AC power supply)	SPW481	8 years	X	Average ambient temperature of 40ºC or lower
Power Supply Module (220-240 V AC power supply)	SPW482	8 years	X	Average ambient temperature of 40ºC or lower
Power Supply Module (24 V DC power supply)	SPW484	8 years	X	Average ambient temperature of 40ºC or lower
Battery Pack	S9185FA (*2)	3 years	X	Average ambient temperature of 30ºC or lower (*1)
		1.5 years	X	Average ambient temperature of 40ºC or lower (*1)
		9 months	X	Average ambient temperature of 50ºC or lower (*1)
	S9450FE (*3)	3 years	X	Average ambient temperature of 30ºC or lower (*1)
		1.5 years	X	Average ambient temperature of 50ºC or lower (*1)
		1 year	X	Average ambient temperature of 70ºC or lower (*1)
Aluminum Electrolytic Capacitor	–	8 year	–	For SPW481, SPW482, and SPW484 power supply modules and power supply units for fan units (S9159FA and S9160FA) Average ambient temperature of 40ºC or lower
Built-in Fuse	S9109VK	8 years	–	For SPW481 power supply module
	S9109VK	8 years	–	For SPW482 power supply module
	A1546EF	8 years	–	For SPW484 power supply module
Fan Unit	AIP602	4 years	X	Average ambient temperature of 60ºC or lower

X: Can be replaced. –: Cannot be replaced.
*1: Including temperature during storage.
*2: For Safety Control Unit with SCP461 and SCP451.
*3: For Safety Control Unit with S2CP471.

Unit Devices (SNT10D Unit for Optical Bus Repeater Module)

Component	Part number	Recommended replacement period	Replacement by user	Remarks
Power Supply Module (100 - 120 V AC power supply)	SPW481	8 years	X	Average ambient temperature of 40ºC or lower
Power Supply Module (220 - 240 V AC power supply)	SPW482	8 years	X	Average ambient temperature of 40ºC or lower
Power Supply Module (24 V DC power supply)	SPW484	8 years	X	Average ambient temperature of 40ºC or lower
Aluminum Electrolytic Capacitor	–	8 years	–	For SPW481, SPW482, and SPW484 power supply module Average ambient temperature of 40ºC or lower
Built-in Fuse	S9109VK	8 years	–	For SPW481 power supply module
	S9109VK	8 years	–	For SPW482 power supply module
	A15456EF	8 years	–	For SPW484 power supply module
SFP optical module (*1)	–	–	–	Recommended replacement period – every four years if in a G3 environment

X: Can be replaced.
–: Cannot be replaced.
*1: Applies to SNT401, SNT411, SNT501, and SNT511.

Control Devices (AVR10D, AW810D)

Part names	Part numbers	Recommended replacement cycle	Replacement by user	Remarks
Aluminum Electrolytic Capacitor	–	8 years	–	For PW441, PW442, PW444 Average ambient temperature of 40ºC or lower
Built-in power fuse	S9109VK	8 years	–	For PW441, PW442, PW444

–: Cannot be replaced.

S2NN30D

Table Periodic Replacement Parts Having Defined Life Spans

Part names	Part numbers	Recommended Replacement Interval	Replacement by user	Remarks
Power Supply Unit (100-240 V AC)	S2PW503	8 years	Yes	Average ambient temperature 40 °C or less
Power Supply Unit (24 V DC)	S2PW504	8 years	Yes	Average ambient temperature 40 °C or less
Bus Module	S2EN501-S1□□□□ S2EN501-S2□□□□ S2EN501-S□1□□□ S2EN501-S□2□□□	4 years	Yes	In the G3 environment, replacement is recommended due to corrosion of the SFP and SFP connectors.

5. Post-installation Inspection and Environmental Preservation

Post-installation Inspection

Upon the completion of installation of the instrumentation, before turning on the power inspect the items listed below to avoid contaminating the system with dust or condensation.

Table Inspection before Power On

	Inspection items (daily inspection/maintenance items)
Environment	☐ No water intrusion from cable ducts. ☐ No wind/rain blowing in ☐ Air-conditioned ☐ Cable ducts and cabinet bottoms covered to prevent entry of wind, dust, moisture ☐ Cabinets and surroundings cleaned ☐ No dust entering from air vents ☐ Free of salty, ferrous, corrosive gas ☐ No direct sunlight on equipment
Equipment	☐ No condensation or traces on cabinet interior/exterior ☐ No discoloration or rust on cabinet interior/exterior ☐ No condensation or traces on modules (disconnect cards on the upper, middle, and lower stands, and left and right sides of the cabinet to check that there is no condensation on the modules or defects anywhere in the cabinet.) ☐ No dust remaining inside cabinet

It is recommended that you turn on the power in the presence of Yokogawa when turning it on first.

Post-installation Environment Preservation

The following precautions should be taken to preserve the proper operating environment after the system has been installed:

- Seal the pits if they are shared by equipment in other rooms, preventing entry of dust and moisture from the other rooms.
- Seal all cable ducts of equipment and building with putty upon completion of cabling.
- Always turn on air conditioner. Turning it on/off may cause condensation inside equipment. If you turn on the power of an air conditioner after a long stop, turn on the air conditioner first and the system. Otherwise condensation may occur.
- Monitor and record the room ambient temperature and humidity. To maintain the reliability of the equipment, be sure to remove the cause if they fluctuate violently.
- Note that leaving exits and entrances open during installation, or leaving open cable ducts whiles pulling cables, may result in condensation.

Revision Information

- Title : ProSafe-RS Installation Guidance
- Manual No. : TI 32P01J10-01EN

Nov. 2020/15th Edition
1.8 Compliance with Marine Standards
■ Marine Standard-compliant ProSafe-RS Components [Added S2SC70☐ (with S2CP471), SSC60☐ (with S2CP471), S2CP471, S2BN1D-☐9, A2BM4. Deleted YCB146 and YCB128.]
■ Installation of Ferrite Cores for Vnet/IP [Added S2CP471.]

July 2020/14th Edition
1.2 Control Room Environment
■ Conformity Standards [Added ECAS-Ex Type "n"]

May 2020/13th Edition
1.2 Control Room Environment
Installation Specification [Note for S2LP131 was deleted.]
3.5 Connecting Signal Cable
■ Process I/O Signal Connection [Note added]

Mar. 2020/12th Edition
Introduction Updated descriptions of trademark.
3.2 Connecting Power
● Sleeve Terminal Processing [Table for sleeves was revised.]
3.5 Connecting Signal Cable
● Pressure Clamp Terminal (for Pressure Clamp Terminal Block) (for terminal block, terminal board, and relay board) [Table for sleeves was revised.]
● Pressure Clamp Terminal, Spring Clamp Terminal (for N-IO Node) [Table for sleeves was revised.]
3.6.2 Signal Cable Connections
Table Signal Cable Connections for I/O Modules [Note of S2LP131 was revised.]
4. Installation Specifications
Table Maximum Current Consumption of I/O Modules [Note of S2LP131 was revised.]

Jan.2020/11th Edition
Introduction Updated descriptions of trademark.
1.2 Control Room Environment
■ Conformity Standards [Added C-tick Marking]

Nov. 2019/10th Edition
Safety Precautions Descriptions of symbols are revised.
1.5 Noise Countermeasures [Changed spark killer to RC network]
1.8 Compliance with Marine Standards
Table Marine Standard-compliant ProSafe-RS Components [Added S2CP471]
2.5.5 Installation Guideline for Cabinet (FIO)
Table Number of Nodes to Be Installed and Need to Install Fans [Changed SSC60☐-F to S2SC70☐-F]
3.4 Power and Ground Cabling
Figure Example of N-IO Node devices Installation and grounding wiring [Revised]
Figure 19-inch Rack-mount Devices and Wiring [Revised]
3.6.3 Connecting Signal Cables to I/O Modules
■ Connecting Signal Cables to Analog Input Modules [Added how to connect Three-wire transmitter]
3.8 Connecting Bus Cable [Removed CP461 and CP451 from the figures]
4. Installation Specifications
■ Durability of Parts [Added S9450FE, Deleted A1159EM]

Mar. 2019/9th Edition
1.2 Measurement Categories [Updated the description of safety standard.]
Conformity Standards [Updated the description of safety standard.]
1.5.1 Examples of Spark-killer and Diode Installation [Added note *2.]
1.8 Compliance with Marine Standards [Added ENV3 to LR.]

Table Marine Standard-compliant ProSafe-RS Components (1/3) [Added the description of S2BN1D.]
Precaution on Installing Components [Add explanation.]
Figure Wiring for power cables [Updated the figure.]
Figure Locations of Ferrite Core Installation for Input/Output Modules, Terminal Boards and Relay Boards [Added note *2.]
When Leaving a Large Space between Unit Components [Added the specification of EMI shielding gasket.]
2.5.6 Installation Guideline for Rittal cabinet for N-IO [Updated the specification for cabinet.]

Jan. 2019/8th Edition
1.2 Control Room Environment
■ Conformity Standards
● Application Standards [Notes on surge immunity are changed]
● EMC Conformity Standards [Notes on surge immunity are changed]
1.5.2 Countermeasures against Static Electricity [Arrangement Information of wrist straps and conductive sheets are deleted]
1.7 Corrosive-gas Environment Compatibility
■ Outline of G3 Environment Compatibility [Contact information for environmental diagnosis is deleted]
2.2 Unpacking
IMPORTANT [Contact information for Condensation is deleted]

Oct. 2018/7th Edition
Front page ProSafe-RS Logo change
Safety Precautions Revision of logo mark description
1.2 Control Room Environment [Add note]
1.7 Table G3 Environment-compatible Products[Add A2BM4]
2.5.3 DIN Rail Mountable Devices [Add A2BM4 and S1XEU4D]
2.5.4 Wall Mountable Devices [Add A2BM4]
2.5.6 Figure Example of Mounting an SCU for N-IO and N-IO Nodes in a Cabinet is revised
Example of Mounting an SCU for N-IO and N-IO Nodes in a Cabinet (In case of field wiring via terminal board) is added
Example of Mounting N-IO Nodes (Non-Intrinsic Safety Barrier) in a Cabinet (In case of field wiring via terminal board) is added
3.1 Cables and Terminals [Add A2BM4]
3.4 Power and Ground Cabling [Add S2BN1D and A2BM4]
3.5 Connecting Signal Cable [Add description for field wiring]
[Add A2BM4]
3.7.2 Base Plate [Add S2BN1D-□9□□□ and note]
[Add figure of A2BM4]
3.7.3 Base Plate for Barrier [Clerical error correction]
4. Installation Specifications [Clerical error correction]

Mar. 2018/6th Edition
1.2 Control Room Environment ["ground" is change to "grounding"]
1.3 Notes for the field power supply unit of N-IO is added.
1.5.1 Eamples of Spark-killer and Diode Installation [Title is changed]
1.8 S2LP131 is added.
2.5.3 Figure Mounting stopper to the DIN rail is revised.
2.5.6 Example of Mounting an SCU for N-IO and N-IO Nodes in a Cabinet
[Mounting conditions are corrected.]
Example of Mounting N-IO Nodes (Non-Intrinsic Safety Barrier) in a Cabinet
[Mounting conditions are corrected.]
Example of Mounting N-IO Nodes (Intrinsic Safety Barrier) in a Cabinet
[Mounting conditions are corrected.]
3.5 Figure Area for Signal Cable from Field is revised.
Figure Example of Node Interface Unit and I/O Unit Cable Wiring (Cabinet) is revised.
Figure Example of Node Interface Unit and I/O Unit Cable Wiring (Junction Box) is revised.

Nov. 2017/5th Edition
1.2 S2LP131 is added.
1.7 S2LP131 is added.
1.8 Clerical error correction.

2.3 Notice for storage is added.
3 Figure of SBM54D is revised.
3.6.2 S2LP131 is added.
4. S2LP131 is added.
Clerical error correction.

June 2017/4th Edition
1.2 Safety Standards [CSA] is revised.
1.8 Clerical error correction.
3.2 Clerical error correction.
3.5 Clerical error correction.
3.8.3 Notice for N-ESB bus is revised.

Apr. 2017/3rd Edition
1.2 Clerical error correction.
1.5.1 Example of spark-killer installation for N-IO is added.
1.7 S2MDV843 is added.
1.8 S2MDV843 is added.
3.2 Clerical error correction.
3.7 S2MDV843 is added.
Clerical error correction.

Oct. 2016/2nd Edition
Safety Precautions [Symbol definitions were revised]
Symbol Marks of this Technical Information [Symbol marks were chaged]
1. System Installation Requirements
1.2 Control Room Environment
Installation Specification [Alt. 3000m was added]
Applied Standards
EMC Conformity Standards [The errors on notes were corrected]
Standard for Hazardous (Classified) Locations [Standards were added]
Marine Standards [DNV GL was added]
Installation Environment Specifications
Table Installation Environment Specifications [Alt. 3000m was added]
1.8 Compliance with Marine Standards [DNV GL was added] [N-IO models were added]
Table Marine Standard-compliant ProSafe-RS Components
[The suffix code limitation was added to AVR10D]
2. Transportation, Storage and Installation
2.5 Installation
2.5.3 DIN Rail Mountable Devices [Models were added]
2.5.4 Wall Mountable Devices [Mounting method of S2BN4D was revised]
[Grounding method was revised]
2.5.6 Installation Guidelin for Cabinet (N-IO) [Section was added]

Nov. 2015/1st Edition
Newly published

Written by Yokogawa Electric Corporation

Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Subject to change without notice.

Attachment 9.14 Security Standard of System Product

TI 33Y01B30-01EN

Technical Information

Security Standard of System Product

TI 33Y01B30-01E

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

TI 33Y01B30-01E
©Copyright Aug. 2006 (YK)
7th Edition Nov. 2019 (YK)

Blank Page

Introduction

This document is a guide to the security countermeasures that can be used to protect the production control system from threats and reduce the risks for assets related to production activities. In this document, risks and measures are explained in generalized terms as much as possible, and the security control techniques are explained and referenced to industry standard models.

To cope with the growing threats, this guide will be revised as necessary. Also, there are other documents for each product to describe the detailed implementation procedures.

Target Products

This document is written for the following system products. However, the general explanations can be used for other equipments and software products.

- Integrated Production Control System — CENTUM VP
- Safety Instrumented System — ProSafe-RS
- Network Based Control system — STARDOM
- Plant Resource Manager — PRM
- Paper Quality Measurement and Control System — B/M9000 VP
- Solution-Based Software Packages
  - OPC Interface Package — Exaopc
  - Plant Information Management System — Exaquantum
  - Operation Efficiency Improvement Package — Exapilot
  - Event Analysis Package — Exaplog
- SCADA Software — FAST/TOOLS

Trademark Acknowledgements

The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

All Rights Reserved Copyright © 2006, Yokogawa Electric Corporation

Blank Page

Security Standard of System Product

TI 33Y01B30-01E 7th Edition

CONTENTS

1. Quick Start 1-1
2. Necessity for Security 2-1
3. Security Standards and Certifications 3-1
   - 3.1 ISMS 3-2
   - 3.2 CSMS 3-8
   - 3.3 NIST 3-9
   - 3.4 ISASecure 3-10
   - 3.5 ISA99 3-10
   - 3.6 IEC 62443 3-12
4. Security Control 4-1
   - 4.1 Basic Strategy 4-2
   - 4.2 Network Architecture 4-4
     - 4.2.1 Network Segmentation 4-4
     - 4.2.2 Classification of Devices Composing the System 4-6
     - 4.2.3 Access Control by Firewall 4-7
     - 4.2.4 Dual-Home Server 4-8
     - 4.2.5 OPC Interface 4-9
     - 4.2.6 Application of Wireless Networks 4-10
     - 4.2.7 Remote Monitoring 4-15
     - 4.2.8 Remote Maintenance 4-18
   - 4.3 Anti-malware Software 4-21
     - 4.3.1 Antivirus Software 4-21
     - 4.3.2 Whitelisting Software 4-22
   - 4.4 Security Updates Management 4-23
   - 4.5 System-Hardening 4-24
     - 4.5.1 System-Hardening of PC Components 4-24
     - 4.5.2 System-Hardening of Network Devices 4-25
   - 4.6 Monitoring the System and the Network 4-28
     - 4.6.1 Audit Logs 4-28
     - 4.6.2 IDS/ IPS 4-29
     - 4.6.3 NMS 4-31
   - 4.7 Windows Domain Management 4-32

4.8 Security Function of Yokogawa System Products 4-34
4.8.1 CENTUM VP 4-38
4.8.2 ProSafe-RS 4-40
4.8.3 STARDOM 4-41
4.8.4 Plant Resource Manager (PRM) 4-42
4.8.5 B/M9000 VP 4-43
4.8.6 Exaopc 4-44
4.8.7 Exaquantum 4-45
4.8.8 Exapilot 4-46
4.8.9 Exaplog 4-48
4.8.10 FAST/TOOLS 4-49
4.9 Staff Security Policy 4-50
4.9.1 Education 4-50
4.9.2 Training 4-50
5. Physical Protection 5-1
5.1 Define Physical Boundary 5-2
5.2 Management of Removable Devices 5-4
5.3 Third Party Maintenance 5-5
6. Business Continuity Plan 6-1
6.1 Plan 6-2
6.2 Training 6-3
6.3 Maintenance 6-4
6.4 Measures against Software Vulnerability 6-5

1. Quick Start

First we will show the outline of the network configurations of the system for which this document is written and the sections where each configuration is described in this document. Please use this part as a navigator to the contents of this document.

Outline of the configuration

Chapter 2 : Necessity for Security

In this chapter, the outline of the environment surrounding the production control system is shown. The assets that should be protected by security measures and examples of security risks will be explained.

Chapter 3 : Security Standards and Certifications

In this chapter, frameworks and standards are explained when security measures are applied to IACS (*1).

*1: IACS is an abbreviation for “Industrial Automation and Control System(s).” It is a generic name for industrial control systems,and it consists of control systems such as DCS, SIS, PLC, SCADA, networked electronic sensing, and monitoring diagnostic systems. This term is often used in security related documents for control systems.

Chapter 4: Security control

The main theme of this chapter is technical security measures. Please see “Figure Outline of the system” for the description and its actual application to the system configuration.

Chapter 5: Physical protection

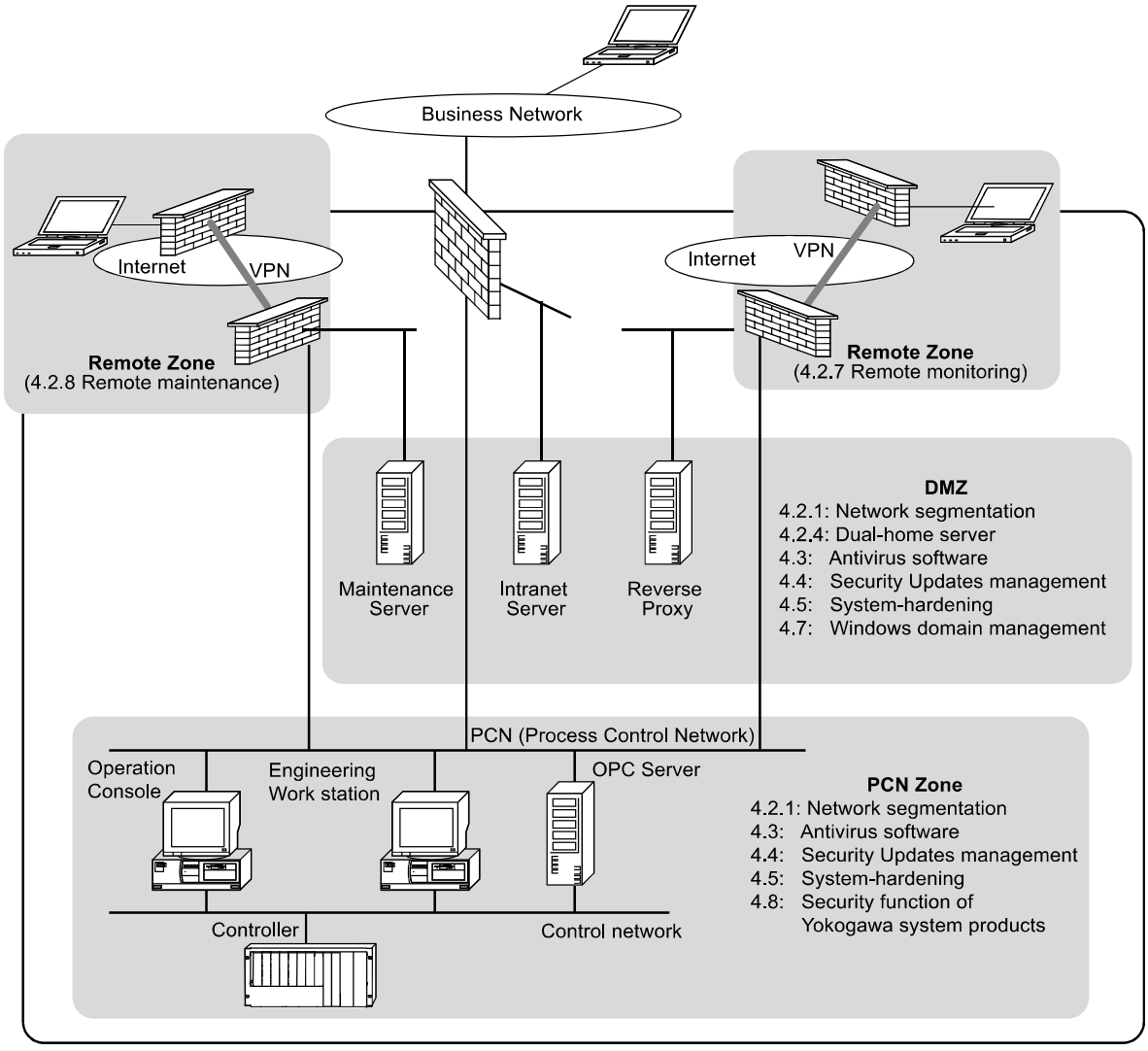
In this chapter, the consideration of physical protection of instruments is explained.

Chapter 6: Business continuity plan

In this chapter, we provide the users with information about what is to be planned for the time when the security incidents should happen and result in damages.

Sections where each configuration is described

Guide about system configuration



F0101E.ai

Figure Outline of the system

Guide about management of systems

3: Information Security Management System (ISMS)

4.9: Staff Security Policy

5: Physical Protection

6: Business Continuity Plan

Glossary

The following table describes the terms commonly used in this document.

Table Glossary terms(1/2)

Term	Description
ANSI	Abbreviation for “American National Standards Institute.”
CSMS	Abbreviation for “Cyber Security Management System.” It is modified from ISMS for control systems. It is standardized by ISA99 (to IEC 62443).
DCS	Abbreviation for “Abbreviation for “Distributed Control System.” In Yokogawa products, CENTUM VP falls under this category.
DMZ	Abbreviation for “Demilitarized Zone.”
DoS	Abbreviation for “Denial of Service.” It is an attack that sends a large (meaningless) service connection request to various servers such as Web server, FTP server, mail server, etc., increases the load on the server, causes the server to go down due to overload, or hinders in services for other legitimate users.
EDSA	Abbreviation for “Embedded Device Security Assurance.” It is a certification program for control devices. Originally, it was a certification program based on ISA99 by ISCI, and called as "ISASecure EDSA certification. It is now proposed as IEC 62443-4.
ENG	Engineering Station of CENTUM VP.
FCS	Field Control Station of CENTUM VP.
HIS	Human Interface Station of CENTUM VP.
HMI	Abbreviation for “Human-Machine Interface.”
IACS	Abbreviation for “Industrial Automation and Control Systems.” It is a term used in ISA99 and IEC 62443, and it means a generic expression for industrial control systems. It includes DCS, SIS, PLC, SCADA, SBP. Moreover, advanced control solutions, manufacturing execution system (MES), etc. are included.
ICS	Abbreviation for “Industrial Control System.” This term is used in NIST, etc. It is the same meaning as PCS in this document.
IEC	Abbreviation for “International Electrotechnical Commission.”
IPS	Abbreviation for “Intrusion Prevention/Protection System.” It is a real-time system that detect an intrusion to networks or servers, defends by cutting off connections, informs administrators, and outputs logs. The one that has an intrusion detection function only is called "Intrusion Detection System (IDS)."
ISA	Abbreviation for “International Society of Automation.” Originally, it was "Instrument Society of America," but changed to "The Instrumentation, Systems, and Automation Society" in 2000. Moreover, it has changed to the current name in 2008.
ISA99	It points to ANSI/ISA-99 series "Security for Industrial Automation and Control Systems." It was called ISA-SP99 before. At present, ISA-99 is unified to IEC 62443. In accordance with this situation, its ISA number has changed from ISA-99 to ISA-62443.
ISCI	Abbreviation for “ISA Security Compliance Institute.” It is a subordinate organization of ISA, and specialized in security.
ISMS	Abbreviation for “Information Security Management System.” It is organized security measures for general information systems. It became an international standard as the ISO/IEC 27000 series.
NIST	Abbreviation for “National Institute of Standards and Technology” in USA.
NMS	Abbreviation for “Network Management System.” It manages network devices and network information (IP address, port connection information, circuit information, etc.), and grasps the operating situation and an omen of disorder in real-time.
OPC	Abbreviation for “Open Productivity & Connectivity.” At first, it was used as an abbreviation for "OLE for Process Control," but it was changed to the current name in 2008.
PCN	Abbreviation for “Process Control Network.” A control bus used by DCS and SIS. This term is defined in this document.
PCS	Abbreviation for “Production Control System.” It includes DCS and SIS. This term is defined in this document.
PLC	Abbreviation for “Programmable Logic Controller.” In Yokogawa products, FA-M3 falls under this category.

Table Glossary terms (2/2)

Term	Description
RAS	Abbreviation for “Remote Access Server.”
SBP	Abbreviation for “Solution-Based Package.” In Yokogawa products, Exa series software falls under this category.
SCADA	Abbreviation for “Supervisory Control and Data Acquisition.” In Yokogawa products, FAST/TOOLS falls under this category.
SCS	Safety Control Station of ProSafe-RS.
SENG	Safety Engineering Station of ProSafe-RS.
SIS	Abbreviation for “Safety Instrumented System.” In Yokogawa products, ProSafe-RS falls under this category.
VPN	Abbreviation for “Virtual Private Network.”

2. Necessity for Security

Along with the recent advancement in network and information technologies, latest production control systems have adopted open technologies used in information systems, such as OS and communication protocols. It is an accelerating factor for establishing close connections between information systems and production control systems.

On the other hand, in this kind of open environment, production control systems are targeted by malicious attackers represented by computer viruses and others that cause hazardous incidents.

Nowadays, security threats aimed at production control systems are increasing by malwares (i.e. worms, viruses, Trojan horse, etc.) and appearance of Advanced Persistent Threats (APT) (i.e. targeted attacks).

In order to operate industrial plants and factories in safe and stable conditions, it is inevitable to protect the plants' production equipment.

The assets to protect

Followings are examples, but not limited to, of the important assets related with the activities of production.

Examples of data assets

- Production schedules information
- System configuration
- Application configuration
- Tuning parameters for control
- Recipes information
- Audit trails information

Example of instrument assets

- Engineering work stations
- Operator consoles
- Controllers
- Field instruments
- Network devices

Example of human and environmental assets

- Employees
- Factories and plants
- Natural environment

When the security of the assets mentioned above is threatened, it will lead to:

- the confusion and interruption of the production activities
- the leakage of the confidential information such as recipes that may affect the production activities
- the damages to human beings
- the destruction of factories and plants
- the destruction of the environment

Such consequences can bring a lot of harm to the enterprises.

The goal of the security measures is to protect such assets from the threats and to help the enterprises reduce the risks of losing property.

TIP

The standard of "ISA 99.00.01-2007: Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts, and Models" is referenced by this document. Hereinafter, this standard will be referred to as ISA 99.00.01

TIP

In ISA 99.00.01 standard, the Asset-Based criteria have defined what assets to be protected and the Activity-Based criteria have defined the activities. These criteria are referenced by this document.

TIP

Moreover, this document consults "ANSI/ISA-99.02.01-2009: Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program," and standards/draft of "ISA/IEC 62443." Security related information that is opened to the public on the Internet is referred too.

3. Security Standards and Certifications

In the industrial control system, various standards have been independently established for each industry and region in the past. However, the adoption of open technologies such as UNIX / Windows and Ethernet has led to common problems such as security vulnerabilities.

ISA (International Institute of Measurement and Control), which is mainly based in the United States, has been addressing this problem from an early stage. As a security standard for production control systems (DCS, PLC, SCADA), standardization began as ISA SP 99 in 2002. After that, the ISA 99 was compiled as a security standard that supervises the control system (= IACS) including not only a single control device, but also the surrounding IT equipment and MES (Manufacturing Execution System).

Meanwhile, IEC (International Electrotechnical Commission) was independently aiming to formulate standards related to the security of industrial control systems. However, it has not progressed quite easily, and the whole industry has become an era to strongly demand security standards. Therefore, IEC 62443 was enacted in a form to incorporate the preceding ISA 99 almostly.

Conversely, the ISA side also changed the ISA 99 to ISA 62443 in a form adjusted to the IEC number. Therefore, now it is becoming written as ISA/IEC 62443.

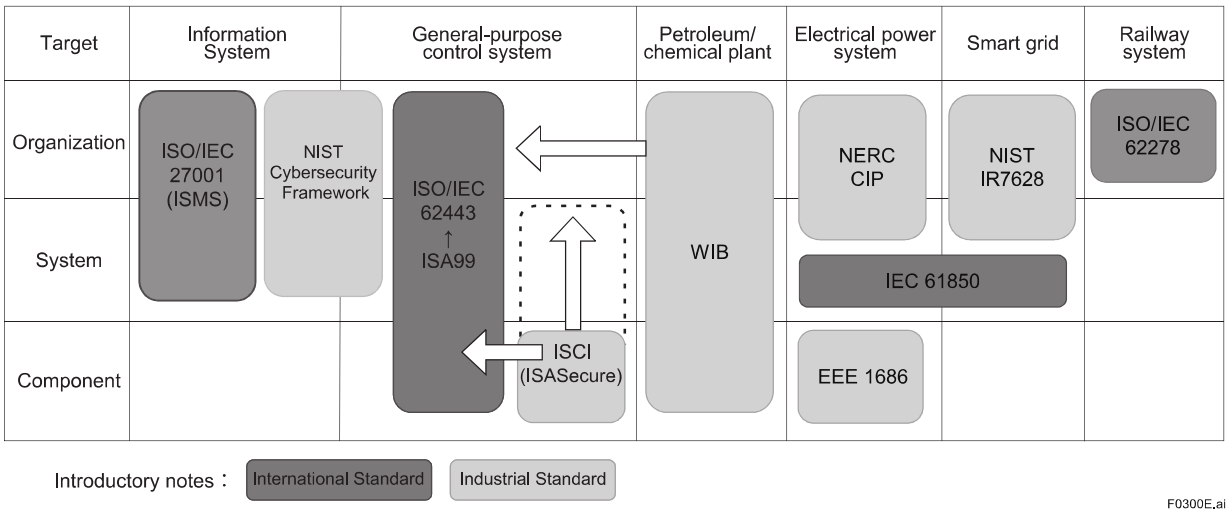


Figure International/Industrial standards for IACS

This chapter introduces the overview of the standards related to the security of industrial control systems. Because the security related information changes quickly, the contents of this document may not be up-to-date. Organizations involved in industrial control systems are constantly required to observe their trends and to respond to the times.

3.1 ISMS

The threats to the information system are increasing day by day and one after another new threats are emerging. Therefore, the security measures need to be reconsidered all the time. This program is called Information Security Management System (ISMS). It is a management framework for an information system based on the risk assessment. In this chapter, the procedures to construct ISMS for operational organizations of the information system is explained.

The following procedures are taken to construct ISMS.

- Organization of the security committee
- Identification of the assets
- Identification and evaluation of the threats
- Identification and evaluation of the vulnerability
- The evaluation of the risks
- Design and implement of the security measures
- Examination and enforcement of system change management
- Continuous monitoring and revision

SEE ALSO ISMS became an international standard as ISO/IEC 27001. For more details, refer to the Web site below:

https://www.iso.org/isoiec-27001-information-security.html

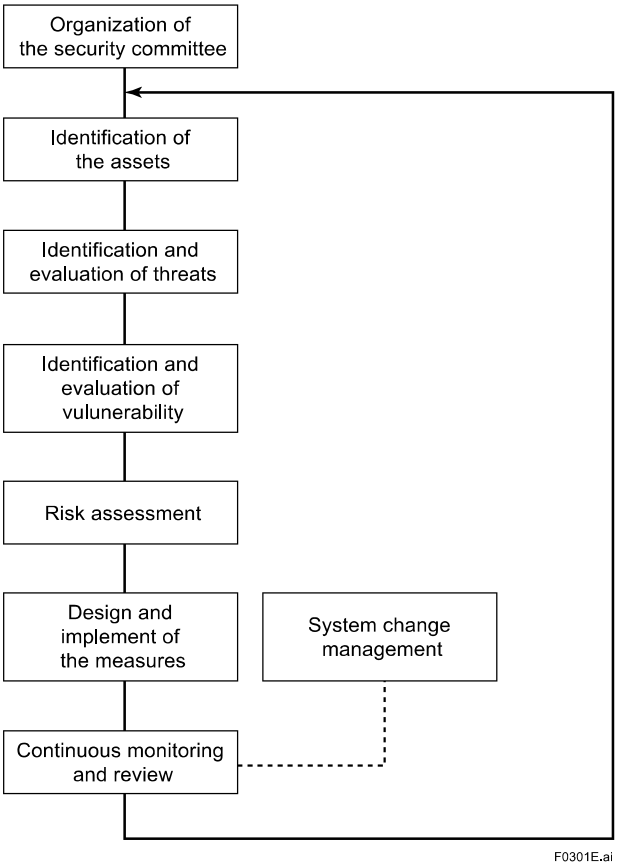


Figure Procedures to construct ISMS

Organization of the Security Committee

The security committee is the leading organization of the activities of ISMS. Please take notice of the following when it is organized.

Commitment of management

The objective of the security committee is to protect the assets of enterprises. That means that the management is responsible for this. In addition, it is necessary to get the collaboration of everybody involved in the production activities in order to enforce efficiently the security measures. Therefore, the management should express their opinions about the security activities clearly.

The management should commit itself to the security committee and take the initiative.

The cross-functional organization

The security committee consists of the representatives of all the divisions involved in the production activities. For example, we can assume an organization with the following divisions.

- Production division
- Production control system management division
- IT system management division
- Business management division
- Maintenance division

Identification and Evaluation of the Assets

The purpose of this phase is to list all the assets to be protected, identify the asset owners and evaluate the value of each asset. The assets with larger value have the higher criticality. In chapter 2, an example of assets to be protected is described.

Followings are the examples how the criticality of the assets are classified.

- Criticality A : Very High
- Criticality B : High
- Criticality C : Low
- Criticality D : Very Low

Identification and Evaluation of the Threats

Here, we need to make clear the potential threats to the assets listed above.

In identifying the list of threats, it is necessary to think from the following points of view.

Illegal access to the assets by the people with malicious intent, the people are:

- Those inside the enterprise
- Those outside the enterprise
- Those hacking around by way of networks
- Those having chance to physically access the assets (Who can perform direct operation and enter the area where the assets are placed.)

- **Illegal access to the assets by the software with malicious intent**
  - By way of networks
  - By way of removable media

- **Incidental illegal access to the assets caused by mistaken or careless operations**

  The level of possible occurrence of the identified threats will be evaluated.

  The example of the classification of this will go as follows.
  - Level A: The possibility of its occurrence is high.
  - Level B: The possibility of its occurrence is moderate.
  - Level C: The possibility of its occurrence is low.

Identification and Evaluation of Vulnerability

The purpose of this phase is to identify the vulnerability of each asset, also to identify the vulnerability of each equipment of the asset. The term “vulnerability” means the situation or condition that threats can affect the assets.

The followings are examples of the vulnerability.

- Incompleteness of the security measures or their implementations
- Incompleteness of the enforcement procedure or the procedure documentation
- Incompleteness of the security committee organization
- The lack of physical protection
- Incompleteness of Firewall settings placed on the border of the network to be protected against the external networks
- Inadequate virus definition files or engine of antivirus software (Non-updated Virus definition file or engine)
- Incompleteness of the Security Updates (Non-updated Security Updates)
- Incompleteness of backups (The system is not backed up.)
- The lack of understanding to PCS (process control system) and it’s operational environment
- The lack of the awareness of security among the people such as operators

Risk Assessment

In this phase, the risk of each asset or each instrument housing the assets is evaluated.

The risk is shown as below:

Risk = Threat x Vulnerability x Consequences

By doing risk-assessment, you can clarify the priority of the security measures. In risk assessment, the consequences are estimated such as loss of business by the stop of system function, and the expense for restoring from the damage of the production control system. By the degree of these quantitative consequences, the priority of each measure needs to be determined. Then, you can clarify which part should need concrete measures, considering which measures have to be taken over which risk, or which risk is tolerable.

However, consequences may include the damages to environment and human being, and the damages to public confidence to the enterprise. Therefore sometimes it is difficult to estimate the consequences as uniform operation loss of money.

Design and Implement of the Measures

In planning the security measures for production control system, it is necessary to make the security policy that regulates the rule of the security management. The actual security measures should be designed or selected along this rule.

Security policy

The security policy is made to regulate how the security of production control system can be managed. The followings are the examples of security controls that should be included in the security policy.

- User ID management
- Password management
- Connection to business network
- Remote access
- Computer virus
- Media management
- Physical protection
- Education, training

Notes about the measures

There are many cases where the technique or customs developed in IT systems are applied to the security measures for the production control systems. However, production control systems have different characteristics from those of IT systems, so it is necessary to take them into consideration in making the measures. We will show the differences between IT systems and production control systems as follows.

Availability

High level availability is required for production control systems. In IT systems, some operations are made on the assumption of reboot, but in case of production control systems, uninterrupted operation is most common.

Real-time ability

Real-time ability is important for production control system. For instance, it is necessary to respond quickly to the operations from HMI and so on. It is also required to make a stable throughput as well as a real time response to the data-collections and setting requirements from the upper level systems.

Consideration of Security Updates and anti-malware software

Since the high level availability and real-time ability are required for production control system, it is necessary to check the Security Updates and anti-malware software updated beforehand and consider the application, the means and timing of update for them to a large extent.

● Priority of Availability, Integrity and Confidentiality

When considering the security objects in the Production Control System, the availability of system, network, endpoint equipments such as controller and PC should have the first priority. Another important security object is integrity of data used by Production Control System. If there is loss of integrity, the reliability of production control is reduced. Finally it is possible to cause a safety problem. Also, production management may not function correctly by the loss of correct data, and the excessive cost concerning the opportunity loss and restoration may occur. Moreover, availability of system and network may be affected by loss of the data integrity. Therefore, it is very difficult to determine the priority between availability and integrity.

On the other hand, when considering the confidentiality of data and information of Production Control System, the confidentiality generally has lower priority than other two security objects. However, consideration on confidentiality may be important. User ID and the password of the production control system can flow on the network; and if they are sniffed, an attacker can attack the system as an authorized user.

■ System Change Management

It is a very important element to decide the procedures of System change management in order to keep the system secure. Whatever addition or change may be made, it has to be done in such a way as to maintain the availability, real-time ability and the degree of security. For this purpose, when some additions or changes are made, it is necessary to decide the procedure of System change management, such as going back to the first step and repeating the whole procedure from the identification of the assets to risk assessment, and to carry it out.

Apart from the addition, deletion and replacement of hardware and software, the followings are regarded as system changes, but not limited to.

Changes in settings of network devices

Changes in the settings of network devices such as in switches, routers or firewalls.

Security Updates

Before the applying the Security Updates, it is necessary to make sufficient tests.

Operation

After the construction of ISMS and the application of the security measures to the system, the system begins to operate. In this section, we will explain the activities to carry out in the phase of operation.

Organization of the team for the incident

In the operation phase, it is necessary to organize the team that will play the major role in handling the incidents.

This team takes the responsibility for the followings.

- Evaluation of the consequences caused by the security incident and the influence upon the production activities. These consequences include the damages upon health, safety, environment and public confidence.
- Inquiry into the cause and the planning and enforcement of the measures to prevent such an incident from happening again.
- Restoration of production control system from the incident.
- Gathering information on the latest threats and incidents

The procedures to take care of the incidents must be planned as a business continuity plan. This topic is explained in the chapter 6.

Daily monitoring of the system

Daily monitoring is done so as to detect the illegal access to the system in operation. The log information on the following instruments will be monitored, but not limited to.

- Monitoring log of the PC component
- Access control log of firewall
- Monitoring log of network monitoring device
- Detecting event of IPS (*1) if IPS is installed.

*1: Intrusion Prevention/Protection System:
This is a system to detect hackers to our network and/or server and to protect our system by blocking unauthorized connection, notifying a system manager and outputting logs in real time.

We will describe the monitoring of the systems in detail in Chapter 4.6.

Regular auditing

The system in operation is regularly audited to check if the settings are appropriately defined and managed. The information on the settings of the following instruments will be audited, but not limited to.

- Network devices: Information on routing control devices such as routers or switches.
- Security devices: Access control rules of firewall, detecting rules of IPS.
- System hardening of PC components: Setting information of personal firewall of PC components and the like.
- Software in use: Installations of application software to PCs are controlled, and all software is configured appropriately.

3.2 CSMS

CSMS Overview

Regarding the management and operation of information systems, application of information security management (ISMS) by ISO/IEC 27001 is common. However, regarding IACS, a mechanism of security management that takes into consideration its characteristics and properties is required. Therefore, security management for IACS based on ISMS was formulated and standardized as ISO/IEC 62443-2-1.

In Japan, as the CSMS (Cyber Security Management System for IACS), the world first certification system was built.

In ISMS, the outflow of information to be protected is a problem, and Confidentiality, Integrity, Availability are often emphasized in the order of “CIA”. But CSMS cited interruptions in operation as the most avoidable situation, focusing on the order of “AIC” and characterized by considering HSE (Health, Safety & Environment).

SEE ALSO For CSMS, please refer to the following web page.

https://isms.jp/csms/doc/JIP-CSMS120E-10.pdf

CSMS Program

CSMS is introduced and operated in the following procedure.

- Initiate CSMS program
- High-level risk assessment
- Detailed risk assessment
- Establish security policy, organization and awareness
- Select and implement countermeasures
- Maintain the CSMS

Target Organization of CSMS

CSMS certification means that the target organization establishes a security management system for the construction and operation of IACS and objectively evaluates the suitability and effectiveness by a third party.

The following companies are subject to CSMS.

- Organization that own control systems (asset owners)
- Organization that handle the operation and maintenance of control systems
- Organization that develop control systems (system integrators)

3.3 NIST

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) published “Framework for Improving Critical Infrastructure Cybersecurity” in February 2014. It is mainly written for enterprises engaged in important infrastructure, but it can be fully utilized by other organizations. It is also called “CSF” and its use is expanding abroad.

This framework classifies cyber security measures into five functions, “Identify”, “Protect”, “Detect”, “Respond”, “Recover”, and shows these functions in 23 categories.

Table NIST Cybersecurity Framework

Functions		Categories		Subcategories	Informative References
ID (Blue)	Identify	ID.AM	Asset Management	. . . .	. . . .
		ID.BE	Business Environment		
		ID.GV	Governance		
		ID.RA	Risk Assessment		
		ID.RM	Risk Management Strategy		
		ID.SC	Supply Chain Risk Management		
PR (Purple)	Protect	PR.AC	Identity Management and Access Control	. . . .	. . . .
		PR.AT	Awareness and Training		
		PR.DS	Data Security		
		PR.IP	Information Protection Processes and Procedures		
		PR.MA	Maintenance		
		PR.PT	Protective Technology		
DE (Yellow)	Detect	DE.AE	Anomalies and Events	. . .	. . .
		DE.CM	Security Continuous Monitoring		
		DE.DP	Detection Processes		
RS (Red)	Respond	RS.RP	Response Planning	. . . . .	. . . . .
		RS.CO	Communications		
		RS.AN	Analysis		
		RS.MI	Mitigation		
		RS.IM	Improvements		
RC (Green)	Recover	RC.RP	Recovery Planning	. . .	. . .
		RC.IM	Improvements		
		RC.CO	Communications		

Each category is further divided into several sub categories, and 108 sub categories in total. Measures are not very detailed and it have not mentioned any technical means.

In the informative references, links to other standards etc. related to each sub category are shown.

SEE ALSO For more information about NIST Cybersecurity Framework, please refer to the following Web page.

https://www.nist.gov/cyberframework

3.4 ISASecure

ISASecure is a security certification system developed by ISCI (ISA Security Compliance Institute), a lower-level organization of the United States-based industry association ISA (International Society of Automation). ISASecure is integrated into IEC 624434.

ISCI prepares certification programs for each subject to be certified. EDSA (Embedded Device Security Assurance) certification for control devices, SSA (System Security Assurance) certification for control systems, and SDLA (Security Development Lifecycle Assurance) certification for development process.

SEE ALSO For information about ISASecure's authentication, please refer to the following Web page.

http://www.isasecure.org/en-US/Certification

Embedded Device Security Assurance (EDSA) Certification

EDSA focuses on the security of embedded devices of control systems. There are three levels of certification level, and the level becomes higher in order of level 1 → 2 → 3.

EDSA has the following three tests.

- Functional Security Assessment (FSA)
- Software Development Security Assessment (SDSA)
- Communication Robustness Testing (CRT)

Yokogawa CENTUM VP and ProSafe-RS controllers have obtained EDSA certification.

http://www.yokogawa.com/pr/news/2014/pr-news-2014-20-en.htm

http://www.yokogawa.com/pr/news/2014/pr-news-2014-02-en.htm

https://www.isasecure.org/en-US/End-Users/ISASecure-Certified-Components

System Security Assurance (SSA) Certification

SSA is an authentication program for a specific subset of the control system developed by ISCI.

- Security Development Artifacts for systems (SDA-S)
- Functional Security Assessment for systems (FSA-S)
- Functional Security Assessment for embedded devices (FSA-E)
- System robustness testing (SRT)

Security Development Lifecycle Assurance (SDLA) Certification

SDLA is a program to evaluate the secure product development life cycle for suppliers of industrial control systems. Depending on the level of development life cycle, it is certified with four levels (ISASecure SLDA levels 1 to 4).

3.5 ISA99

ISA99 Overview

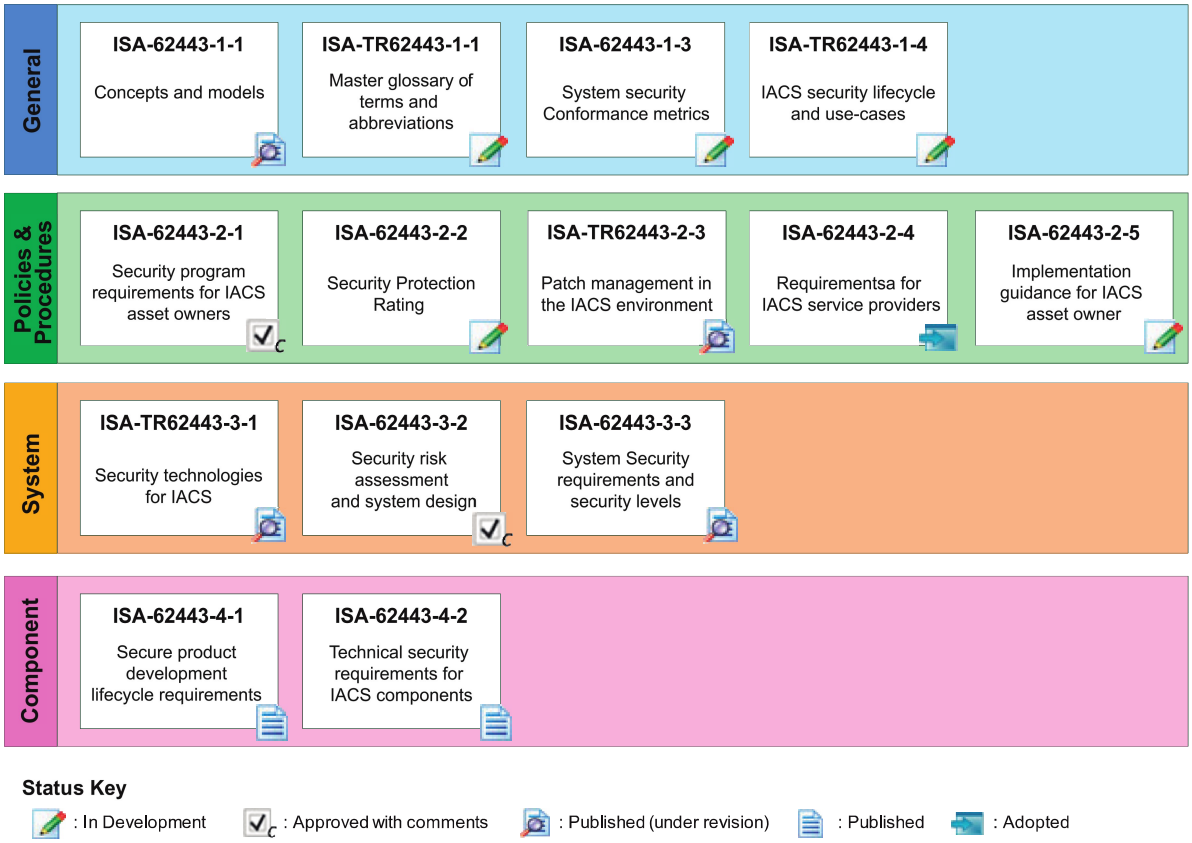
ISA99 is a security standard for Industrial Automation and Control Systems (IACS) formulated by ISA described in section 3.4. Recognizing that comprehensive security measures are necessary for IACS has been in the 1990s. However, depending on the end user and system / equipment provider, and the country and regional differences, the essential requirements were different.

Therefore, it was difficult to formulate internationally unified standards. Meanwhile, the US led the way to establish security standards as ISA. That is ISA99.

The ISA99 was eventually to be incorporated into IEC (International Electrotechnical Commission) 62443 as an international standard. Then, the ISA side changed the number from ISA-99 to ISA-62443 in accordance with the number of the IEC.

ISA-62443

As mentioned above, now ISA99 changed ANSI/ISA-62443 has been developed together with IEC 62443. ISA-62443 is not yet complete as it is trying to encompass various security measures. The figure below shows the outline of ISA-62443 as of 2019.



F030501E.ai

Figure ISA-62443 Overview

SEE ALSO For more information about ISA 99 (ISA/IEC 62443), refer to the following Web page.

https://www.isa.org/isa99/

3.6 IEC 62443

IEC 62443 Overview

As mentioned in Section 3.5, IEC 62443 is a standard created based on ISA99. Although the contents are almost the same, the requirement of WIB which was not found in ISA99 was imported as IEC 62443-2-4. In addition, it is being rewritten from the following point of view as being an international standard.

- Terms and language usage are being revised to make it easier for people who are not English native speakers.
- Consideration is given to operations in organizations with different situations in various countries and regions, and expressions are widely generalized.

Table IEC 62443 Overview

Category	IEC No.	Edition	Type	Title	Publication date
General	62443-1-1	1.0	Technical Specification	Terminology, concepts and models	2009-07-30
Policies and Procedures	62443-2-1	1.0	International Standard	Establishing an industrial automation and control system security program	2010-11-10
		2.0	(in preparation)	Security program requirements for IACS asset owners	–
	62443-2-2	1.0	(in preparation)	IACS protection levels	–
	62443-2-3	1.0	Technical Report	Patch management in the IACS environment	2015-06-30
	62443-2-4	1.1	International Standard	Security program requirements for IACS service providers	2017-08-24
System	62443-3-1	1.0	Technical Report	Security technologies for industrial automation and control systems	2009-07-30
	62443-3-2	1.0	(in preparation)	Security risk assessment and system design	–
	62443-3-3	1.0	International Standard	System security requirements and security levels	2013-08-07
Component	62443-4-1	1.0	International Standard	Secure product development lifecycle requirements	2018-01-15
	62443-4-2	1.0	International Standard	Technical security requirements for IACS components	2019-02-27

As of 2019, IEC 62443 has not been completed yet. Items in various states, such as those under formulation, those under voting, or those under revision.

For this reason, it is important for organizations involved in IACS to constantly observe their trends and take actions in line with the times.

Related Standards and Certifications

WIB Certification

WIB is an international organization of end users in the process industry, mainly in the Netherlands and Belgium. This WIB summarizes the security requirements for the supplier of the control system and it is subject to certification as "Achilles Practices Certified Solutions" by WurldTech Inc. of Canada (now under of GE digital). This is what we call WIB certification.

Yokogawa's CENTUM VP and ProSafe-RS have obtained this WIB certification.

https://www.ge.com/digital/applications/achilles-practices-certified-solutions

WIB certification is incorporated into IEC 62443-2-4.

Achilles Certification

In the world of IACS, "Achilles certification" usually means "Achilles Communications Certified Products". This is the CRT for ISASecure EDSA authentication described in Section 3.4.

Yokogawa's CENTUM VP and ProSafe-RS and STARDOM controllers have acquired this Achilles certification.

https://www.ge.com/digital/applications/achilles-communications-certified-products

4. Security Control

This chapter explains how the security controls protect the production related assets from the threats. The security countermeasures for production control system should be examined, designed, operated and evaluated while the process safety and physical defense are simultaneously taken into consideration.

4.1 Basic Strategy

It is necessary to consider the basic strategy we will describe in this chapter when carrying out the actual security control.

Risk Definition

Risk is defined by a formula as follows.

Risk = Threat x Vulnerability x Consequences

Threat is a potential attack over the system vulnerability. And risk means the potential damage or loss that is caused by the attacks over the vulnerability. Therefore, the measures to reduce risks can be categorized as follows.

- Removal of vulnerability
- Restriction of use
- Control of attack
- Mitigation of consequences

Each security control explained in this chapter corresponds to these measures.

Security Zone

ISA99.00.01 defines security zone as a logical or physical group which share common security requirements and the same security level. By making the multiple zones where each zone satisfies different security requirements, defense-in-depth strategy can be realized. The security controls are explained in this chapter, and these security controls should be designed based on the concept of zone.

Defense-in-depth strategy

Threats to information system are under daily evolution. What is more, the threats can happen not only in the external networks like business networks, but also on PCN (Process Control Network), which is an internal network. We have to get armed with the defense-in-depth strategy.

As shown in the figure, by defense-in-depth strategy, we mean the protection measures composed of more than one security control to protect the assets. By the use of this kind of multi-layer measures, another layer will protect the assets even if one layer is destroyed, so the assets are protected more firmly.

Network boundary security

It is a contact point between control network and an external network such as a business network, and it prevents the external threats from entering control networks.

vInternal network security

It tries to decrease the consequences of the threats occurring on the control network as much as possible. For instance, it divides the control network into multiple zones, and constructs the network in order not to allow the damages in one zone to affect other zones.

End point security

It is a measure for excluding the vulnerability of end point and increasing the strength of the security. For example, it applies Security Updates to PC, and excludes the security hole.

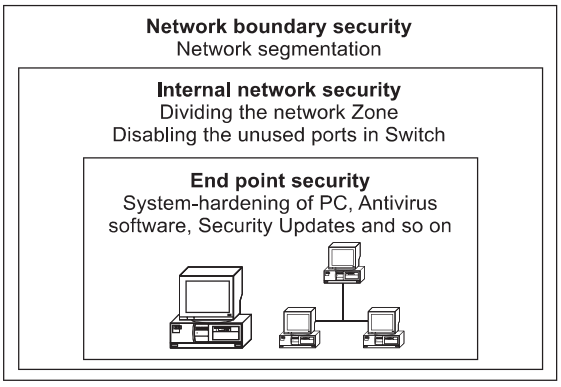


Figure Defense-in-depth strategy

Deny-all strategy

Deny-all strategy is a strategy that allows only the minimum accesses and prohibits the others. Security control with deny-all strategy makes it possible to protect the assets firmly, for it does not permit more accesses to the assets than necessary and it limits the space for illegal accesses to the least. It is necessary to take it into consideration, especially when enforcing the access control rule of firewall or system hardening of PC components.

4.2 Network Architecture

A secure network configuration is explained for connecting a Production Control System (PCS) with an external network such as a business network.

4.2.1 Network Segmentation

Segmentation of networks is the basis of security control. There are two types of segmentation, vertical and horizontal.

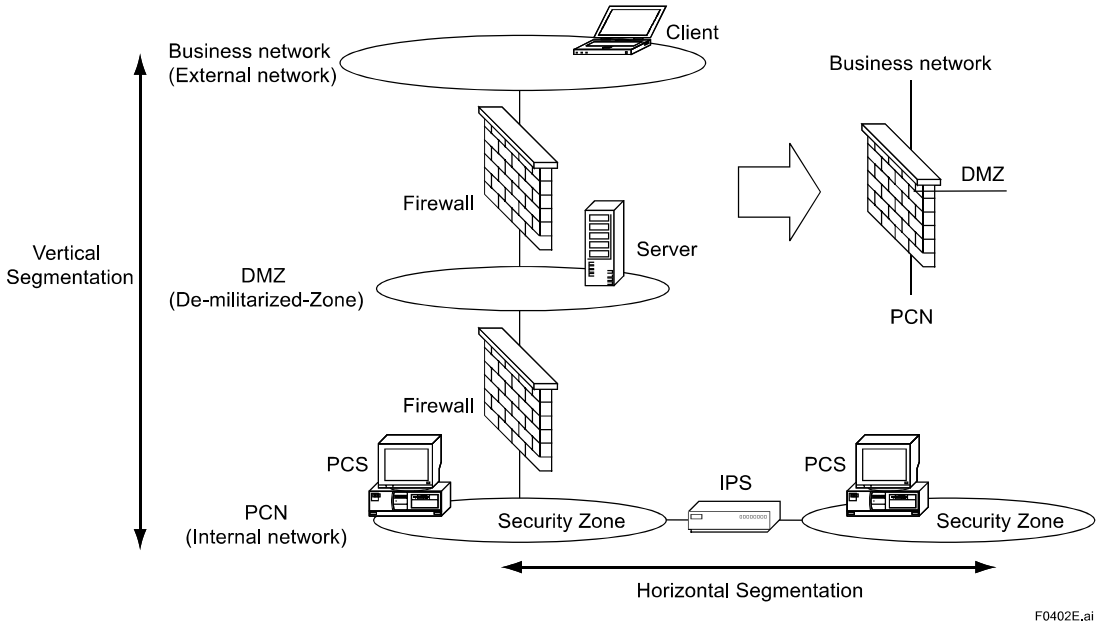


Figure Network segmentation

TIP

In terms of logic, the configuration of DMZ is supposed to be a network protected by two firewalls, as shown in the figure. However, it is usually only a single firewall with three or more network ports.

Vertical segmentation

In the vertical segmentation, the network is divided into the following three segments. Among the segments, the passage of network traffic is controlled and the threats from external networks are excluded. The access from business network is possible only to the servers on DMZ, and it is not possible to access PCN directly. In addition, it can conceal the PCS addresses from client on business network. That is, the vertical segmentation is for protecting the PCN from external networks such as business networks.

Business network

This is an external network on which the clients that may access the data of production control system are connected. This segment belongs to Level 4 of ISA 99.00.01 Reference Model.

DMZ (De-Militarized Zone)

The servers that directly communicate with the clients are placed in this zone. The servers placed here communicate with both PCS and the clients. DMZ is a buffering area placed between PCN and business network. The servers on DMZ need to be firmly fortified with the antivirus software and Security Updates, for the servers may be directly accessed from the external networks. This segment is located between Level 4 and Level 3 of ISA 99.00.01 Reference Model.

PCN (Process Control Network)

PCN is an external network that the production control system is connected. The devices placed here can not be accessed directly from business networks. The data of PCS are passed to the business networks through the servers on DMZ, so it is not necessary to access PCN directly from the business networks. This segment belongs to Level 3 of ISA 99.00.01 Reference Model.

Horizontal segmentation

The internal network is divided into multiple security zones. For example, IPS (Intrusion Prevention/Protection System) is connected in between the 2 security zones, and filters out the illegal traffics that run between the security zones. By dividing PCN into security zones, it is possible to prevent other security zones from the threats of worms that occurred in one security zone.

SEE ALSO For notices about constructing IPS, refer to “4.6.2 IDS/ IPS”.

4.2.2 Classification of Devices Composing the System

The devices are placed in different segments according to the following classification.

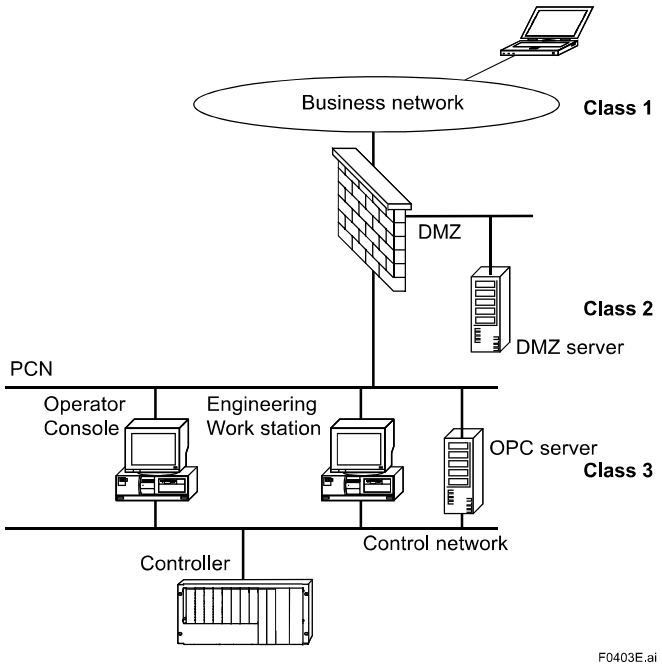


Figure Equipment class

- **Class 1: Computers connected on business network (external network)**

  The computers in this class are connected on a business network and access the data on the PCS via a server in the DMZ. This computer is usually managed by the information system department in an enterprise.

- **Class 2: DMZ server**

  The servers in this class are used for publishing the data of PCS to the computers of Class 1. It communicates with both the clients on the business network and the PCS connected on PCN. That is, the server obtains the data by accessing PCS and publishes the data to the devices of Class 1. The servers used for publishing the virus definition files or Security Updates are also classified in this class.

- **Class 3: PCS (Production Control System)**

  The devices of this class do not communicate directly with computers on the business network. The PCS devices belong to this class. They are not directly accessed from the business network.

Classification is based on the consequences of a security incident. The devices that are closer to the process have the higher priority, because the consequences are more serious. In this classification, Class 3 has the highest priority.

4.2.3 Access Control by Firewall

A firewall can restrict the communications of the three network segments to a minimum level. Moreover, applying a deny-all strategy can block all communication traffics except those permitted. (*1)

*1: It is called “Cleanup” and is specified at the end of Access Control Rule.

Port (service), IP address control

With a firewall, external accesses to the servers on the open segments, and the accesses to the control devices on the internal segments (control system segment) from the servers on the open segments are restricted to a minimum level so that only the permitted accesses are allowed.

More over, a firewall generally hides itself from the outside so that the accesses to firewall are prohibited. (*1) Therefore, the access control rule should be configured comprehensively by permitting only the necessary accesses from/to the specific sources/destinations and the accesses through the designated communication ports (or identified by the specific service names).

*1: It is called “Stealth”, for it conceals the firewall. As an exception, only the communications from the administrator console that manages the firewall need to be permitted.

DoS (*1) defense

The features of firewalls vary with firewall types. Some types of firewalls are able to defend against the DoS attacks by temporarily restricting the number of TCP connections. Applying this feature would protect the DMZ servers from the DoS attacks that would make them overloaded.

*1: Denial of Service attack: It is a kind of attacks by sending a large amount (meaningless) of service connection requirements to servers such as Web servers, FTP servers, Mail servers and so on, to make the servers overloaded and block the services to the legal users.
It is expanded to Distributed Denial of Service (DDoS) that attacks all at once from multiple places by using third party computers as a stepping-stone.

IP Spoofing (*1) defense

Restricting the network addresses from all the segments can defend against IP spoofing attacks. It can also repel the illegal packet sent from an outsider but disguised as if it were from an internal network address.

Therefore, the addresses permitted for each segment should be defined to the firewall so that only the packets with the permitted addresses can enter the segment.

*1: IP Spoofing: It means creating and sending packets with false IP addresses of the senders in order to conceal the origin of attackers. When the server receives a packet from the outsider but the packet is disguised with an internal network address, the server may assume the packet is from an address of an internal sender and relay the packet in the internal network. Because the sender is not insider, the server may fail when tries to respond. Many DoS attacks are taking advantage of this mechanism.

4.2.4 Dual-Home Server

It is not recommended that the dual-home servers (*1) for both Ethernet and Control bus be placed in DMZ. As an alternative, the dual-home server can be placed on PCN and place a reverse proxy server (*2) in DMZ.

The reverse proxy server will take the requirements from the business networks and then, pass them to the dual-home server on PCN.

*1: Dual-Home Server: a server with two or more network interfaces.
*2: Reverse Proxy Server: a proxy server to relay demands for a particular server. Every access to this particular server goes through this proxy server.
Regular proxy relays access from internal network to external network. Reverse proxy, on the other hand, relays access from external network to internal network.

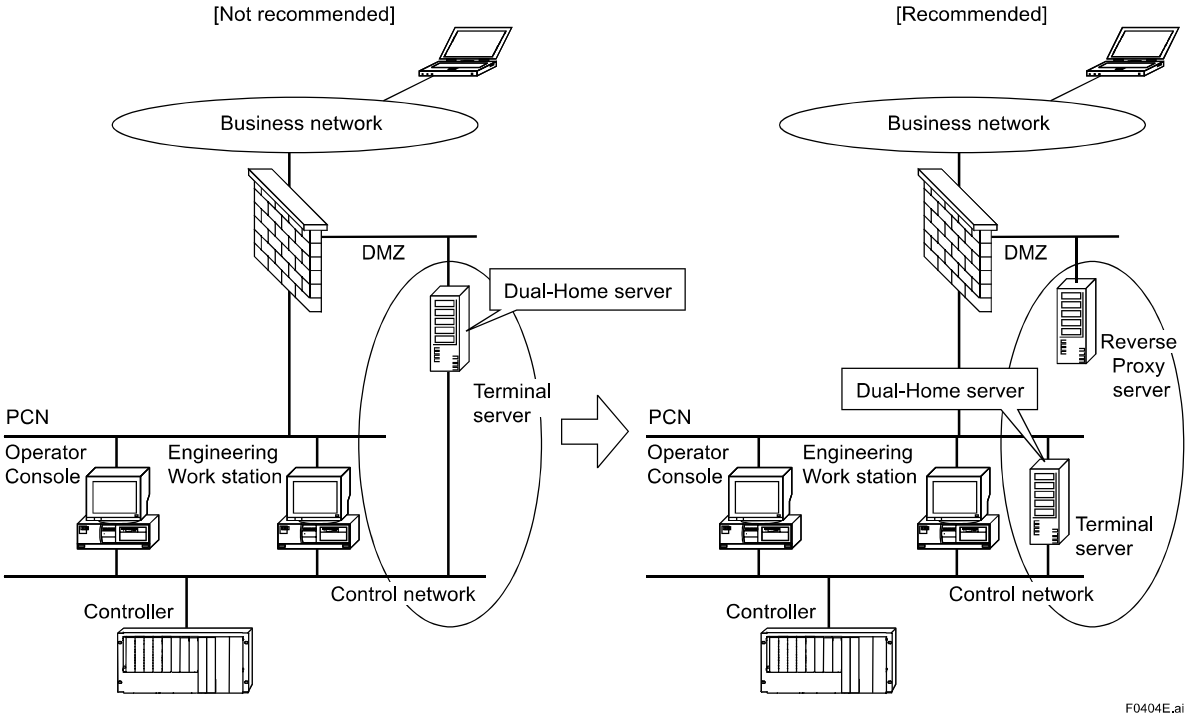


Figure Dual-Home Server

In the recommended example in the right-hand side, the terminal server is placed as a dual-home server. The applications, such as the operator console applications, are running in the terminal server. Via reverse proxy server in DMZ, it is possible for the users in the PC placed on business network to display and operate the applications running in the terminal server.

4.2.5 OPC Interface

This configuration shows that a user on a PC located on the business network can display and operate the OPC client applications by using a terminal server. The terminal server is used because the reverse proxy server can not be directly used to route to the OPC server. The terminal server is placed in PCN, and OPC client is running in the terminal server PC. OPC server is placed as a dual-home server, and it is connected to both of PCN and control network.

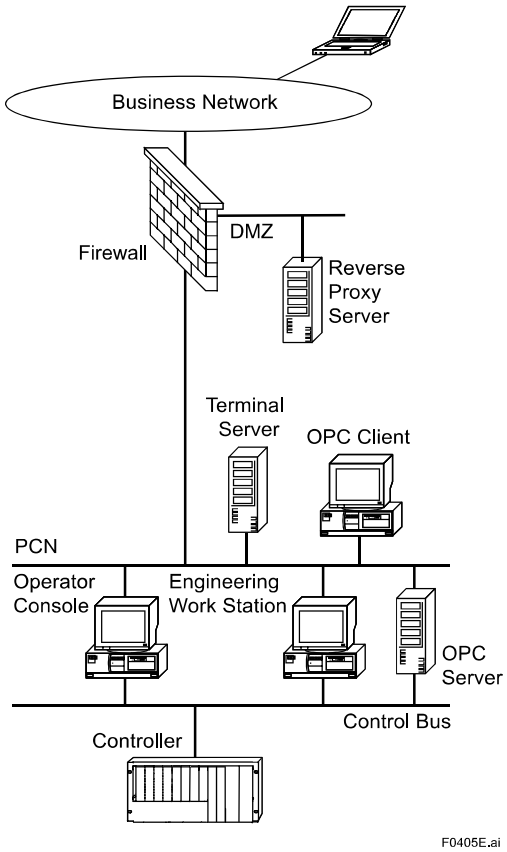


Figure Example of OPC interface configuration

By this configuration, it is possible to display and operate the OPC client applications via a Reverse Proxy Server in DMZ from the PC of business network, while the OPC client applications are running in the terminal sever of PCN.

4.2.6 Application of Wireless Networks

In this section, we will explain the security of wireless network.

Wireless LAN (IEEE 802.11)

These days, the use of wireless LAN of IEEE 802.11 series has been increasing rapidly. It became widely known to the public as “Wi-Fi” and now used in private and business environments.

In control systems, the cases have been increasing where the fieldsmen using the mobile terminals to access PCN through the wireless access points located in the company premises. The characteristics of wireless LANs increase the security risk that an outsider may use an over-the-counter wireless card for illegal access from the locations wherever the wireless transmission reaches. Moreover, outsiders may sniff the communication, tamper with the data,or hack the system by using tools such as the War driving (*1) tool.

Therefore, when wireless LANs are connected with PCN, it is necessary to take care of the following points.

*1: War driving: It is a means of cracking technique to seek for the access points of wireless LAN, moving by car in the streets lined with office buildings.

Connection of access points

Do not connect access points with PCN directly, but connect it with DMZ, and control accesses to PCN with firewall.

Authentication of terminals

It is necessary to register MAC addresses of terminals which are allowed to be connected so that to prevent the illegal terminals from getting connected. If an unauthenticated terminal is connected, the network will be threatened by the illegal usage. Moreover, it is nearly impossible to detect illegal wireless access such as wireless sniffing.

The setting of ESSID (*1)

Set the ESSID of access points and prohibit “Any connections”.

*1: ESSID: The network identifier of wireless LAN of Extended Service Set Identifier IEEE 802.11 series. It can prevent any terminals other than those with the same identifier as ESSID from accessing the access points. When “Any access” is permitted, the terminals with any ID can be connected.

Encryption

It is necessary to encrypt communication data by using WPA (*1).

*1: WPA is an encryption standard developed by the Wi-Fi Alliance to protect wireless LANs. It overcomes the weaknesses of the WEP encryption that was used and strengthens network security.
Moreover, WPA2 which is improved from WPA adopts Advanced Encryption Standard (AES), so weak points of WEP and WPA are all relieved. However, vulnerabilities of WPA2 were publicly disclosed on October, 2017. Thus, updating for the revised program is required when using WPA2.
Incidentally, WPA3 that solved the vulnerabilities of WPA2 fundamentally will be released to the public in the latter half of 2018.

The system-hardening of access points

It is highly recommended to harden the access points with the following preventions so that they can be concealed from the scanning of access points such as War-driving.

- Disable the broadcast of ESSID (Beacon signal).
- Disable the response to a probe request.

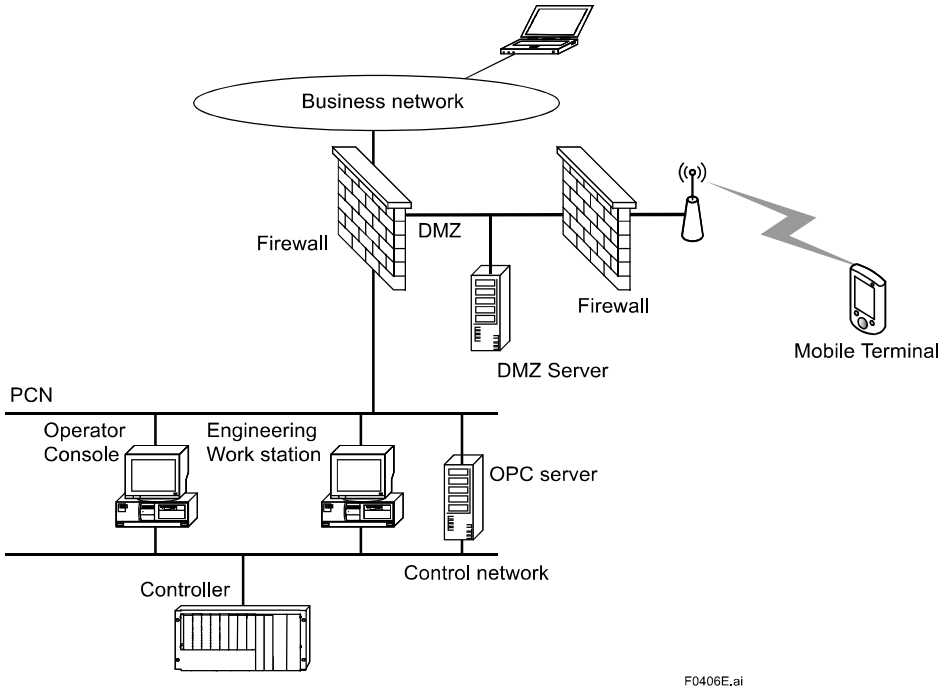


Figure Example of Wireless Network Configuration

Wireless application to control bus

When you extend the control channel of Vnet/IP or HSE (High Speed Ethernet) of STARDOM with a wireless network, you need to pay attention to the following points.

- The available band width will be restricted. (11Mbps - 54Mbps)
- The state of electric wave easily gets deteriorated because of the obstruction of electric wave and rainfall
- When the state of electric wave gets deteriorated, the performance in the band width will be lower.

In addition, control the accesses with a L3 switch and apply access points so that only the communications between the two domains connected with each other can be relayed.

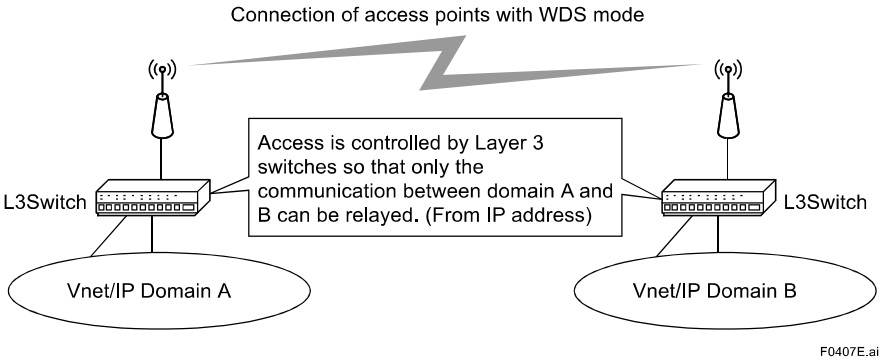


Figure Example of the configuration of the extension of Vnet/IP control channel

Field wireless (ISA 100.11a)

Field wireless networks compliant with ISA 100.11a are highly relaible in ensuring the safety of production sites and the security of information. They take care of concerns such as message confidentiality (encryption, authentication, access control), message integrity, and network availability.

You can obtain a higher level of security by implementing the following measures when building a system that handles field wireless devices.

Basic measures

- Completely separate the network for control system usage from that for field wireless usage.
- Control access by installing a switch between ISA100 gateway (*1) and computers.
- Set up firewalls for both the system and ISA100 gateway and build a VPN between them to connect to the Wide-area Universal Field Network (*2).

*1: A device that connects to the field wireless and the wired Ethernet. The Yokogawa product “YFGW710 Field Wireless Integrated Gateway” is an example of such a device.
*2: A system that uses monitoring devices such as CENTUM to monitor the process data of wireless devices by passing through the ISA100 gateway in a wide area network. It may pass through open IT networks on the way, reducing reliability and real-time performance.

Additional measures for higher security

- Separate the network for control system usage from that for field wireless usage even if they are at the same security level, and set up a firewall between the networks. (horizontal integration)
- Set up a firewall between all layers. (vertical integration)
- Install the PRM Field Communication Server on two different computers. One is for CENTUM while the other is for field wireless.
- The Field Wireless Configurator and Field Wireless Management Tool are also installed on different computers.

The following figure shows an example of a field wireless system configuration that takes security into account.

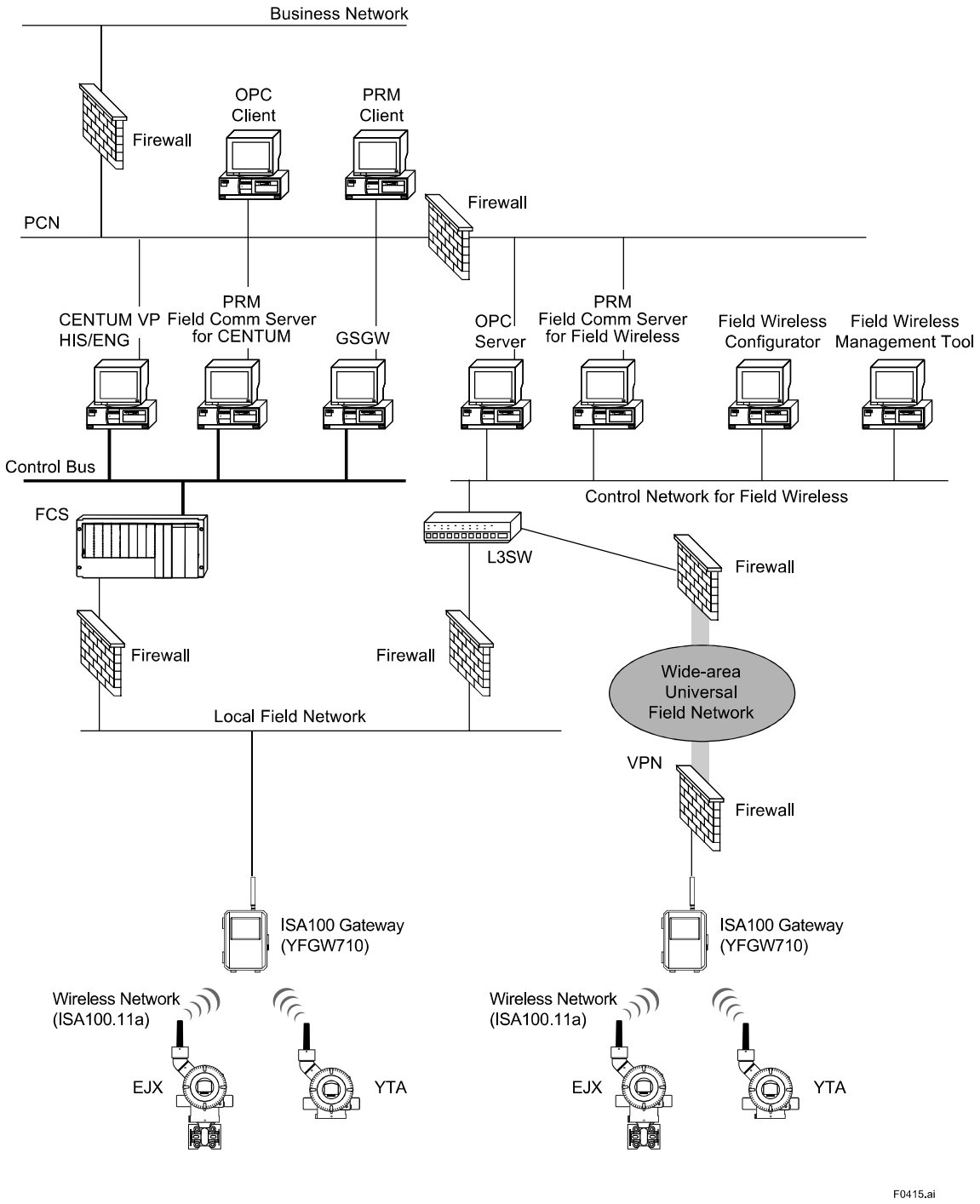


Figure An example of a field wireless system configuration with consideration for security

4.2.7 Remote Monitoring

We will explain the configuration of remote control networks for the physically remote- located clients through the terminal server.

Wide area network

The communication route for remote monitoring between the remote clients and the local firewall, the wide area network provided by the public communication services will be used.

The wide area network could be:

- Digital dedicated line
- Dial-up connection by ISDN (*1)
- Closed network (IP-VPN (*2), Wide-area Ethernet (*3) and the like)
- Internet

Although a dedicated digital line is a recommended option from the viewpoint of security and the quality of network transmission, it is not economical.

Internet is economical, since the inexpensive high speed Internet connections are available, but it has such disadvantages as unstable network quality and insufficient network security.

*1: ISDN: Integrated Services Digital Network
It is one of the telephone networks, such as analogue line network, mobile-phone network and PHS network. In using it in dial-up as a data communication line, it can be used as 64kbps or 128kbps line.

*2: IP-VPN
It signifies the Virtual Private Network constructed by way of Wide area IP communication network owned by public communication services. The use of IP-VPN makes it possible to operate remotely separated networks as if they were directly connected by LAN. The actual network consists of a large number of routers connected with one another.

*3: Wide area Ethernet
It is a wide area communication network provided by some public communication services, combining switching hubs (layer 2 switches) used in Ethernet. It is possible to construct VPN environment where only the contracted points are connected by Ethernet like IP-VPN. In case of IP-VPN the only protocols that can relay are IP protocols, but in the wide area Ethernet, it is possible to use various protocols, not just IP.

WAN that can constitute a close network is recommended.

(Digital dedicated line, IP-VPN, Wide area Ethernet and so on.)

In connection through internet, it is necessary to construct VPN tunnel between the points where Client is set and the plant.

We will cite the example of the configuration of network through IP-VPN network and Internet.

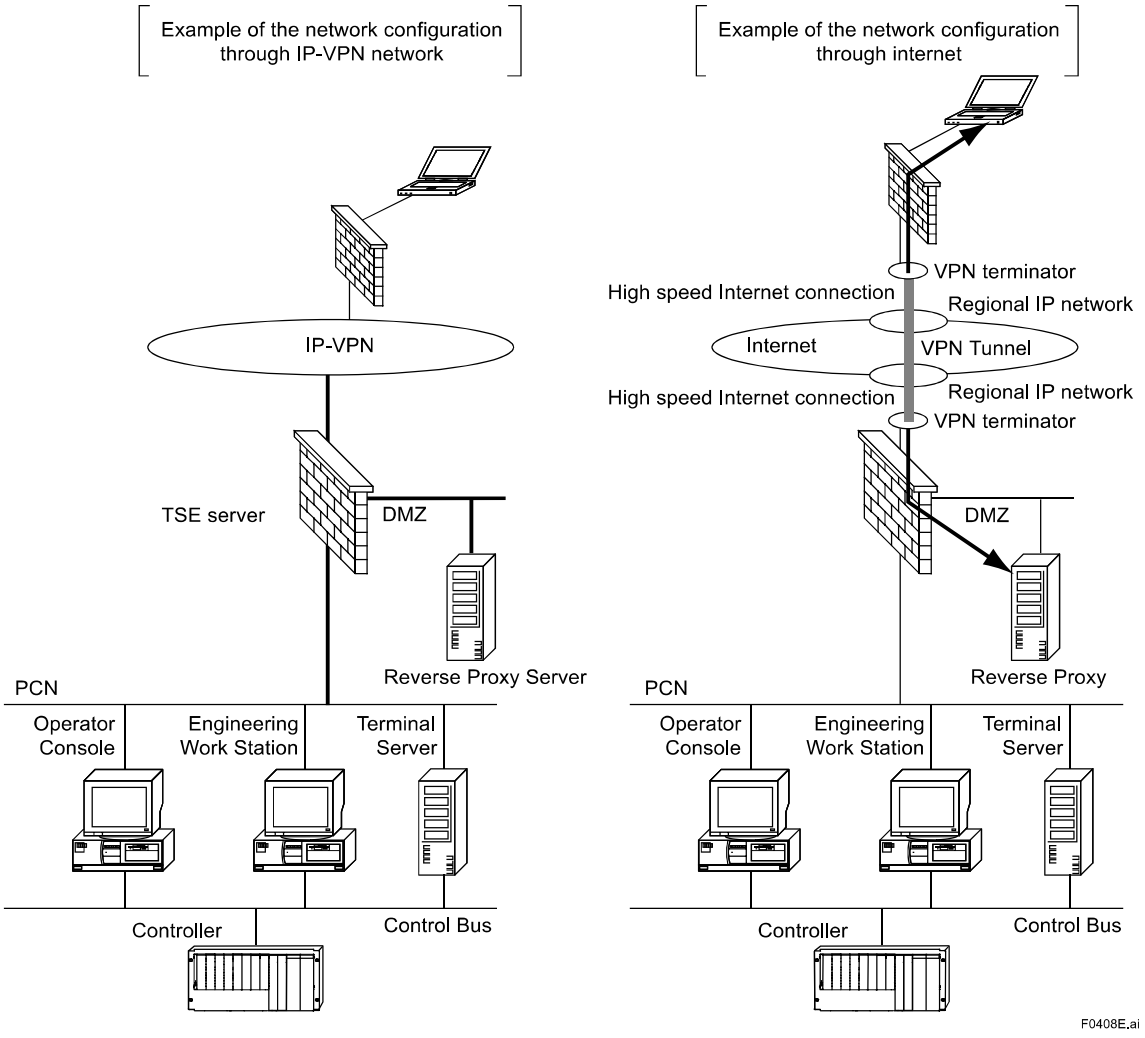


Figure Example of the configuration of remote monitoring network

Personal authentication

In remote monitoring system, sometimes, there is necessity for identifying a person to operate and monitor the plant as well as restricting his access rights to the specified devices.

In this case, a reverse proxy server that capable of authenticating the remote users for accessing the PCN should be applied. An example configuration of the system is shown below.

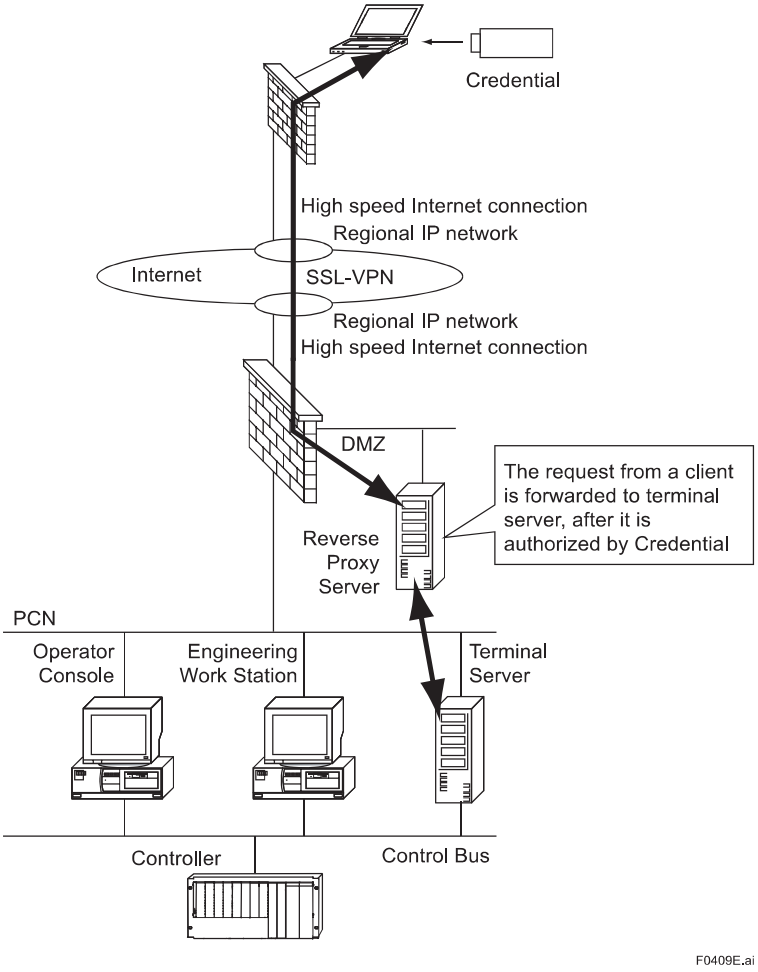


Figure Example of Personal Authentication

Before operation and monitoring, a user is authenticated between a client and the Reserve Proxy server based on individual credential. If the authentication is successful, the Reverse Proxy server will relay the request from the client to the terminal server.

The communication between the clients and the Reverse Proxy server is encrypted by SSL-VPN (*1).

*1: SSL-VPN : SSL-VPN is a technique to realize VPN, by using SSL (Secure Socket Layer), an encrypting protocol, widely used in internet. Since it is not necessary to install special software in the side of Client, unlike IPSec, it is widely used in the remote access environment of the enterprises.

4.2.8 Remote Maintenance

The remote maintenance through modem refers to the situation that a production control device or a network device vendor is using the telephone line or internet to establish the connection to access PCN for maintenances.

In a system like this, PCN can be accessed by through the telephone network or public line like internet. If there are any vulnerability in this system, it will open a backdoor (*1) to PCN, so that the PCN will be exposed to the threats of security.

*1: Backdoor: a backdoor which enables hacking.

Remote maintenance through modem

If a remote access environment or the remote access to PCN is established by using modem, the access route will bypass the protection of the firewall. Consequently, the remote access environment will not be secure, the remote access route will be the backdoor to PCN and the production control system will be exposed to the threats of security.

When constructing the environment for remote maintenance by use of modem, security should be obtained by the following measures.

- **Use of RAS (Remote Access Server)**

  Make sure that every remote access to PCN be made via RAS. A remote access protocol such as PPP (point to point protocol) that authenticates all the remote access connections between a remote PC and RAS should be used.

- **Use of callback**

  After the authentication with RAS, if it turns out to be a previously registered client, the client will get a callback.

- **Authentication by using the caller ID**

  By using a modem that have the caller ID feature with the phone number, only the calls of the previously registered phone numbers can be accepted. Also it is possible to use the caller ID feature of RAS instead of the modem's authentication feature.

- **Modem management**

  Turn off the power supply of the modem or disconnect the telephone line from the modem unless the remote maintenance is necessary.

The system-hardening of RAS

- User management

  The user IDs of minimum required users should be registered in the maintenance server. Moreover, when there is a user change, registration of the user ID should be changed accordingly.

- Password management

  The password registered in RAS should be the one impossible to guess and should be changed regularly.

- Antivirus

  Harden RAS with antivirus software and get it prepared for computer viruses. See the chapter 4.3 for more details.

- Security Updates

  Apply the latest Security Updates to RAS and exclude the security holes ever known. See the chapter 4.4 for more details.

For more descriptions about system-hardening, refer to the text on system-hardening in the chapter 4.5.

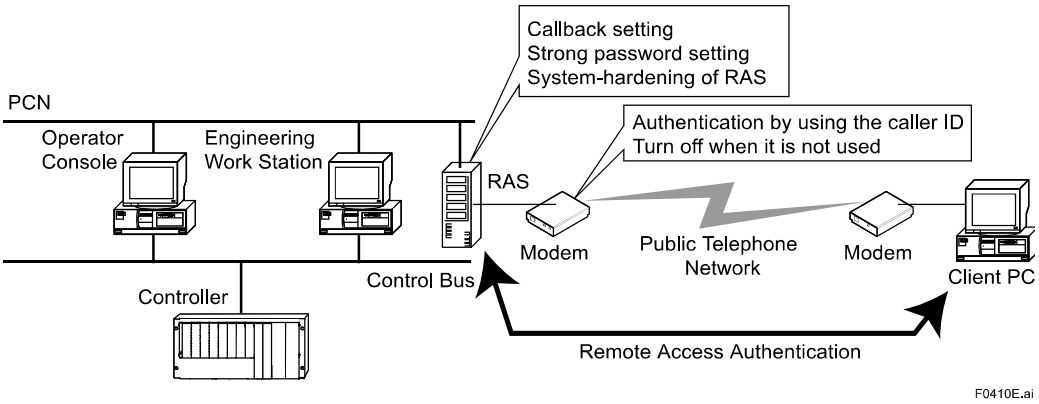


Figure Example of the configuration of remote maintenance by Modem

Remote maintenance through internet

When internet is used as a relaying line, PCN will be put in an environment where an unlimited number of people can freely access it. Therefore, it is important to enforce the security.

Security should be enforced with the following measures.

Internet VPN

For remote maintenance through internet, it is necessary to construct VPN between the two connected points.

Access control by firewall

The communication from outside should be restricted by firewall in accordance with the explanations in 4.2.3.

Maintenance server

Do not allow the remote maintenance terminals to access PCN directly but allow the access to PCN though a maintenance server set in DMZ.

The system-hardening of the maintenance server

- User management

  The user IDs of minimum required users should be registered in the maintenance server.

- Password management

  The password registered in the maintenance server should be the one impossible to guess and should be changed regularly.

- Antivirus

  Harden the maintenance server with antivirus software and make it robust against computer viruses. See the chapter 4.3 for more details.

- Security Updates

  Apply the latest Security Updates to the maintenance server and exclude the security holes ever known. See the chapter 4.4 for more details.

For more descriptions about system-hardening, refer to the text on system-hardening in the chapter 4.5.

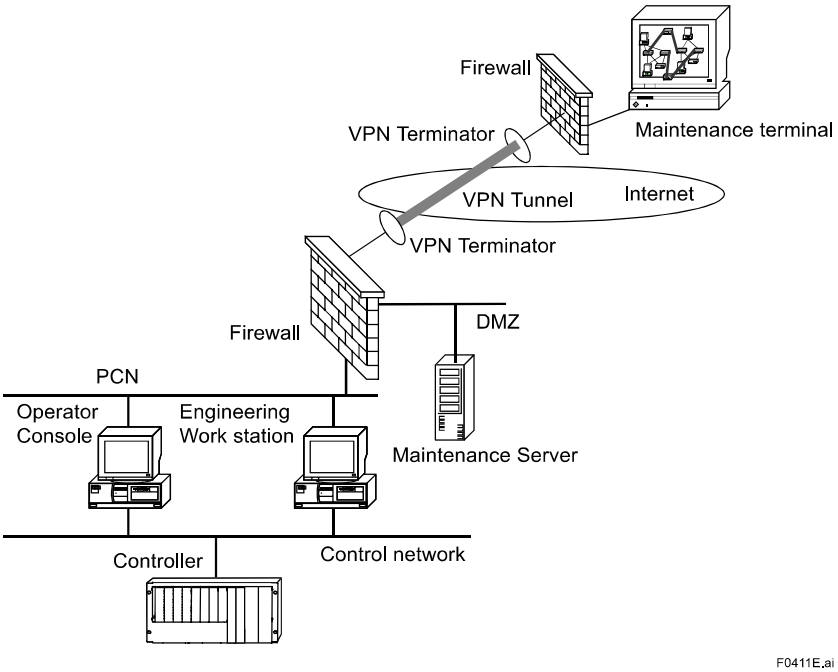


Figure Example of the configuration of remote maintenance via internet

4.3 Anti-malware Software

4.3.1 Antivirus Software

Antivirus software is effective as one of the countermeasures against malwares. Installation of antivirus software in Windows-based devices is strongly recommended, if those are components of a production control system, along with the following suggestions.

Applying antivirus software products

A production control system requires real time response and stable throughput to the operator actions via HMI and data acquisition by its supervisory systems. Due to its characteristics, antivirus software may have influence over performance of the PC.

Yokogawa has verified the performance of standard antivirus software in combination with Yokogawa's control system software.

SEE ALSO Yokogawa offers antivirus software as a fundamental solution. For more information, refer to:
Basic Endpoint Security solution (GS 43D02T30-05EN)

Environment of antivirus engine and virus definition file updates

When using antivirus software, it is most important to keep updating antivirus engine and virus definition files.

It is recommended to provide a server for updating these files in the DMZ, as accessing the external server for updating directly is vulnerable to the network configuration.

Daily management

In some cases, rebooting of a PC is required when a antivirus engine or virus definition file is updated. In other cases, the updating may bring an unexpected influence over operations of the PC. Therefore, a management procedure is required to verify if updating the antivirus engine or the virus definition file is safe before distributing them to all the PCs.

Prior confirmation

To reduce risks in conducting a prior confirmation, either one of the following measures can be taken.

- Use a system dedicated for testing. Then perform the test on the actual system.
- Conduct a test on one of the PCs in the actual system, and apply the tested updates to the rest after confirming that there is no problem.

4.3.2 Whitelisting Software

Malware inactivation

If only authorized programs are set to executable in advance, the execution of malware or unauthorized programs can be blocked. This is the malware inactivation by whitelisting method. This measure is most effective in reducing the security risk of PCs on which Microsoft Security Updates are not applicable or difficult to install. For more details, contact Yokogawa service window.

SEE ALSO Yokogawa offers antivirus software as a fundamental solution. For more information, refer to:
Standard Whitelisting Software for Endpoint Security (GS 30A15A30-01E)

4.4 Security Updates Management

Security Updates (Microsoft Security Updates) remove vulnerabilities known to Windows and protect production control system from unauthorized accesses and invasion by malwares.

Installing Security Updates

Yokogawa constantly investigates Microsoft Security Updates and conduct integration tests if those security Updates are relevant to Yokogawa products before offering. And Yokogawa let customers know the importance and priority of each security Updates.

For applying those Security Updates, it has to follow customers' security policies. Customers are to perform testing prior to applying those Security Updates considering the influences to the production control systems in advance.

Yokogawa suggests that all the applicable Security Updates must be applied to the control system as soon as possible. For installation of the Security Updates, please contact Yokogawa service department.

SEE ALSO For more information about security service, refer to:
Endpoint Security Service (GS 43D02T30-02EN)

Prior confirmation

To reduce the risk in applying Security Updates, ensure that those Security Updates works before those are applied to the PCs in the production control system.

To reduce risks, either one of the following measures can be taken in advance.

- Use a system dedicated for testing. Then perform the test on the actual system.
- Conduct a test on one of the PCs in the actual system, and apply the tested Security Updates to the rest after confirming that there is no problem.

SEE ALSO For more information about applying security Updates, refer to:
Basic Policy for Microsoft Software Updates (Including Security Patches) with Yokogawa ICSS Products (TI 33Y01B30-02E)

4.5 System-Hardening

System-hardening is explained here, to protect our system from hacking.

4.5.1 System-Hardening of PC Components

Assignment of passwords

The passwords used on the PC components are the information to prove that the user is an authorized user. If a password is leaked to an outsider, it may result in the illegal use or destruction of the data in the system. It is important to make some rules concerning the password management and to manage the passwords safely by obeying the rules.

The password policy is as follows:

- When setting a password, do not use an easily guessed password such as your name, your birth date or your telephone number.
- Change the password regularly.
- Do not tell your password to anyone but those concerned.
- Do not let anyone but those concerned take a glimpse of your password, when you are typing it.
- Do not write down your password on the paper.
- Contact the system administrator as soon as possible when you feel that your password may have leaked out.

We suggest using the following password policy in the PC components.

- The length of the password: 8 letters or more.
- The password must meet complexity requirements.

  A password must contain the characters from at least three (3) of the following types:

  English uppercase letters (A, B, ……., Z)

  English lowercase letters (a, b, ……., z)

  Westernized Arabic numerals (0, 1, ……., 9)

  Non-alphanumeric (special characters) such as punctuation symbols

Access control by personal firewall

A personal firewall helps decrease number of unauthorized accesses from external networks by restricting accesses to services on PC components.

The following personal firewall policy for PC components is recommended.

- Enable Windows firewall function
- Generate a list of services or TCP/UDP port numbers connected with outside, then register them on the firewall. If the scope (IP address and subnet) of the senders who ask for connections are already known, set the scope up.

The personal firewall settings are different by product.

SEE ALSO About Yokogawa's approach to the system-hardening of PC components, refer to "4.8 Security Function of Yokogawa System Products."

4.5.2 System-Hardening of Network Devices

Hardening network devices with defensive measures against malwares and unauthorized accesses is important. In this section, guides for system hardening for each network device are described.

Firewall

Firewall, a main device for a boundary security, is exposed to external networks and system hardening for it is of high importance. System-hardening of the firewall must be performed in the following manners:

Use a dedicated firewall

The use of a dedicated firewall is recommended for preventing the network from various troubles, rather than using a device with a firewall built with many other functions.

Administrator password

When assigning an administrator password, use one that cannot be easily guessed, by using the following rules:

English uppercase letters (A, B, ……, Z)

English lowercase letters (a, b, ……, z)

Westernized Arabic numerals (0, 1, ……, 9)

Non-alphanumeric (special characters) such as punctuation symbols

The administrator password must contain characters from at least three (3) of the above types.

Mnagement of Management Segment (*1)

Firewall needs a management console in order to set the access control rules or confirm the logs and alerts. Usually, the special tools are installed in PC or Web browsers are used. The management console can change the access control rules, so in order to prevent the illegal operations of the outsiders, it is necessary to put the management console in the environment where it is not possible to be accessed from the outside. The following measures should be taken.

- Make the independent segment for it and separate it from other segments.
- The settings in the firewall should allow only the operations from the designated management console.

*1 When the remote management service of the vender is used, these restrictions are not valid. In that case, the rules for the system requirements of the service should be followed.

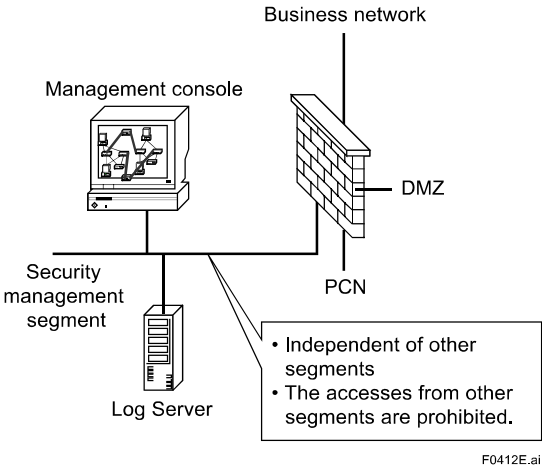


Figure Segment of security management

The restriction on network services

Only the services of minimal requirements should be allowed. Especially for the permissions on using ftp, tftp, telnet should be very careful. If they are not necessary, they should be blocked.

Management of the information on change in the setting

Set the firewall to remain the logs of all setting changes.

Software update

Update only the necessary software after confirming the release information of the vender and taking care of the security holes.

Switch

Recently, the intelligent switches are widely used. The settings of an intelligent switch can be changed through networks. Therefore, if this part is vulnerable, the devices connected to the switch will be exposed to the threats of illegal accesses. It is necessary to do the system-hardening of this part in the following way.

Disable the management via networks

The maintenance port should be used when changing the switch settings and stop the services like telnet or http so as to avoid the setting changes from the network.

Privileged password

When a user changes the settings of a switch, checking the password is the most common way for user authentication. Therefore a password that cannot be easily guessed should be set as the privileged password for changing the switch settings.

Port security

If the unused ports of a switch can be used freely, the danger of being connected by the unauthorized devices will exist. Do the followings on the switches with the port security features.

- Disable the unused ports.
- Check the MAC addresses to restrict the connection to the ports.

For a non-intelligent switch, such measures cannot be applied so that some physical measures should be taken to prevent the ports from the unauthorized accesses (for example, by installing the switch in a locked rack).

SNMP setting

Intelligent switches support SNMP. SNMP enables the network management tool to monitor the state of switches. It is possible to read and write the management information with SNMP by an outsider so that the following measures need to be taken to prevent the illegal operations.

- Restrict the communications of the switch to those with network management tools.
- Disable the setting change through SNMP. (Deny SET command)
- Set a community name that cannot be easily guessed. Treat it with the same care as a password.

Network monitoring device

Network monitoring device monitors the state of network devices such as the switches by using SNMP or Ping. The following measures should be taken.

Restriction on the accesses from the outside

If a network monitoring device is used to monitor the devices on PCN and DMZ, there will be no need to allow any access from the external network, so that the settings on the firewall should be set to block the outside accesses.

Restriction on network service

Only the services of minimal requirements should be allowed. Especially for the permissions on using ftp, tftp, telnet should be very careful. If they are not necessary, they should be blocked.

Wireless access points

Take the following measures to the access points so that they can be concealed from the scanning of access points by War-driving or other similar tools.

- Disable the broadcast of ESSID. (Beacon signal)
- Disable the response to the broad request.
- Assign an administrator password that cannot be easily guessed.

4.6 Monitoring the System and the Network

Day by day, the new vulnerability of OS or network service is found and the way of attacking them is under constant evolution.

Therefore, whatever security measure the system may take, still, it is impossible to wipe out all the possibility of security incidents. It is important to monitor the system and the network without fail and if something should be wrong with them, detect the signs that may lead to incidents and try to minimize the damage as much as possible.

4.6.1 Audit Logs

Using the audit logs is effective for detecting and tracking the signs of illegal accesses. It is necessary to assign some persons responsible for regularly monitoring the audit logs.

Time-stamps are important for logs. Time should be kept accurate using NTP and so on.

TIP

It is necessary to keep the logs for a certain time in order to track the security incidents or to secure the evidence.

PC

Enable the logs for the following events.

PC component

- Audit logon events (Success / Failure)
- Audit account management (Success / Failure)

Windows Domain controller

- Audit logon events (Success / Failure)
- Audit account logon events (Success / Failure)
- Audit account management (Success / Failure)

Firewall (including personal firewall)

Regular monitoring the logs of firewall may detect the illegal access attempts from the outside.

- All the packets that violate the access control rules set in firewall should be logged.
- Worrying that the log files may become too big for the firewall, a log server can be placed in the security management segment to store the logs output from the firewall.

4.6.2 IDS/ IPS

IDS stands for Intrusion Detection System. IPS, on the other hand, is called Intrusion Prevention/ Protection System. IDS and IPS have a mechanism to inform administrators when fraud or abnormality is detected. In order to catch the omen, the logs should be audited on a regular basis.

IDS

IDS can be divided into two types, network type and host type, depending on the monitoring method of communication results. The network type IDS (Network-Based IDS: NIDS) is what monitors data flowing over the network. The host type IDS (Host-Based IDS: HIDS) is placed on the server to be monitored and monitors the data and logs received on the server generated as a result of communication. In addition to intrusion detection, it also supports tampering with files.

IDS is also classified as “Misuse detection type” and “Anomaly detection type” depending on a method of detecting unauthorized intrusion or malicious access. The misuse detection adopted in many IDS is a method to detect intrusion by matching it with a pattern or rule called a pre-registered “signature.” If the IDS finds a packet that matches the signature, it treats it as an intrusion or attack. With this type of algorithm, only intrusions using known methods can be detected.

The other hand, the anomaly detection is possible to find intrusions using unknown method by detecting traffic different from usual. Set the threshold of normal times for conditions such as login time, network traffic status, usage command etc, and judge it as abnormal when it is different. Recent IDS products often adopt both of these detection methods.

IPS

IPS is connected with networks by in-line. Basically, the IPS functions as a bridge, monitoring the traffics, detecting and excluding illegal packets like worms.

It is used:

- To segregate the PCN network into zones. (See the chapter 4.2.1)
- To protect the devices that cannot update the Security Updates and the virus definition file of at real time.

Besides excluding the illegal packets, IPS also broadcasts the notification and logs the events, so that it can also be used for monitoring the network.

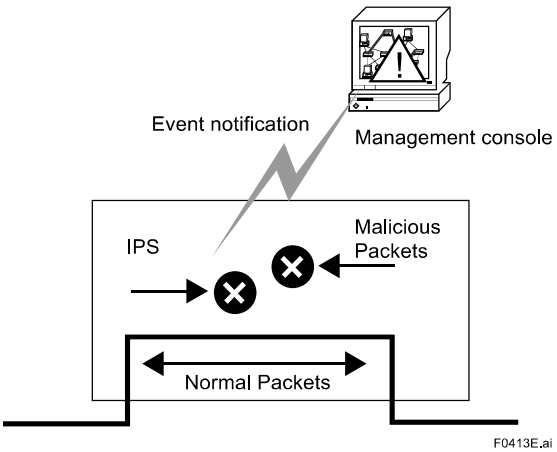


Figure The operation of IPS

Monitoring of detection events

When IPS detects and excludes the illegal packets, the notification about the events will be sent to the management console. Right after the notification is sent from IPS, a team for handling the incidents should act immediately to take care of the situation.

Notices about constructing IPS

- Handling excessive self-defense

  The communication settings defending IPS needs to be tuned in according to the environment where the IPS is placed. When the tuning is not appropriate, some inconveniences such as the intercepting the required communication frames may occur.

- Setup a route for handling troubles

  When IPS is installed in a network by in-line, if some trouble occurs in IPS, the communication between the two networks connected to IPS will be interrupted. Some IPSs have a (fail open) feature to pass all the communications at the time of troubles. However, how to handle communication packets at the time of troubles need to be decided according to the requirements of the actual systems.

- Updating signature

  In IPS, a signal called signature is used to detect the illegal packet. This signal functions the same as virus definition file in the antivirus software, so that it is necessary to update it periodically.

Difference between IDS and IPS

The difference between IDS and IPS is as follows.

- IDS only notifies that there is abnormal communication.
- IPS notifies abnormal communication and carries out even further blocks.

Yet another major difference is that IDS monitors the original copy of the communication and notifies the anomaly, but because IPS needs to block abnormal communication, it will be in between communication routes.

Therefore, in the event that a device of IPS fails, priority is given to maintaining communication, so it is necessary to pay attention that all communications are permitted as basic operation.

4.6.3 NMS

NMS (Network Management System) manages the network devices and the configuration information (IP address, port connection information, line information, etc.) present on the network, and grasps the operational status and signs of failure in real time. By performing network management, it is possible to prevent the occurrence of failures beforehand. In addition, it can gather information necessary for measures to efficiently use the network.

NMS mainly collects various information from network equipment using SNMP (Simple Network Management Protocol) and tells the administrator in an easy-to-understand manner.

SNMP

SNMP (Simple Network Management Protocol) is a UDP/IP based protocol for network monitoring and network management. It is used for status monitoring, resource monitoring, performance monitoring, traffic monitoring of network devices such as routers and switches, Windows and UNIX servers, etc. In general, CPU usage, memory usage, disk usage, process monitoring, Windows event log monitoring, and syslog monitoring are performed for the server. For network devices, it monitors the number of packets sent and received on each port, the number of error packets, the port status, CPU usage, memory usage, and so on. Some vendors have published items specific to the device, and fine monitoring is possible.

4.7 Windows Domain Management

**As Windows computers were used to run the HMI of production control systems, the Windows Domain Controller has been introduced to manage the HMI.
This section describes the operations of Windows Domain Management with considerations for security.**

TIP

The Windows domain is managed by Active Directory. Active Directory is a directory service created by Microsoft. It was released first with Windows 2000 Server. It enables centralized management of hardware resources—servers, clients, printers—on the networks, and information about users—user attributes, access rights—that use these resources. In Active Directory, the server that contains the domain database is called the Domain Controller.

Windows domain configuration for an office environment

In recent years, the needs for the clients in the office environment using their user accounts in the PC to access the process data server become more and more popular.

Generally the accounts of the PCs in office LAN are managed in a shared resource managed in the Windows domain. This section describes the Windows domain configuration for an office environment.

The users allowed to access the open process data server need to be managed. However, since the domain administrator may be different from the process data server administrator, the authorizations for accessing the process data server should be granted by the process data server administrator and independent from the Windows domain administrator.

To group the users into local groups is an effective way to manage the users for accessing the process data server.

1. Register the process data server as a member server of the domain.
2. Create a local group in the server and grant the group with the permission to access the server.
3. Register the users in the domain into this group for accessing the process data server.

In this way, the accounts of the users are managed by the domain, and it becomes possible for the local group to manage the right of the server to access.

In addition, the local groups can be granted with different privileges for accessing the process data server so that the rights of each user can be managed accordingly. The accesses are as follows.

- Permission to read data

  User has right to logon the server and read data in the server.

- Permission to write data

  User has right to logon the server and read/write data in the server.

- Permission to change the engineering settings

  In addition to the above privilege, user also has right to change the engineering settings.

By setting these privileges, it is possible to manage the user access rights properly.

Windows domain management in the production control system

Windows domain management in the PCN enables centralized management of user accounts and increases system availability. However, if the domain controller is down, there is a risk that the names cannot be resolved. It is, therefore, recommended to have a redundant Windows Domain Controller.

TIP

If a computer in the system is installed with applications that are not supported by Windows Domain Management, use the existing stand-alone management for that computer.

4.8 Security Function of Yokogawa System Products

In this clause, the security functions of Yokogawa system products that should be applied to the control system as the security countermeasures are explained from the technical point of view. Each system product is provided with the function to strengthen the security for the operation and monitoring consoles, control units and engineering stations. The security functions of an operation and monitoring console is prepared for the securities on operating the industrial plant; The security functions of an engineering station is prepared mainly for protecting the database of the system. Both operation and monitoring console and engineering station manage the security by identifying the users with the User ID and Password. The ProSafe-RS system is provided with the strengthened security functions in the controllers so that safety control means more safety.

Security of system products

Different measures have been implemented to ensure the security of Yokogawa system products. This section describes the generic IT security that uses Windows security function, and product-specific security functions.

IT security

The IT Security Setting that uses Windows security function was supported since CENTUM VP R4.01 and ProSafe-RS R2.01. Configuring IT security hardens the computer and protects it from threats.

The threats handled by IT security can be categorized as follows:

(1) Network attacks

(2) Direct attacks by manipulating computer components

(3) Theft of computer components or important data

Three different security models are available to enable you to handle these threats. These models flexibly support different system configurations and operations.

Table Security models

Model	Feature
Legacy model	This model does not strengthen the security. It prioritizes collaboration with old products and products where IT security is not applied.
Standard model	This model focuses on the relevant system operations and collaboration with other systems. It can counter threats (1) and (2).
Strengthened model	This model is used to counter all the three threats stated above. Operations may be affected if full security is in place.

Yokogawa IA system products provide a tool that automatically configures the security setting for the threats above. There are two kinds of security settings - IT security version 1.0 and IT security version 2.0.

- IT security version 2.0

  This version was designed after reconsidering the IT security version1.0 and includes more security measures. It supports the Standard and Strengthened (*1) security models.

- IT security version 1.0

  This version had been offered as the security measures of CENTUM VP R6.03 and earlier versions. It supports the Legacy, Standard, and Strengthened (*1) security models.

*1: Please contact Yokogawa for more details about settings of the strengthened model.

IT security version 2.0 and IT security version1.0 can coexist in the same project in CENTUM VP.
The following tables show the security threats that are coped by this security measures.

Table IT security version 2.0

Security measure	Threat handled		
	(1)	(2)	(3)
Password Policy-[Minimum password length]	Yes	Yes	No
Password Policy-[Minimum password age]	Yes	Yes	No
Password Policy-[Maximum password age]	Yes	Yes	No
Password Policy-[Enforce password history]	Yes	Yes	No
Disable 'Password Policy-[Store passwords using reversible encryption]'	Yes	Yes	No
Password Policy-[Password must meet complexity requirements]	Yes	Yes	No
Access Control for files and folders	Yes	Yes	No
Access control for product registry	Yes	Yes	No
Access Control for DCOM (OPC) objects	Yes	Yes	No
Personal firewall tuning	Yes	No	No
Set 'Personal Firewall-[Allow unicast response]' to 'No'	Yes	No	No
Stopping unused Windows services	Yes	No	No
Account Lockout Policy-[Account lockout threshold]	Yes	Yes	No
Account Lockout Policy-[Reset account lockout counter after]	Yes	Yes	No
Account Lockout Policy-[Account lockout duration]	Yes	Yes	No
Disabling NetBIOS over TCP/IP	Yes	No	No
Applying the StorageDevicePolicies function	No	Yes	Yes
Disabling USB storage devices	No	Yes	Yes
Applying the software restriction policies	Yes	Yes	No
. . . (0mission) . . .			
Security-[Require secure RPC communication]	Yes	No	No
Security-[Require user authentication for remote connections by using Network Level Authentication]	Yes	No	No
Sync your settings-[Do not sync Apps]	Yes	No	No
Sync your settings-[Do not sync start settings]	Yes	No	No
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Yes	No	No
Disable 'Windows Logon Options-[Sign'-in last interactive	No	Yes	No
user automatically after a system'-initiated restart]'	No	Yes	No
Notifications-[Turn off toast notifications on the lock screen]	Yes	Yes	No
Disabling Built-in Administrator Account or Changing User Name	No	No	Yes

Table IT security version 1.0

Security measure	Threat handled		
	(1)	(2)	(3)
Access control	Yes	Yes	No
Personal firewall tuning	Yes	No	No
Stopping unused Windows services	Yes	No	No
Disabling the built-in Administrator account or changing its user name	Yes	Yes	No
Hiding the last logon user name	Yes	Yes	No
Applying the software restriction policies	Yes	Yes	No
Applying AutoRun restrictions	No	Yes	No
Applying the StorageDevicePolicies function	No	Yes	Yes
Disabling USB storage devices	No	Yes	Yes
Disabling NetBIOS over TCP/IP	Yes	No	No
Changing the LAN Manager authentication level	Yes	No	No
Applying the password policy	Yes	Yes	No
Applying the audit policy	Yes	Yes	No
Applying the account lockout policy	Yes	Yes	No
HDD password function by BIOS	No	No	Yes

For details about IT security, refer to IM of each product.

- CENTUM VP Security Guide (IM 33J01C30-01EN)
- ProSafe-RS Security Guide (IM 32P01C70-01EN)
- STARDOM IT Security (IM 34P02Q93-01E)
- Plant Resource Manager Security Guide (IM 33Y05Q13-11E)
- Exaopc Security Guide (IM 36J02A01-01E)
- Exapilot Security Guide (IM 36J06B01-01E)
- Exaplog Event Analysis Package Security Guide (IM 36J06A01-01E)
- FAST/TOOLS Windows IT Security Guide (TI 50A 01A10-04EN)

TIP

The content of “IT Security Guide for System Products (for each product)” issued as TI 30A15B3x-01E is old. For the latest information, please refer to the above IM.

4.8.1 CENTUM VP

The security settings of CENTUM can be classified into two functions, the IT security function based on Windows security feature, and the CENTUM VP peculiar security function.

IT security function of CENTUM VP

The IT security function to enhance security is supported on CENTUM VP. System-hardening of CENTUM VP IT environment is realized by using Windows functions. For example, the usage of CENTUM VP tools and access permissions to folders/files are managed by access control for users and groups of Windows. Therefore, it is possible to apply the security countermeasures in such circumstances to allow a Windows user as an operator to logon to the PC for using the operator windows and tools but restricted from starting the engineering to tools.

Moreover, some communication types and communication ports can be disabled by Windows firewall and DCOM settings.

IT security version 2.0 is applicable for CENTUM VP R6.04 or later.

Authentication mode

In R4.02 or earlier of CENTUM, you can define users and their respective access rights for CENTUM Engineering or CENTUM Operation and Monitoring function. These users are independent from Windows users. That is the CENTUM Authentication mode. By using the Windows Authentication Mode that was newly added in CENTUM VP R4.03, you can integrate Windows accounts with Operation and Monitoring users, and ensure a secure system within the Windows user management framework. In case of necessity more strong security, it is recommend to use windows authentication mode. And, by making good use of the centralized user management made possible with Windows domain configuration, you can significantly improve the usability of the system.

CENTUM VP specific security function

CENTUM VP have a specific security function for controlling accesses, mainly for controlling the accesses to the controller data and application database. The HIS user used for this access control is specially defined for CENTUM VP. As mentioned earlier, from CENTUM VP R4.03 onwards, the Windows Authentication Mode is available to associate Windows User Account function with CENTUM User management.

In CENTUM VP, the users are usually divided into 4 groups; Operators, System engineers, Recipe engineers and Report users. The access control is applied to each user group. The user groups are largely divided into the following 2 categories.

- HIS group user: Operators (Operation and Monitoring Function)
- ENG group user: System engineers (System View/Builders)

  Recipe engineers (Recipe Management Function)

  Report users (Report Function)

These are the access control functions. (*1)

- Register or delete user IDs
- Set user rights for each user ID
- Automatic User-Out
- Check Illegal access
- Lockout users
- Release locked user IDs
- Reconfirm with double authentications (*2)
- Check validity period of password
- Check and block the obsolete password
- Set minimum password length
- Automatic logon Windows
- Set CENTUM desktop environment

*1: With the Windows Authentication Mode, some of these access control functions are handled by the Windows User Account Management function.
*2: In security terms, this is known as Dual Lock function.

For the security of the system, we recommend that the above mentioned access control functions be applied according to the privileges of the users.

SEE ALSO For more details about the access control functions of ENG group user, refer to:

Access Control Package (GS 33J10D20-01EN)

Access Administrator Package (FDA:21 CFR Part 11 compliant) (GS 33J10D40-01EN)

4.8.2 ProSafe-RS

ProSafe-RS supports the IT security function based on Windows security feature, also the CENTUM VP peculiar security function can be applied on ProSafe-RS/CENTUM integrated system. In addition, ProSafe-RS has peculiar security functions to enhance security as Safety Instrumented System.

IT security function of ProSafe-RS

The IT security function to enhance security is supported on ProSafe-RS R2.01 and later. System-hardening of ProSafe-RS IT environment is realized by using Windows functions. Moreover, the IT security function can be applied on ProSafe-RS/CENTUM VP integrated system. Therefore, it is possible to apply the security countermeasures in such circumstances to allow a Windows user as a CENTUM VP engineer to logon the PC for using the CENTUM VP engineering tools but restricted from starting the ProSafe-RS engineering tools.

IT security version 2.0 is applicable for ProSafe-RS R4.03 or later.

CENTUM VP specific security function

This security function can be used on ProSafe-RS and CENTUM VP integrated system. By using the security control function with HIS user, it is possible to control access permission to the data of SCS (Safety Control Station).

ProSafe-RS specific security function

ProSafe-RS has the following securities in order to inhibit the access to the system by the unauthorized users or from the unauthorized devices to prevent the unintended changes resulted from the operation errors of the users.

Table Outline of the security function of ProSafe-RS

	Access control by password	Access control by hardware key switch	Remarks
Change in project database	Applicable	N/A	Access control rule can be set for the whole SCS or for each program in SCS.
Non-safety operations to SCS	Applicable	N/A	Access control by SCS Maintenance Support Tool in SENG
Safety-related operations to SCS	Applicable	Applicable	Access control is applied to both the operations from SENG and from HIS. Permit or Deny is handled in SCS.

The passwords should be used and the passwords should be difficult for an outsider to guess. For more information about assigning passwords, see the descriptions about the password assignment rules cited in the chapter 4.5.

In addition, a hardware key switch can also be used for access control according to the requests from the customers.

SEE ALSO There is a function that sets the operation rights of engineers. For details, refer to:

Access Control and Operation History Management Package (GS 32P04D30-01EN))

4.8.3 STARDOM

STARDOM has two types of security functions, an IT security function based on the Windows security function, and a STARDOM specific security function.

IT security function of STARDOM

The IT security function to enhance security is supported on STARDOM R3.20 or later. It makes use of Windows functions to harden the STARDOM IT environment. For example, it uses the access control function for Windows users and groups to control usage of STARDOM tools and access to folders/files. In addition, this function configures Windows Firewall and DCOM to limit communication types and communication port numbers.

Security settings are easy to use by the tool that is included in this product. STARDOM supports Legacy model and Standard model.

STARDOM specific security function

In STARDOM, the operators are divided into various groups and the operable range for each group is specified, as in CENTUM VP. Moreover, the record of the operation by the operators can be kept. Manage the passwords carefully so as not to allow an outsider masquerading as a user to operate the system. The following are the security functions of STARDOM. Apply these functions to the PCs according to the requirements for preventing the operational errors and improving the operation safety.

- Set operation range for each user group
- Protect the operation files
- Manage HMI server passwords
- Notify the password change
- Notify the password expiration in advance
- Notify the password expiration
- System inhibitions: Inhibit some Windows functions
- Desktop inhibitions: Inhibit some operations on Windows desktop
- Application inhibitions: Inhibit some operations on Internet Explorer

4.8.4 Plant Resource Manager (PRM)

PRM has two types of security functions, an IT security function based on Windows security function, and a PRM specific security function.

IT security function of PRM

The IT security function to enhance security is supported on PRM R3.03 or later. It makes use of Windows functions to harden the PRM IT environment. For example, it uses the access control function for Windows users and groups to control usage of PRM tools and access to folders/files. In addition, this function configures Windows Firewall and DCOM to restrict communication types and communication port numbers.

IT security version 2.0 is applicable for PRM R4.01 or later.

PRM specific security function

With regards to security, PRM is equipped with the functions of access control of users, access control of the connected devices and management of operation history.

Access control of operators

In PRM, users are managed by their user names. In order to use the functions of PRM, it is necessary to have a user name and a password. The passwords should be carefully managed so as not to allow an outsider to operate the system illegally.

A user must belong to a user group. Moreover, each window on PRM is provided with a setting for the access privilege of each user group. A number of default user group are already built in the PRM, however, the new user groups can be added according to the actual security management policy.

A further concept in PRM is the permissions for each user. The operation privilege of a user is not only subject to the privileges set for each user group but also subject in detail to the permissions for the individual user.

Access restrictions on the connected devices

PRM can not only restrict the users on operating various PRM functions, but also restrict users on accessing various devices connected with PRM. The permissions for accessing the connected devices need to be configured according to the authority of each user.

Audit trails of the operations

PRM keeps the records of all operations. All the operation events on PRM, all the operations on the devices connected to PRM and all the inspection events and inspection results of these devices are logged as audit trails. The audit trails can be displayed and printed out.

4.8.5 B/M9000 VP

B/M9000 VP has two types of security functions, an IT security function based on the Windows security function, and a B/M9000 VP specific security function.

IT security function of B/M9000 VP

This function was prepared to strengthen the security for B/M9000 VP, similar to that of CENTUM VP. It makes use of Windows functions to harden the B/M9000 VP IT environment. For example, it uses the access control function for Windows users and groups to control the usage of B/M9000 VP and CENTUM VP tools and access to folders/files. In addition, this function configures Windows Firewall and DCOM to restrict communication types and communication port numbers.

B/M9000 VP specific security function

B/M9000 VP has unique access control functions for screen customization. This security function is managed separately from Windows security. Users are classified into operators, staff, and engineers, and different access control functions are used for each of these user groups.

User groups are classified into three major categories:

- Operator group: operators
- Maintenance group: staff
- Engineer group: instrument engineers, engineers

The following access control functions are available:

- System installation and uninstallation, system device registration and deletion. (engineer group)
- System backup and restore, screen customization. (maintenance group)
- Screen operation. (operator group)

To ensure that the system is secure, it is recommended to configure these access control functions according to user rights.

4.8.6 Exaopc

Exaopc has two types of security functions, an IT security function based on the Windows security function, and an Exaopc specific security function.

IT security function of Exaopc

This function makes use of Windows functions to harden the Exaopc IT environment. For example, it uses the access control function for Windows users and groups to control usage of Exaopc tools and access to folders/files. In addition, this function configures Windows Firewall and DCOM to restrict communication types and communication port numbers.

IT security version 2.0 is applicable for Exaopc R3.76 or later

Authentication mode

Exaopc R3.70 or later uses the user authentication mode when accessing to CENTUM data. Either “CENTUM authentication mode” or “Windows authentication mode” is applicable.

Exaopc specific security function

OPC security interface

Exaopc can set its security by OPC Security compliant interface, when OPC client uses DA/A&E/HDA/Batch server function. The username/password specified here is used by the following CENTUM security function.

CENTUM security function

CENTUM VP specific security functions can also be applied to Exaopc. For example, access restrictions by user groups can be used. This allows you to set fine security for OPC clients.

4.8.7 Exaquantum

Exaquantum has its own unique security functions, which are as follows.

Exaquantum specific security function

The security function of Exaquantum is realized according to the users and groups managed by Windows. Each user can be defined with adequate security. For an example, an engineer or a user can change the process data, while another user can only read the process data by registering the different users to different groups as explained in below. As a result, the operation errors and illegal operations by the unauthorized users can be prevented. In addition, the operation events by the users can be recorded as audit trails.

Exaquantum has preset the default users beforehand in the system. It is especially important to manage the passwords of default users strictly. On assigning the passwords, you should follow the rules explained in the chapter 4.5 System-Hardening.

The following shows the groups regarding to the security management.

Connection security group

This group is for the users to connect with Exaquantum server; and granted with the following privileges.

- Referencing data
- Displaying graphics

Management security group

This group is for the users to change the management information or write data on Exaquantum; and granted with the following privileges.

- Changing database settings
- Creating tags
- Writing data

Writing data security group

This group is for the users to write tag data; and granted with following privileges:

- Changing data
- Writing to DCS

Graphic editing security group

This group is for the users to edit graphics; and granted with following privileges:

- Editing graphic displays

RBNS security

This is a set of settings about the permissions for reading and writing to the tags corresponding to each security groups regarding the following privileges:

- Referencing data
- Changing data

4.8.8 Exapilot

Exapilot security functions can be classified into two types, an IT security function based on the Windows security function, and an Exapilot specific security function.

IT security function of Exapilot

This function is created to strengthen the security for Exapilot R3.70 and later versions. It makes use of Windows functions to harden Exapilot VP IT environment. For example, it uses the access control function for Windows users and groups to control the usage of Exapilot tools and access to folders/files. In addition, this function configures Windows Firewall and DCOM to restrict communication types and communication port numbers.

IT security version 2.0 is applicable for Exapilot R3.97.00 or later.

Authentication mode

Exapilot has two types of user authentication mode below.

- Windows authentication mode

  The way to authenticate a user by using the Windows function.

- Exapilot authentication mode

  The way to authenticate a user by using Exapilot specific function.

Exapilot specific security function

Exapilot has a security function to authorize operation permissions for each user, where the user is controlled by Exapilot. Exapilot specific security is classified into three types; system security to apply on all operations; main procedure security to apply on main procedures; and subprocedure security to apply on sub procedures. By setting these securities, each user can have suitable security rights for administrator, operator and engineer privileges. As a result, operation errors and illegal operations by the unauthorized users can be prevented. In addition, the operation events by the users can be recorded as audit trails.

It is recommended to assign the passwords that cannot be easily guessed by the outsider to the users and set the operation privilege of each user to a minimum level. On assigning the passwords, you should follow the rules explained in the chapter 4.5 System-Hardening.

System security

Exapilot system security restricts access and permissions on the following operations for each user.

Operations that can be restricted

- Operation window
- Builder window
- Utilities window
- Security window
- The other tools

Main procedure security

Main procedure security restricts the building and running operations of individual procedures for each user.

Operations that can be restricted

- Building operation
- Running operation

Subprocedure security

Subprocedure security restricts the building and running operations of individual procedures for each user.

Operations that can be restricted

- Building operation
- Running operation

4.8.9 Exaplog

Exaplog has two types of security functions, an IT security function based on the Windows security function, and an Exaplog specific security function.

IT security function of Exaplog

This function makes use of Windows functions to harden the Exaopc IT environment. For example, it uses the access control function for Windows users and groups to control usage of Exaopc tools and access to folders/files. In addition, this function configures Windows Firewall to restrict communication types and communication port numbers.

Exaplog specific security function

Execution of the Exaplog program is limited by the user group as shown in the table below.

Window name/ Tool name	PLG_ANALYST (PLG_ANALYST_LCL)	PLG_SUPER_ ANALYST (PLG_SUPER_ ANALYST_LCL)	PLGMAINTENANCE (PLG_MAINTENANCE _LCL)	EXA_MAINTENANCE (EXA_MAINTENANCE_ LCL)
Event analysis tool (PLView)	Yes	Yes	Yes	
Long-term summary tool (PLSummary)	Yes	Yes	Yes	
Exaplog administration (PLAdmin)		Yes	Yes (*3)	
Tri-REPORT data import tool		Yes	Yes	
Command under Exaplog¥tool		Yes	Yes	
Password change tool			Yes	
IT security tool				Yes
Software Configuration View	Yes (*1)	Yes (*1)	Yes	Yes
EXA Information Gathering Tool				Yes (*2)
Install				Yes
Client Install				Yes

*1: Exaplog information can be displayed. User accounts without administrator's authority cannot display registry information.
*2: For the start method, refer to the instruction manual for the EXA Package Information Gathering Tool.
*3: PLG_MAINTENANCE is used to change the setting for automatic start of Exaplog with PLAdmin.

4.8.10 FAST/TOOLS

FAST/TOOLS has two types of security functions, an IT security function based on the Windows security function, and a FAST/TOOLS specific security function.

IT security function of FAST/TOOLS

IT security version 2.0 is applicable for FAST/TOOLS R10.04 or later. This function makes use of Windows functions to harden the FAST/TOOLS IT environment. For example, this function configures Windows Firewall to restrict communication types and communication port numbers, stops unused Windows services, and uses the access control function for Windows users and groups to control usage of FAST/TOOLS and access to folders/files.

FAST/TOOLS specific security function

The FAST/TOOLS specific security function falls into two categories.

(1) User Management function

FAST/TOOLS has security mechanism considering the SCADA based application security. This mechanism is possible to manage users considering functional authorization such as read-only permission and full system configuration permission versus area authorization. Additionally, FAST/TOOLS supports sophisticated user profiles which can integrated with Active Directory user management by mapping user group name on AD to FAST/TOOLS user profiles. And, FAST/TOOLS supports “Single sign-on” based on Active Directory.

(2) Communication function

FAST/TOOLS enables users to Monitor, Control and Engineer their application systems in a wide distributed network configuration. FAST/TOOLS supports security countermeasures to data connections as below.

- Secure Communication by encryption (Client to Server)
  Operation data is displayed in Web-HMI client and Mobile client via FAST/TOOLS Web server. FAST/TOOLS supports Secure Socket Layer(SSL) to secure this data connections.
- Secure Connection by encryption (Server to Server)
  Communication between two FAST/TOOLS Systems used in FAST/TOOLS distributed systems is encrypted. FAST/TOOLS multi-node network security is based on industry standards that are also used for secure communication on the Internet, including DTLS and public/private keys.
- OPC UA
  OPC UA is the next-generation standard of OPC developed by OPC foundation. OPC UA provides a cohesive, secure, and reliable cross-platform framework for access to real-time and historical data and events. FAST/TOOLS supports both Server (DA/AC/HA) and Client (DA) roles of OPC UA. FAST/TOOLS together with the security features of the OPC UA, supports users connecting new or existing equipment to secure, high reliable and manageable network.

4.9 Staff Security Policy

One of the major threats that may lead to security incidents is “human.” A human mistake, such as an incorrect operation, can be a major threat.

4.9.1 Education

The purpose of the education is to make the staff to have skills and knowledge of security so that they act in accordance with the security rules in daily works.

Education should include below items, but not limited to:

- To make the staff be matured for understanding about security.
- To make the staff to aware of the threats and influence to production control system correctly.
- To make the staff to implement security countermeasures and improvement adequately.
- To make the staff to operate the system correctly and manage it tidily. For example, make the staff to understand how to confirm the log to identify the existence of an attack to the system.

The education should be done on these occasions.

- When the staffs are employed
- When the staffs are moved to a new position or the accessed targets of the staffs are changed, an so on

4.9.2 Training

The first purpose of training is to enable the staff to perform the right operation and management so that to prevent the security incidents. Another purpose of the training is to make the stuffs to respond properly on the security incidents, and to make them capable to cope with such occasions. It is also important to make the staff in readiness over incidents.

The procedure in detail is provided in the Business Continuity Plan described in Chapter 6. It is necessary to regularly train the stuffs under the assumed the security incidents for taking the right actions.

5. Physical Protection

To obtain the physical security for a control room where the system is located is a very important element in decreasing the threats of security.

5.1 Define Physical Boundary

The control room where the system is located should be regarded as a security area and physical security must be defined. The secured area is an area protected the barriers.

The barriers here also include the management of the ID cards, the code numbers and the keys for entering the secured rooms. More than one security area can be defined according to the level of security required. Security areas have effects as follows, but not limited to:

- To prevent an unauthorized equipment be connected to the network.
- To prevent the loss of equipments such as PC or backup medias be stolen.

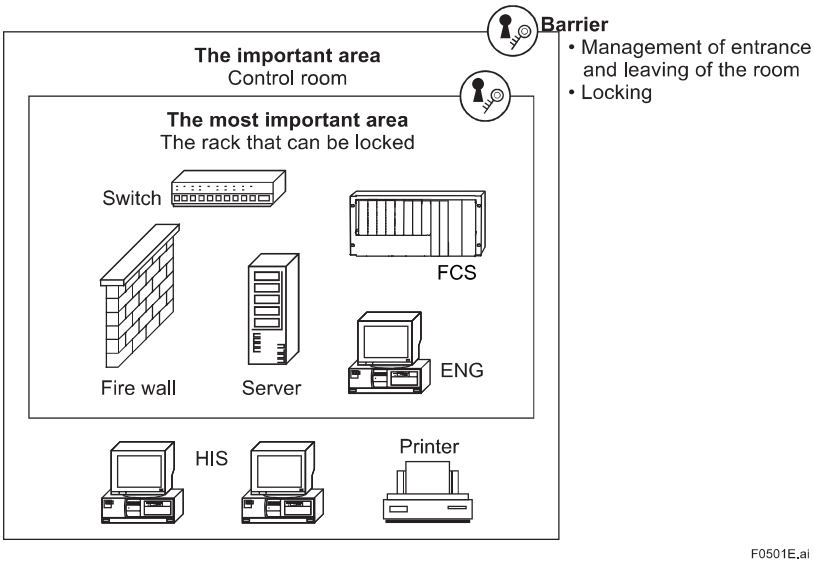


Figure Example of the configuration of security area

Moreover, PC components such as HIS and ENG should be placed in the security area by following reasons.

- To eliminate the opportunity of illegal usage.
- To prevent from installing the tool for stealing information, such as Key Logger.
- To keep the entrance and leaving records and the records can be used as forensic evidences.

Important areas

The control room where the operators operate the devices to control plant every day is considered to be an important area. The devices necessary for the operations are placed here. Only a limited number of people, i.e. operators and engineers should be allowed to enter this area.

Example of devices should be placed in the important area

- Operator stations (HIS etc.)
- Printers

Printer should be placed in the important area to secure the confidentiality of printouts.

The most important area

The important devices are placed in this area, where the devices are not necessarily operated for the daily operations. For an example, the racks that can be locked should be placed in this area. Entering to this area should be strictly controlled so that only a small number of people such as engineers are allowed.

Example: The devices that should be placed in the most important area

- Controllers including the wirings to the devices (FCS,FCJ/FCN,SCS)
- Engineering stations (ENG)
- Network devices (Switches and Gateway Units)
- Security devices (Firewalls)
- Spare equipments such as the PCs.

Example: The media that should be placed in the most important area

- Media used for installing system software to PC.
- Backup media

5.2 Management of Removable Devices

The removable devices such as CD/DVDs, floppy disks or USB memory sticks are not needed in the daily plant operation. It is dangerous to keep them in the freely accessible environment, for there may be the possibility that the files infected by computer viruses or illegal programmes are installed. Thus, it is very important to prevent the removable devices from being used illegally.

We recommend the following measures.

Disabling AutoRun

Windows has a function that automatically runs programs from atached removable drives.

Disable the AutoRun function to prevent virus infection due to misuse of AutoRun.

Disabling the removable devices

Disable the floppy disks, CD/DVD drives and USB devices in the control room. In this case, it is necessary to strictly protect the BIOS settings from the outsiders by authenticating the password and the administrator privilege.

Detaching removable drives

Consider to physically detach removable drives if it does not trouble the operating environment.

Handling USB memory sticks

IMPORTANT

USB memory sticks are widely used as external storage devices due to their large capacity, low price, and easy usage. However, USB worms or virus infection from USB memory sticks have become a very common problem.

Therefore, we need to control the usage of USB memory sticks in production control systems. This can be done by building a stringent management system that restricts the usage of USB memory sticks to limited devices, and enforces absolute compliance to regulations.

5.3 Third Party Maintenance

Some maintenance works of security devices such as PCS or Network devices, the maintenance workers of the third party vendors need to work in the important area or the most important area. Since these works are carried out to the critical devices, it is essential to guarantee the security.

The maintenance works should be carried out in the presence of the user all the time, and the user must check if the third-party maintenance works are properly performed in accordance with the work procedures.

6. Business Continuity Plan

Business continuity plan is explained here.

Since a high level of availability is required for the production system, it is important to decide the business continuity plan in advance. And make sure that the plan, including the training programs, would guarantee the system be properly restored in case an incident happened.

6.1 Plan

When creating a business continuity plan, the following has to be taken into consideration.

Recovery plan

Disaster recovery plan should be made to secure the recovery of the system on an incident. The plan should include the roles and responsibilities of the departments, persons in charge and their contact information. The plan should also include activities of restoration to deal with the confusions and obstacles occurred by the incident.

Acceptable time for restoration

Decide how much time will be required for backup and restore and if redundancy is necessary.

Backup interval

Keep a number of backups to prepare for unexpected incidents such as corrupted storage mediums.

Backup objects

Backup should contain the following three objects.

- Operating system and other system software.
- Application software
- Application parameters. The parameters tailored by the process engineer. For example, Tuning Parameter of CENTUM VP.

Backup management

Keep a number of backups to prepare for unexpected incidents such as corrupted storage mediums.

Storage location of backup media

Keep the backup media in a safe place such as a cabinet that can be locked so that the security is guaranteed. This is required because if the backup information is passed to an attacker, the possibility of cyber attack will be largely increased.

TIP

Yokogawa system products provide tools for efficiently backups.

Clarification of responsibility

It is necessary to make clear what department or who is responsible for the activities in the business continuity plan.

- Backup activity
- Training activity
- Restore activity

Review and update the plan

When the system configuration or the system environment changes, it is necessary to review and update the business continuity plan.

Review and update the plan is required when:

- the new devices are installed,
- the system is upgraded,
- the location of the equipment is changed,
- the business is expanded or changed.

6.2 Training

It is necessary to conduct regular trainings in accordance with the business continuity plan so that in case of emergency, the system can be certainly restored.

It is also essential for the staffs in charge of each activity in the business continuity plan to take part in these trainings.

Not only internal education but also external institution training and public qualification acquisition should be planned. For example, it is necessary to take measures to encourage acquisition of GICSP (Global Industrial Cyber Security Professional), which is international certification for security measures engineering of control systems.

- Global Industrial Cyber Security Professional (GICSP)

  https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

Yokogawa trains engineers with GICSP qualifications.

- Yokogawa Promotes GICSP Training to Enhance Plant Safety

  http://www.yokogawa.com/pr/topics/2015/pr-topics-2015-0508-02-en.htm

6.3 Maintenance

Security measures should not be done once at installation. Daily new vulnerabilities are discovered, and the threat to the control system is increasing. It is necessary to always execute PDCA cycle (plan-do-check-act cycle) for security measures.

Yokogawa prepares the following security countermeasure service and support the continuous operation of IA control system.

(1) AV/OS(*1) Implementation Service

(2) AV/OS(*1) Update Service

(3) Security Information Service

(4) Virus Check Service

(5) Software Backup Service

(6) USB Port Lock Service

(7) Malware Inactivated Service

(8) Security Effectiveness Service

*1: Antivirus software / Microsoft Security Updates

SEE ALSO For details of the above services, please refer to:

Endpoint Security Service (GS 43D02T30-02EN)

6.4 Measures against Software Vulnerability

Vulnerability of software is defined as “a security flaw in a software product or other item that may be attacked by computer viruses or unauthorized access to cause damage to its function or performance.”

Vulnerability and software defect are often confused with each other, and many causes of the vulnerabilities are, in fact, defects. However, vulnerabilities are different from the defects that cause system hang-up or other failures in usual operation by customers. Vulnerability is a potential risk under the usual operation environment of customers, which causes incidents such as system hang-up only after being attacked. From the viewpoint of preventing security incidents, vulnerability must be handled while it is in the state of potential risk.

Yokogawa makes every effort to collect the latest vulnerability information, feed it back to the operations, and makes use of it for improving development processes, operation standards and operating procedures. Yokogawa offers customers not only secure products but also support regarding vulnerability through providing measures and workarounds for vulnerabilities based on the latest information.

- Yokogawa Security Advisory Report List

  https://www.yokogawa.com/library/resources/white-papers/yokogawa-security-advisory-report-list/

- Yokogawa Innovative Plant Automation Security Solutions

  https://www.yokogawa.com/library/resources/white-papers/yokogawa-innovative-plant-automation-security-solutions/

Blank Page

Revision Information

Title: Security Standard of System Product

Manual No.: TI 33Y01B30-01E

Sep. 2006/1st Edition
Newly published

Apr. 2008/ 2nd Edition

Introduction	B/M 9000CS addition to Target Products.
4.2.7	Deleted a description of the Secure Ticket of Personal authentication.

Sep. 2008/3rd Edition

Introduction	CENTUM VP added to Target Products
1	Figure Outline of the system revised
2	Some items added to Examples of data assets
	TIP ISA 99.00.01 added
	TIP Activity-based criteria and Asset-based criteria added
3.4	Examples of the vulnerability revised and some items added
3.5	Risk Assessment revised
	Formula showing Risk revised
3.6	The title is revised to “Design and Implement of the Measures”
	Priority of Availability, Integrity and Confidentiality added
3.8	Description of health, safety, environment added
	Monitoring log of network added to Daily monitoring of the system
	Software in use added to Regular auditing
4.1	Risk Definition and Security Zone added
4.2.1	Level of ISA 99.00.01 Reference Model descriptions added
	Description of IPS revised at Horizontal segmentation
	SEE ALSO 4.6.2 IPS added
4.2.2	Figure Equipment class revised
	Description of classification added
4.2.4	Description of Dual-Home Server revised
4.2.5	Title is changed from “Vnet/IP Open Channel” to “OPC Interface”, and all contents are revised
4.2.6	Description added at Authentication of terminals
4.2.7	Figure Example of the configuration of remote monitoring network revised
	Figure Example of Personal Authentication revised
4.2.8	Description added at Use of RAS, Authentication by using the caller ID and The system-hardening of RAS
	Figure Example of the configuration of remote maintenance by Modem revised
4.4	Security Patches Management revised
4.8.1	The title is changed to “CENTUM VP/CS3000”
	CENTUM VP security description added
4.8.2	Revised “4.8.3 ProSafe-RS” to “4.8.2 ProSafe-RS”
	ProSafe-RS security description revised
4.8.3	Revised “4.8.2 STARDOM” to “4.8.3 STARDOM”
4.8.5	Exaquantum security description revised
4.8.6	Exapilot security description revised
4.9.1	Education revised
4.9.2	Training revised
5.1	Define Physical Boundary revised
6.1	Recovery plan and Backup objects added

Feb. 2011/4th Edition

Introduction	Deleted “R3” from “CENTUM CS 3000 R3” in Target Products
	Deleted the sentence of “CENTUM CS 1000 R3” from Target Products
	Changed “B/M9000 CS” to “B/M9000 VP” in Target Products
	Added “-Based Software” between “Solution” and “Packages”
1	Changed “Security Patches” to “Security Patch” in Figures
	Changed “Public Server” to “DMZ Server” in Figures

4.2.6	Added a lead sentence for this section Added the 1st headline “Wireless LAN (IEEE 802.11)” Changed “wireless network” to “wireless LAN” in the text Changed the 2nd headline “Application to control bus” to “Wireless application to control bus” Added the 3rd headline “Field wireless (ISA 100.11a)” and its description
4.4	Changed “Patches” to “Patch” in the title Added SEE ALSO about security patches
4.7	Changed the title “Configuration of Windows Domain” to “Windows Domain Management” Added a lead sentence and TIP Added the headline “Windows domain configuration for an office environment” Added the headline “Windows domain management in the production control system” and its description
4.8	Changed the title “Security Functions Specific to Each Product” to “Security Function of Yokogawa System Products” Added the headline “Security of System Products” and its description
4.8.1	Changed the description for the authentication mode of CENTUM VP R4.03
4.8.3	Changed “CENTUM CS 3000” to “CENTUM VP/CS 3000”
4.8.4	Added a lead sentence for this section Added the 1st headline “IT security function” and its description Added the 2nd headline “PRM specific security function” Changed “operators” to “users” in the text
4.8.5	Added the chapter “B/M9000 VP” Added 1 to chapter numbers after this chapter
4.8.7	Added a lead sentence for this section Added the 1st headline “IT security function” and its description Added the 2nd headline “Exapilot specific security function”
5.2	Added the headline “Disabling AutoRun” and its description Added the subheading “Handling USB memory sticks” and its description Changed “CD” to “CD/DVD” Changed “the removable devices” to “removable drives”
6.1	Changed “CENTUM is provided with the” to “Yokogawa system products provide” Corrected grammatical errors, usage and wording (Chapter 1, 4.2, 4.2.1, 4.2.2, 4.2.3, 4.2.5, 4.2.6, 5.1, 6)

June 2013/5th Edition

2	Added a description about the recent security threats
4.3	Added a description about antivirus software
4.4	Added a description about applying security patches
4.5.1	Deleted the description about the old security holes

Apr. 2018/6th Edition

All	Deleted descriptions about CS 3000
1	Changed the explanation about chapter 3
3	Reformed chapter 3 in its entirely (Changed “ISMS” to “Security Standards and Certifications”)
4.3	Changed the title of this chapter to “Anti-malware”, and added Whitelisting software
4.6.2	Added “IDS”
4.6.3	Added the whole chapter of “NMS”
4.8	Added the description about IT security version 2.0
4.8	Added and/or changed the descriptions in accordance with the latest version of the products
4.8.6	Added the whole chapter of “Exaopc”
4.8.9	Added the whole chapter of “Exaplog”
6.3	Added the whole chapter of “Maintenance”
6.4	Added the whole chapter of “Measures against Software Vulnerability”

Nov. 2019/7th Edition

All	Change “security patches” to “Security Updates”.
All	Change “pattern” to “virus definition file”.
3.2	Delete a description regarding CSMS certification.
3.3	Update a description regarding NIST Cybersecurity Framework.
3.4	Update a description regarding ISASecure.
3.5	Update a description regarding ISA99.

3.6 Update a description regarding IEC62443.
4.3 Change referenced document to Endpoint Security Service.
4.8.1 Add a description regarding Athentication mode.
4.8.10 Add a description regarding FAST/TOOLS.

Written by Yokogawa Electric Corporation

Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Subject to change without notice.

Attachment 9.15 Safety Control Station (S2SC70D)

GS 32P06D10-01EN

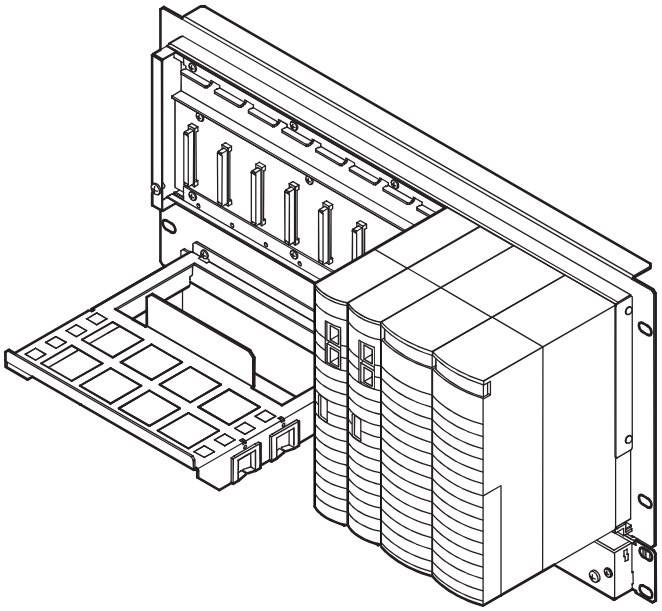
General Specifications

GS 32P06D10-01EN

ProSafe-RS
S2SC70S, S2SC70D
Safety Control Unit, Duplexed Safety Control Unit
(for N-IO/FIO, Rack Mountable Type)

■ GENERAL

This General Specifications (GS) provides the hardware specifications of the safety control unit, which are intelligent parts of the safety control station (SCS). This product supports both N-IO and FIO.



F01E.ai

■ HARDWARE SPECIFICATIONS

For the criteria for the installation environment, refer to “ProSafe-RS Safety Instrumented System Overview (for Vnet/IP)” (GS 32P01B10-01EN).

● Safety Integrity Level

SIL 3

● Module Configuration

Power Supply Module (SPW481, SPW482 or SPW484): 2 modules
Processor Module (S2CP471 or SCP461 style S2 or later): 2 modules for dual-redundant configuration. (*1)

*1: A dual-redundant configuration is enabled by using 2 identical modules with same model code (S2CP471 or SCP461).

● Memory Protection at Power Failured

Application program is stored in the flash memory. Processor module operation data is stored in NVRAM (nonvolatile memory).

● Temperature Adaptability

A fan unit is provided for high temperature use where the safety control units (S2SC70S-F/S2SC70D-F) ambient temperature exceeds 40 °C.

● Control Network

Vnet/IP interface: Dual-redundant

● No. of Node Units Connectable

In order to extend the number of I/O channels, S2SC70☐ allows N-IO nodes and safety node units to be connected to it. The number of individual nodes that can be connected is as follows.

N-IO node (*1): Max. 32/ SCS
Safety Node Unit (SNB10D): Max. 13/ SCS

*1: For details, refer to the GS “ProSafe-RS Outline of I/O Modules (for N-IO)” (GS 32P06F10-01EN).

● Installation Restrictions for Node Units

N-IO Node

An N-IO node is connected via an N-ESB bus or optical ESB bus. A node connection via the N-ESB bus needs an N-ESB bus coupler module (S2EN402 or S2EN404).

A node connection via the optical ESB bus needs an ESB bus coupler module (SEC401 or SEC402) and an ESB bus optical repeater module (SNT401 or SNT411).

Safety Node Unit (SNB10D)

A safety node unit is connected via an ESB bus or optical ESB bus. A safety node unit connection via the ESB bus needs an ESB bus coupler module (SEC401 or SEC402). A safety node unit connection via the optical ESB bus needs an ESB bus coupler module (SEC401 or SEC402) and an ESB bus optical repeater module (SNT401 or SNT411).

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

GS 32P06D10-01EN
©Copyright Nov 2015(YK)
12th Edition Apr. 18, 2023(YK)

● Installation Restrictions for Bus Interface Module

N-ESB Bus Coupler Modules (S2EN402 or S2EN404) shall be installed in an odd-numbered slot and the adjacent slot on the right of slots 1 to 8 according to the number of branches.

A pair of ESB Bus Coupler Modules (SEC401 or SEC402) shall be installed in slots 7 and 8.

A pair of Optical ESB Bus Repeater Master Modules (SNT401 or SNT411) shall be installed in an odd-numbered slot and the adjacent slot on the right of slots 1 to 6 according to the number of branches.

For details, refer to the GS of each module.

● Installation Restrictions

Up to eight I/O modules (for FIO) can be installed to a S2SC70☐.

For the I/O module (for FIO) installation limitations and notes, refer to “ProSafe-RS Outline of I/O Modules” (GS 32P06K60-01EN).

● Power Requirements

Specify suffix codes.
Voltage: 100 to 120 V AC, 50 or 60 Hz
Voltage: 220 to 240 V AC, 50 or 60 Hz
Voltage: 24 V DC

● Power Consumption

- S2SC70S-S /S2SC70D-S

100 to 120 V AC model:	200 VA
200 to 240 V AC model:	230 VA
24 V DC model:	5.5 A

- S2SC70S-F/S2SC70D-F

100 to 120 V AC model:	240 VA
200 to 240 V AC model:	290 VA
24 V DC model:	7.0 A

● Battery

- S2CP471
  Part No. : S9450FE
  Battery’s recommended replacement period: Three years under the average ambient temperature of 30 °C or less.
- SCP461
  Part No. : S9185FA
  Battery’s recommended replacement period: Three years under the average ambient temperature of 30 °C or less.

● Weight

S2SC70S-S:	Approx. 7.9 kg
S2SC70S-F:	Approx. 13 kg
S2SC70D-S:	Approx. 8.5 kg
S2SC70D-F:	Approx. 13 kg

● Mounting

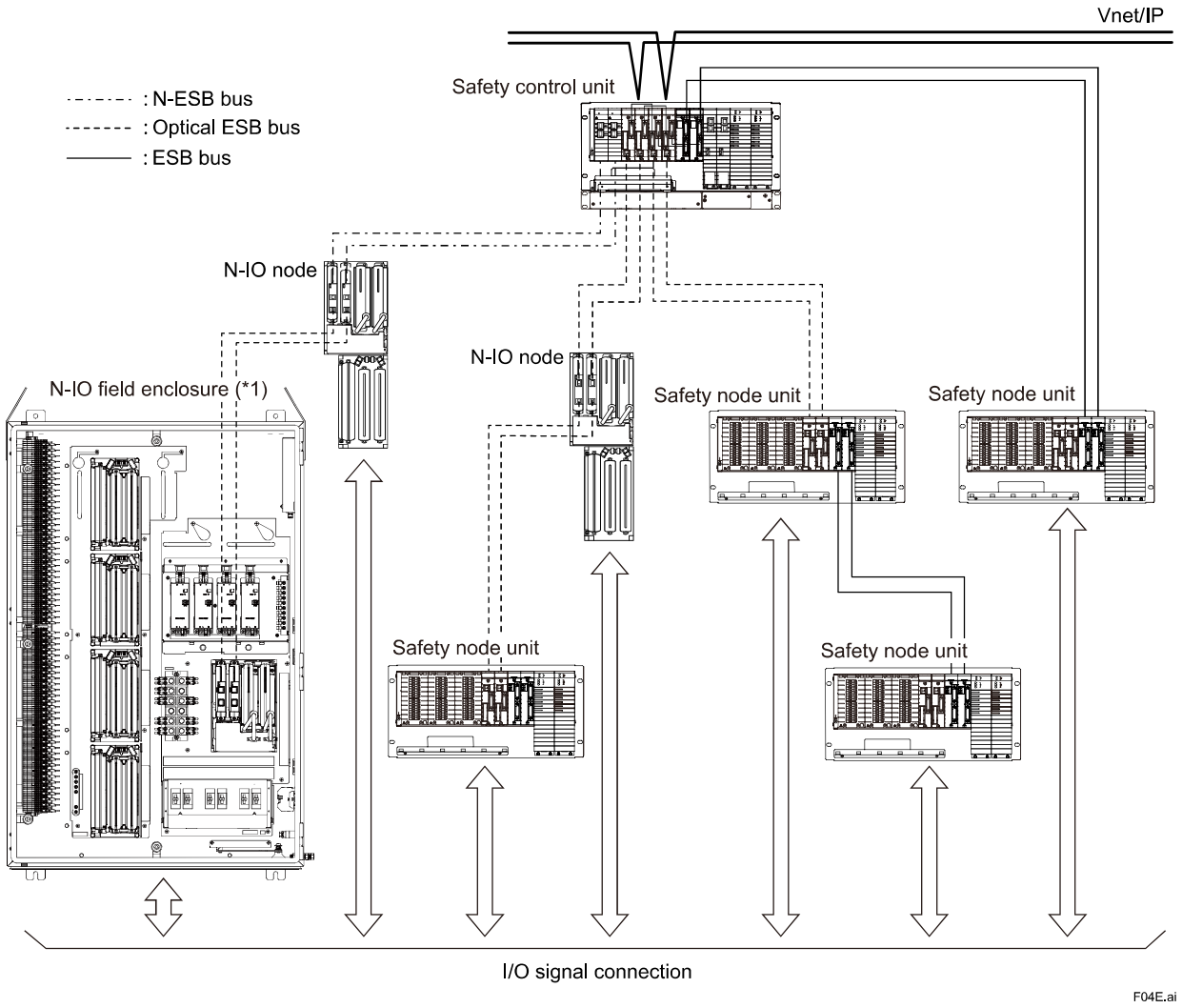
Rack mounting: Rack mount
(S2SC70☐-S, M5x8 screws)
(S2SC70☐-F, M5x12 screws)
Insulation bush (accessory)

● Connection

Power Supply: M4 screw terminal connection
Grounding: M4 screw terminal connection

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

The following shows a configuration example of ProaSafe-RS system of S2SC70□, N-IO node and safety node units.



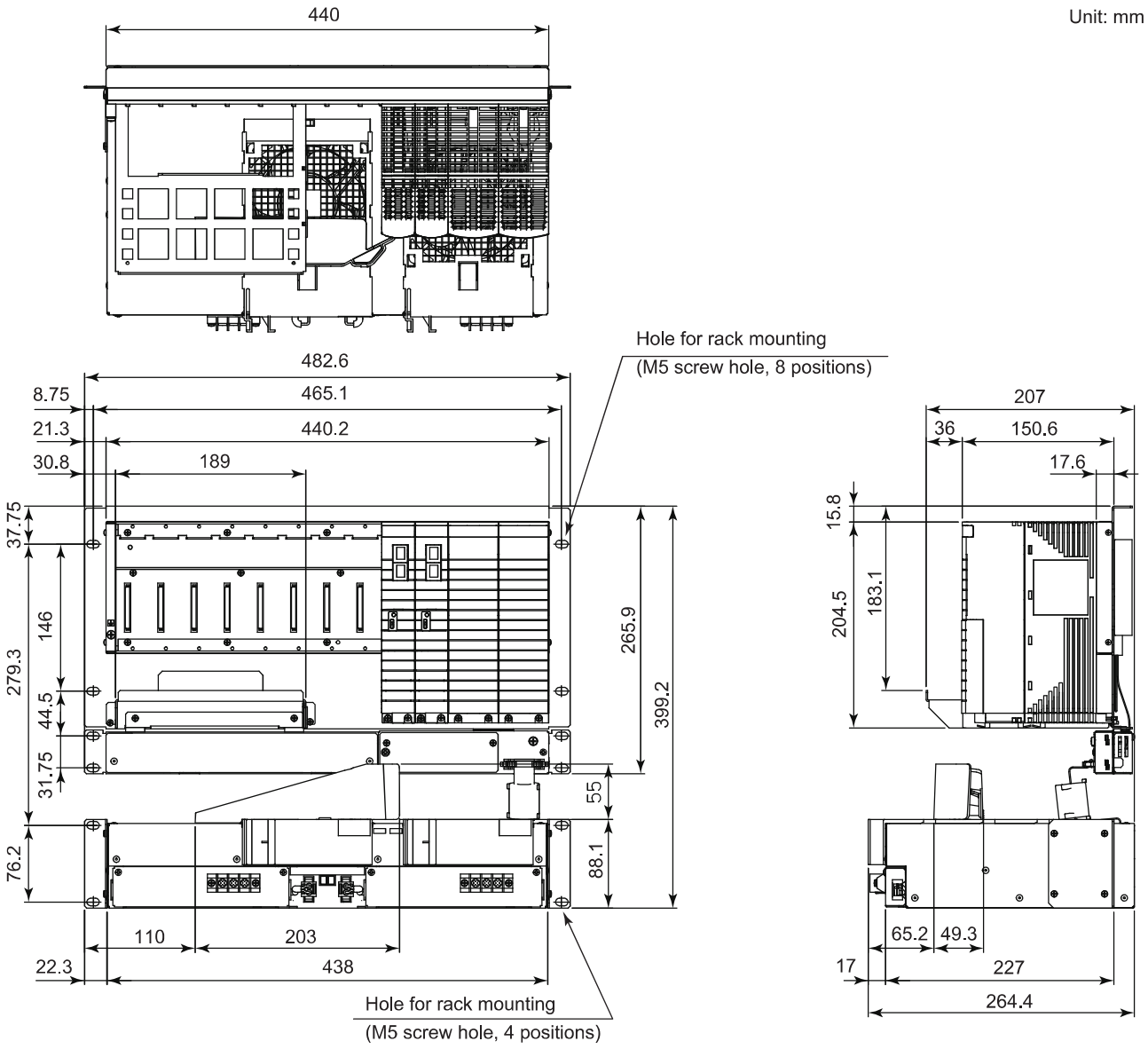
*1: For details, refer to the GS “N-IO field enclosure” (GS 32P06Q10-01EN)

Figure Safety Control Station (SCS) System Configuration

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

■ EXTERNAL DIMENSIONS

Unit: mm



Nominal tolerance:

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

■ SOFTWARE

A software licenses are required for S2SC70S and S2SC70D separately. For details, refer to the GS “Safety Control Function (for S2SC70☐), Safety Control Function for SCS Simulator (for S2SC70☐)” (GS 32P03B30-01EN) and “Project I/O License” (GS 32P03A10-01EN).

■ STANDARD ACCESSORIES

S2SC70S and S2SC70D are delivered with the following standard accessories.

Parts Names	Parts Numbers	Description	Quantity	Remarks
Insulating bush	S9049PM	S2SC70S-S / S2SC70D-S	8	Accessories
		S2SC70S-F / S2SC70D-F	12	

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

■ MODEL AND SUFFIX CODES

Safety Control Unit

		Description
Model	S2SC70S	Safety Control Unit (for N-IO/FIO, Rack Mountable Type) (*1)
Suffix Codes	-S	Standard type (-20 to 40 °C)
	-F	wide range temperature (-20 to 70 °C) type (with Fan unit and ISA Standard G3)
	A	S2CP471, Dual-redundant Vnet/IP, dual-redundant power supply (*2)
	4	SCP461, Dual-redundant Vnet/IP, dual-redundant power supply (*3)
	1	Always 1
	1	100 - 120 V AC power supply
	2	220 - 240 V AC power supply
	4	24 V DC power supply
	0	With no explosion protection
	1	With explosion protection
	1	With ISA Standard G3
	0	Always 0
Option Code	/ATDOC	Explosion Protection Manual (*4)

*1: Supports ProSafe-RS R4.01 or later.
*2: When S2SC70S that is mounted with S2CP471 is used with ProSafe-RS R4.01, R4.02, R4.03, or R4.04, be sure to apply the software patch for supporting S2CP471.
*3: Shipped with SCP461. Also S2CP471 is usable. Replacing from SCP461 to S2CP471 by a user is prohibited. Replacement work must be done by the service engineer authorized by Yokogawa Electric Corporation. See GS 32P06D20-01EN.
*4: Select the option code "/ATDOC" to follow the ATEX Directive and UKEX Regulation when any components are used for explosion protection.

Duplexed Safety Control Unit

		Description
Model	S2SC70D	Duplexed Safety Control Unit (for N-IO/FIO, Rack Mountable Type) (*1)
Suffix Codes	-S	Standard type (-20 to 40 °C)
	-F	wide range temperature (-20 to 70 °C) type (with Fan unit and ISA Standard G3)
	A	S2CP471, Dual-redundant Vnet/IP, dual-redundant power supply (*2)
	4	SCP461, Dual-redundant Vnet/IP, dual-redundant power supply (*3)
	1	Always 1
	1	100 - 120 V AC power supply
	2	220 - 240 V AC power supply
	4	24 V DC power supply
	0	With no explosion protection
	1	With explosion protection
	1	With ISA Standard G3
	0	Always 0
Option Code	/ATDOC	Explosion Protection Manual (*4)

*1: Supports ProSafe-RS R4.01 or later.
*2: When S2SC70D that is mounted with S2CP471 is used with ProSafe-RS R4.01, R4.02, R4.03, or R4.04, be sure to apply the software patch for supporting S2CP471.
*3: Shipped with a pair of SCP461. Also a pair of S2CP471 is usable. Replacing from SCP461 to S2CP471 by a user is prohibited. Replacement work must be done by the service engineer authorized by Yokogawa Electric Corporation. See GS 32P06D20-01EN.
*4: Select the option code "/ATDOC" to follow the ATEX Directive and UKEX Regulation when any components are used for explosion protection.

■ CONFORMITY STANDARDS

Refer to the GS "Standards compliant models" (GS 32P01B60-01EN).

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

■ ORDERING INFORMATION

Specify the model, suffix code(s), and option code(s).
For selecting the right products for explosion protection, please refer to the TI “Explosion Protection” (TI 32S01J30-01E) without fail.

■ TRADEMARK ACKNOWLEDGMENT

The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation
Subject to change without notice.

Attachment 9.16 Safety Node Unit (SNB10D)

GS 32Q06K10-31E

General Specifications

GS 32Q06K10-31E

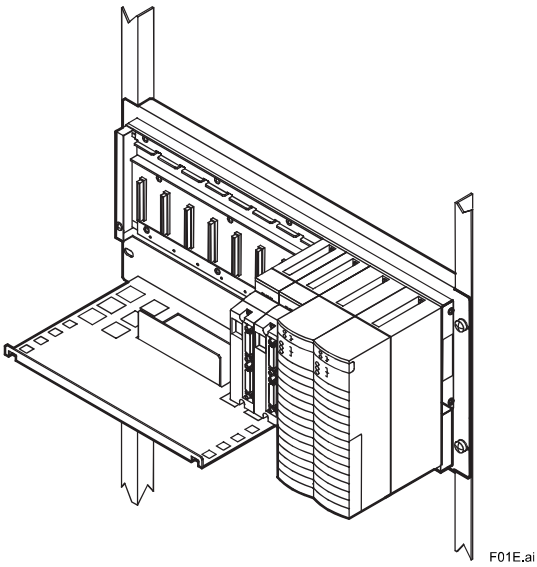
ProSafe-RS
SNB10D
Safety Node Unit (Rack Mountable Type)

■ GENERAL

This GS describes the hardware specifications of the safety node unit (SNB10D). The safety node unit is connected to the safety control unit. The safety node unit has an interface function to transmit analog input signals and contact signals from the field to the safety control unit via an ESB bus. It also has a function to supply power to I/O modules.

The safety node unit is mounted with power supply modules, ESB bus interface modules, optical ESB bus repeater modules, and I/O modules.

For details on the I/O modules, refer to the general specifications (GS 32Q06K30-31E and GS 32Q06K40-31E).


F01E.ai

■ STANDARD SPECIFICATIONS

For the installation environment requirements that are common throughout the system, refer to the general specifications, “ProSafe-RS Safety Instrumented System Overview” (GS 32P01B10-01EN).

- **Safety Integrity Level**

  SIL 3

- **Power Supply Voltage**

  The power supply voltage is specified in the suffix codes.
  Voltage: 100 to 120 V AC and 50/60 Hz frequency
  Voltage: 220 to 240 V AC and 50/60 Hz frequency
  Voltage: 24 V DC

- **Power Consumption**

  100 to 120 V AC specification: 200 VA
  220 to 240 V AC specification: 230 VA
  24 V DC specification: 5.5 A

- **Weight**

  Approx. 5.9 kg

- **Mounting Method**

  Rack mounting: Rack mount with four M5 screws
  Insulation bushes (accessories) are used.

- **Conformity Standards**

  Refer to “Standards Compliant Models” (GS 32P01B60-01EN).

■ CONFIGURATION

- **Module Configuration**

  Power supply module: Supplies power to I/O module (two modules)
  The power supply terminal uses M4 screws.
  ESB bus interface module (SSB401): two modules

■ RESTRICTIONS AND CAUTIONS FOR MOUNTING

Regarding the mounting of I/O modules on the safety node unit, there are restrictions in terms of quantity and slot position. For details, refer to the “■ Node Unit Mounting Restrictions” of “Outline of I/O Modules (for FIO)” (GS 32P06K60-01EN).

YOKOGAWA

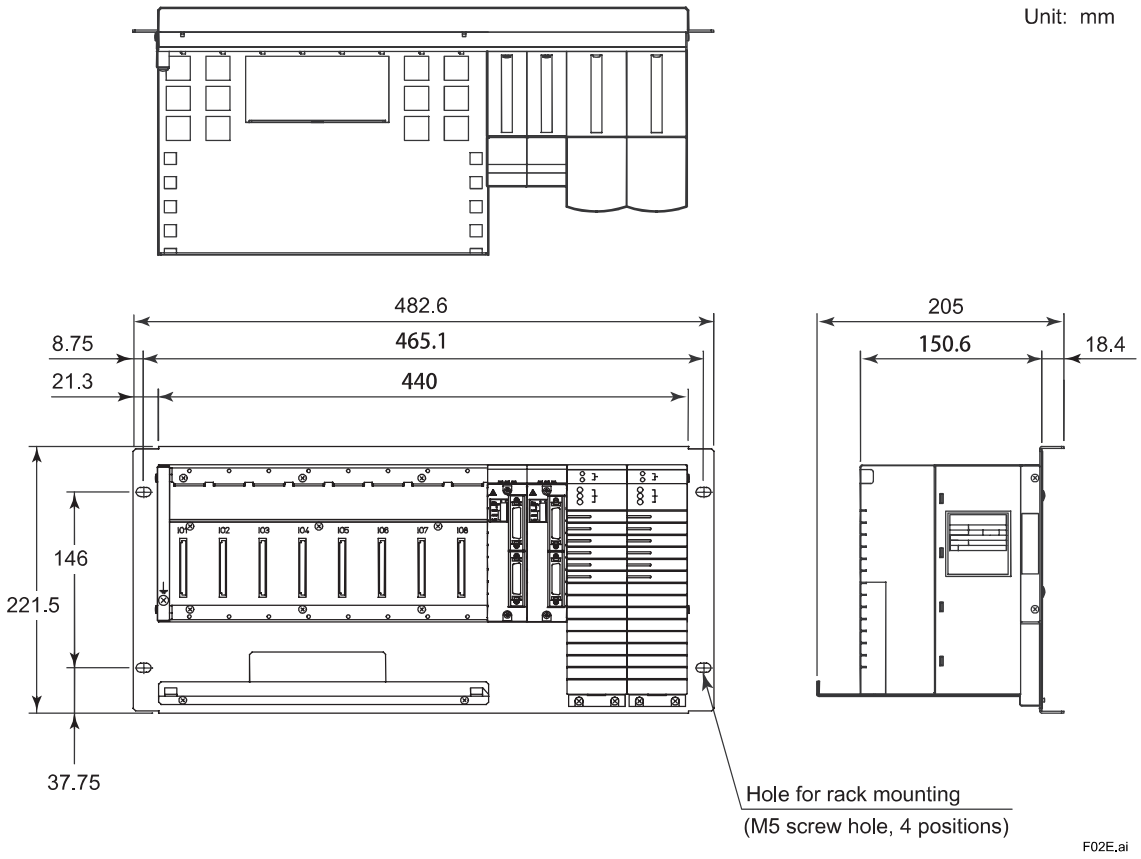
Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

GS 32Q06K10-31E
©Copyright July 2011 (YK)
7th Edition Aug. 15, 2023 (YK)

■ EXTERNAL DIMENSIONS

● SNB10D Safety Node Unit

Unit: mm



Nominal tolerances :

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

■ MODEL AND SUFFIX CODES

Safety node unit

		Description
Model	SNB10D	Safety Node Unit (Rack Mountable Type)
	–4	Dual-redundant power supply (R4.01 or later)
	1	100 to 120 V AC power supply
	2	220 to 240 V AC power supply
	4	24 V DC power supply
	5	ISA Standard G3 and temperature (-20 to 70 ˚C) with no explosion protection
	E	ISA Standard G3 and temperature (-20 to 70 ˚C) with explosion protection
Option Codes	/CU2N	Connector Unit for ESB Bus [Part number: S9342FA]
	/CU2T	Connector Unit with Terminator for ESB Bus [Part number: S9343FA]
	/ATDOC	Explosion Protection Manual

Note: Install the 19-inch rack mountable type devices in a keyed metallic cabinet to conform to the safety standards, the EMC conformity standards and the explosion protection standards.
Note: Please use 1 m or longer YCB301 ESB bus cable to connect SNB10D with a safety control unit .
Note: Select the option code "/ATDOC" to follow the ATEX Directive and UKEX Regulation for use in potentially explosive atmospheres.

Dummy cover

		Description
Model	SDCV01	Dummy cover (for I/O modules)

Note: Be sure to mount a dummy cover on a slot that is not mounted with an I/O module.

■ STANDARD ACCESSORIES

The safety node unit is supplied with the following accessory.

Accessory	Part number	Description	Quantity	Remark
Insulating bushing	S9049PM	SNB10D	4	Accessory

■ ORDERING INFORMATION

Specify the model and suffix codes.
For selecting the right products for explosion protection, please refer to the TI "Explosion Protection" (TI 32S01J30-01E) without fail.

■ TRADEMARK ACKNOWLEDGMENT

The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation
Subject to change without notice.

Attachment 9.17 ESB Bus Coupler Module (SEC401-S1)

GS 32Q06L11-31E

General Specifications

ProSafe-RS
SEC401
ESB Bus Coupler Module

GS 32Q06L11-31E

■ GENERAL

ESB Bus Coupler Module connects safety control units and safety node units via an ESB bus cable.
Two ESB Bus Coupler Modules are mounted on the safety control unit (S2SC70□, SSC60□, or SSC50□).

■ STANDARD SPECIFICATIONS

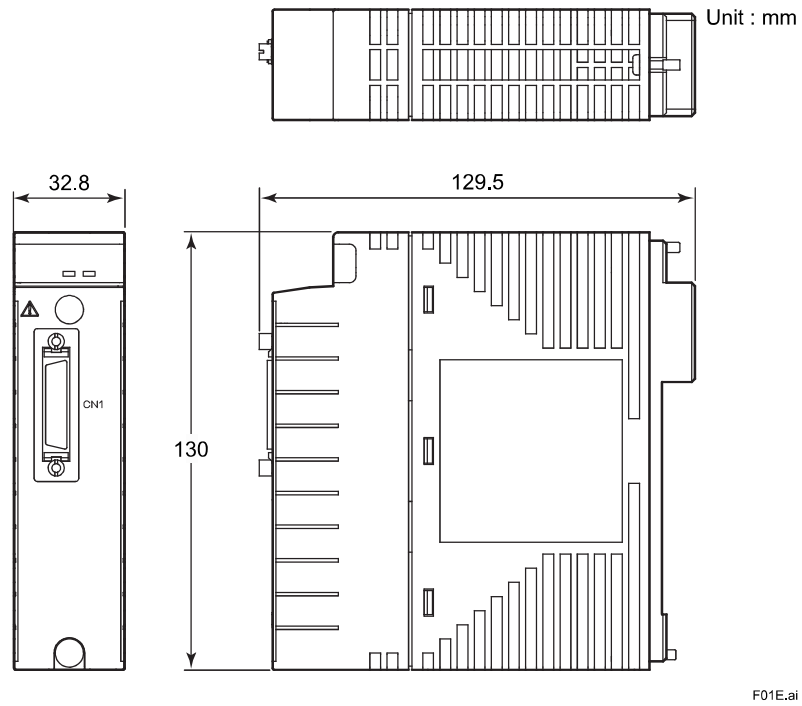
Function:	ESB bus master interface function
Number of connectable units:	9 units maximum (*1)
Transmission speed:	128 Mbps (I/O module data transmission)
Transmission distance:	10 m maximum
Current consumption:	0.5 A
Weight:	Approx. 0.24 kg

The ESB Bus Coupler Module is mounted on the seventh and eighth slots of the safety control unit.

*1: The number of SNB10D and SNT4□□ which can be connected to SEC401 is up to 9.

■ EXTERNAL DIMENSIONS

SEC401 ESB Bus Coupler Module



Nominal Tolerances:
When the reference dimension is over 0.5 mm and equal or less than 120 mm, its nominal tolerance is ± 0.8 mm, while its combination of nominal tolerance is ± 1.5 mm.
When the reference dimension is over 120 mm, its nominal tolerance is in accordance with JEM 1459.

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan
GS 32Q06L11-31E
©Copyright July 2011 (YK)
6th Edition Apr. 25, 2022 (YK)

■ MODEL AND SUFFIX CODES

		Description
Model	SEC401	ESB Bus Coupler Module
Suffix Codes	-5	Standard type with no explosion protection
	-E	Standard type with explosion protection
	1	With ISA Standard G3

■ CONFORMITY STANDARDS

Refer to “Standards Compliant Models” (GS 32P01B60-01EN).

■ ORDERING INFORMATION

Specify the model and suffix code(s).
For selecting the right products for explosion protection, please refer to TI 32S01J30-01E without fail.

■ TRADEMARKS ACKNOWLEDGMENT

The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation
Subject to change without notice.

Attachment 9.18 Analog Input Module (SAI143-H63)

GS 32Q06K30-31E

General Specifications

ProSafe-RS
Analog I/O Modules (for FIO)

GS 32Q06K30-31E

■ GENERAL

This GS describes the hardware specifications of the analog I/O modules that can be mounted on the safety node unit and the safety control unit.

■ STANDARD SPECIFICATIONS

● **Current Input Module**

This module inputs 4 to 20 mA signals from the field.

The SAI143 can be made dual redundant.

Item	Specifications
Model	SAI143 (*1)
Safety Integrity Level	SIL 3
Number of input channels	16 channels, module isolation (*5)
Rated input range	4 to 20 mA
Permissible input range	0 to 25 mA
Input impedance during Power-ON	$250\ \Omega + \frac{\text{Voltage drop in the input protection circuit inside the module}}{\text{Current value}}$ (*6)
Input impedance during Power-OFF	500 kΩ minimum
Rated accuracy	SAI143-S : ±16 µA (Input range 1 to 23 mA) SAI143-H : ±16 µA (Input range 0.05 to 23 mA) (*3) (*4)
Data update frequency	40 ms
Temperature drift	±16 µA/10 °C
Transmitter power supply	16.15 V minimum (at 20 mA) 26.4 V maximum (at 0 mA) (Output current limit: 25 mA)
2/4-wire setting	Individual channel setting Changed by setting pins
Withstand voltage	1.5 kV AC between input signal and system for 1 minute (*2)
Maximum current consumption	5 V system: 320 mA, 24 V system: 550 mA
Weight	Approx. 0.34 kg (For pressure clamp terminal block or MIL cable) Approx. 0.39 kg (With signal cable interface adapter)
External connection	Pressure clamp terminal MIL cable Dedicated signal cable (KS1)
HART communication	Available (SAI143-H)
Transmitter power supply ON/OFF function (*7)	Available in 2-wire setting, for all 16 channels at the same time.

*1: No Zener barriers can be connected to this module. An isolation barrier should be used when an intrinsic safety instrumented system is used.
*2: 500 V AC when dedicated signal cable is used.
*3: ±32 µA (input range under 0.05 mA) (Style code S3 or later)
*4: Rated accuracy of style code S3 or later is ±16 µA (Input range 0.05 to 23 mA).
Rated accuracy of style code S2 or earlier is ±16 µA (Input range 1 to 23 mA).
*5: When SAI143-S□3 or SAI143-H□C is used in the ambient temperature more than 60°C, number of input channels which a user can use is restricted. Refer to “ProSafe-RS Outline of I/O Modules (for FIO)” (GS 32P06K60-01EN).
*6: The maximum voltage drop in the input protection circuit is 0.45 V. The module input impedance varies from 272.5 Ω (20 mA) to 362.5 Ω (4 mA).
*7: This function enables to reset the alarm state of Fire and Gas devices by turning off the transmitter power supplied from this module in 2-wire setting.
Supported by R4.03.00 or later and style code S4 or later.

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

GS 32Q06K30-31E
©Copyright July 2011 (YK)
11th Edition Jan. 22, 2021 (YK)

● Voltage Input Module

This module inputs 1 to 5 V/1 to 10 V signals from the field.
The SAV144 can be made dual redundant.

Item	Specifications
Model	SAV144
Safety Integrity Level	SIL 3
Number of input channels	16 channels, module isolation
Rated input range	1 to 5 V/1 to 10 V
Permissible input range	±30 V
Input impedance during Power-ON	1 MΩ
Input impedance during Power-OFF	100 kΩ
Rated accuracy	1 to 5 V: ±4 mV 1 to 10 V: ±9 mV
Data update frequency	40 ms
Temperature drift	1 to 5 V: ±4 mV/10 °C 1 to 10 V: ±9 mV/10 °C
Withstand voltage	1.5 kV AC between input signal and system for 1 minute (*1)
Maximum current consumption	5 V system: 300 mA 24 V system: 140 mA
Weight	Approx. 0.24 kg (For pressure clamp terminal block or MIL cable) Approx. 0.29 kg (With signal cable interface adapter)
External connection	Pressure clamp terminal MIL cable Dedicated signal cable (KS1)

*1: 500 V AC when dedicated signal cable is used.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

● TC/mV Input Module

This module receives signals from mV and thermocouple (TC). The SAT145 can be made dual redundant.

Item	Specifications
Model	SAT145
Safety Integrity Level	SIL 3
Number of input channels	16 channels, Isolated Channels
Input signal	TC: JIS C 1602, IEC 60584-1 (ITS-90) J: -210 to 1200 °C K: -270 to 1372 °C E: -270 to 1000 °C T: -270 to 400 °C S: -50 to 1767 °C R: -50 to 1767 °C N: -270 to 1300 °C B: 42 to 1820 °C
	mV -100 to 150 mV, -20 to 80 mV, -5 to 25 mV
Switching input signals	TC/mV can be set individually for CH1 to CH16.
Permissible input range	± 5 V
Withstand voltage (*1)	Between input and system: 1500 V AC for 1 minute Between channels: 200 V AC for 1 minute
Input impedance	At least 1 MΩ during Power-ON At least 1 MΩ during Power-OFF
Accuracy	TC ± 40 μV mV ± 40 μV
Allowable total resistance of signal source plus wiring	1000 Ω or less
Effect of allowable signal source resistance (1000 Ω)	± 20 μV (*2)
Reference junction compensation accuracy (*3) (*4)	-20 to 0 °C ± 1.5 °C 0 to 30 °C ± 1.0 °C 30 to 70 °C ± 1.5 °C
Temperature drift	± 40 μV / 10 °C
Data update period	150 ms
Burn-out	Individual channel setting Setting: Burnout upscale/Burnout downscale Detection time: 1.5 s
Ambient temperature (during operation)	-20 to 70 °C
Maximum current consumption	5 V system: 400 mA 24 V system: 200 mA
Weight	Approx. 0.47 kg
External connection	Dedicated signal cable (AKB331)

*1: Use AKB331 of style code S3 or later.
*2: In dual redundant configuration, this effect is ± 40 μV.
*3: Reference junction compensation accuracy is specified on combination with SBT4D.
It varies depending on the temperature environment of SBT4D.
These values indicate Reference junction compensation accuracy against the ambient temperature of terminal board.
*4: This accuracy changes due to the installation condition.
If measured temperature is lower than 0 °C, multiply the above value by the following coefficient (K):

$$K=\frac{\text{Thermoelctromotive force per degree at 0 °C}}{\text{Thermoelectromotive force per degree at measured temperature}}$$

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

● RTD Input Module

This module inputs RTD signals from the field. The SAR145 can be made dual redundant.

Item	Specifications
Model	SAR145
Safety Integrity Level	SIL 3
Number of input channels	16 channels, Isolated Channels
Input signal (*5)	RTD (3 wires) JIS C 1604, IEC 60751 (ITS-90) (*3): Pt100, Pt50, Pt200, Pt500, Pt1000 DIN 43760-1987: Ni100 Minco: Ni120
Withstand voltage	Between input and system: 1500 V AC for 1 minute Between channels: 200 V AC for 1 minute
Accuracy (*1) (*2)	800 Ω range to 400 Ω: ± 160 mΩ to 800 Ω: ± 180 mΩ 4000 Ω range to 2000 Ω: ± 900 mΩ to 4000 Ω: ± 1700 mΩ
Allowable resistance of wiring	150 Ω or less (wiring resistance per wire) (*4)
Measurement current	800 Ω range: 0.5 mA 4000 Ω range: 0.1 mA
Temperature drift	800 Ω range to 400 Ω: ± 150 mΩ / 10 °C to 800 Ω: ± 300 mΩ / 10 °C 4000 Ω range to 2000 Ω: ± 750 mΩ / 10 °C to 4000 Ω: ± 1500 mΩ / 10 °C
Data update period	150 ms
Burn-out	Individual channel setting Setting: Burnout upscale/Burnout downscale Detection time: 1.5 s
Ambient temperature (during operation)	-20 to + 70 °C
Maximum current consumption	5 V system: 500 mA 24 V system: 200 mA
Weight	Approx. 0.47 kg
External connection	Dedicated signal cable (AKB611)

*1: Include the tolerance which is caused by dedicated signal cable AKB611(up to 5 m).
In case of the cable length of AKB611 is more than 5 m, 15 mΩ shall be added to the accuracy per each 5 m.
*2: These values apply for the case when the resistance of field wiring line A and line B are the same value.
If the difference of resistance between line A and line B happens, the different value among them needs to be added.
*3: SAR145 also supports JIS C 1604: 1989 JPt100.
*4: Wiring resistance for signal cable of INnA, INnB and INnC must be identical.
*5: When connecting the RTD modules, use the resisters composed of the passive parts. If an instrument that simulates resistance electronically is connected, it may cause error between reading and actual values. Do not connect voltage signal to the modules.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

● Current Output Module

This module outputs 4 to 20 mA signals to the field.
The SAI533 can be made dual redundant.

Item	Specifications
Model	SAI533
Safety Integrity Level	SIL 3
Number of output channels	8 channels, module isolation (*2)
Rated output range	4 to 20 mA
Maximum range of guaranteed precision	1.25 to 23 mA
Output range	1.25 to 23 mA
Allowable load resistance @ rated range	230 to 600 Ω
Accuracy	±48 μA
Data update frequency	40 ms
Temperature drift	±16 μA/10 °C
Withstand voltage	1.5 kV AC between output signal and system for 1 minute (*1)
Maximum current consumption	5 V system: 320 mA 24 V system: 300 mA
Weight	Approx. 0.26 kg (For pressure clamp terminal block or MIL cable) Approx. 0.33 kg (With signal cable interface adapter)
External connection	Pressure clamp terminal MIL cable Dedicated signal cable (KS1)
HART communication	Available

*1: 500 V AC when dedicated signal cable is used.
*2: When SAI533-H□3 is used in the ambient temperature more than 60°C, number of output channels which a user can use is restricted. Refer to “ProSafe-RS Outline of I/O Modules (for FIO)” (GS 32P06K60-01EN).

■ HART COMMUNICATION

Analog I/O module with HART communication on ProSafe-RS allows Plant Resource Manager (PRM) to manage the HART communication devices connected to input and output modules on SCS. Also, the analog output module allows PRM client to conduct Partial Stroke Test (PST) on HART-supported valve positioner equipped with the PST function.

The HART communication functions on ProSafe-RS are interference-free and have no impact on the safety functions on SCS.

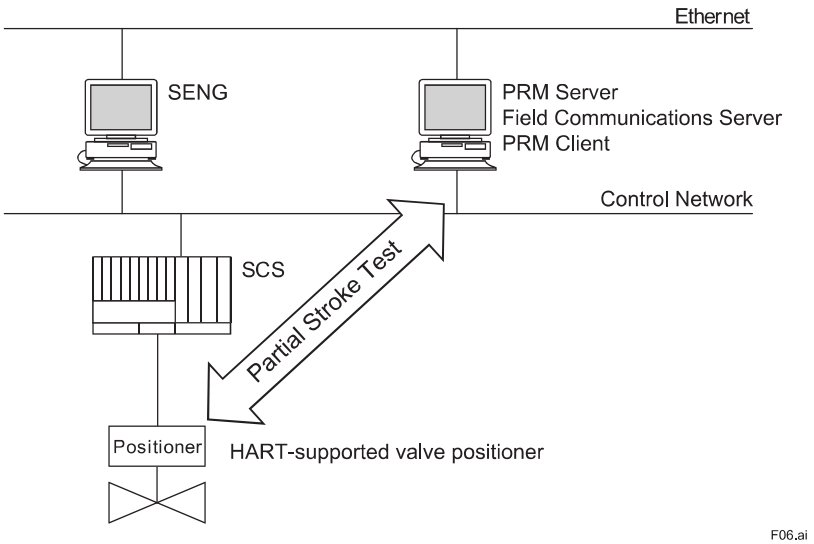


Figure Example of the HART Communication Function System Configuration

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

● Analog I/O Modules for HART Communication Function

The following table shows analog I/O modules for HART communication function available to ProSafe-RS.

Model	Module	Description
SAI143-H	Analog Input module (Current input)	4 to 20 mA, 16 channels, module isolation
SAI533-H	Analog Output module (Current output)	4 to 20 mA, 8 channels, module isolation

One HART device is connectable for each channel. Each channel is equipped with a power supply function to the HART device.

Each module has only one HART modem and is communicable concurrently with only one HART device.

● HART Communication Specifications

Table HART Communication Specifications

Function	Description
Communication mode	Serial half duplex, start-stop synchronization, 1 start/ 8 bit/ odd parity/ 1 stop
Applicable standard	HART Protocol Revision 5.7 (*1)
Transmission speed	1200 ±2 bps
Modulation technique	Binary phase-continuous FSK 1: 1200 Hz ±1 %, 0: 2200 Hz ±1%
Frame length	5 to 267 bytes Contents of max. 267 bytes: Delimiter: 1 Address: 5 Command: 1 Byte count: 1 Data: 255 (includes two bytes of response code) Check byte: 1
Frame detection	3 byte header byte-count carrier (ON/OFF) Preamble: 5 to 20 bytes
Error detection coding	Longitudinal/vertical parity
Response time	Max. 28 characters (256.7 ms)
No response timer	33 characters (305 ms) for primary, 41 characters (380 ms) for secondary
Bus monitor	8 characters (75 ms)
Response window	20 ms

*1: The HART 5, 6, and 7 devices can be connected but applying the HART protocol 5.7 function.

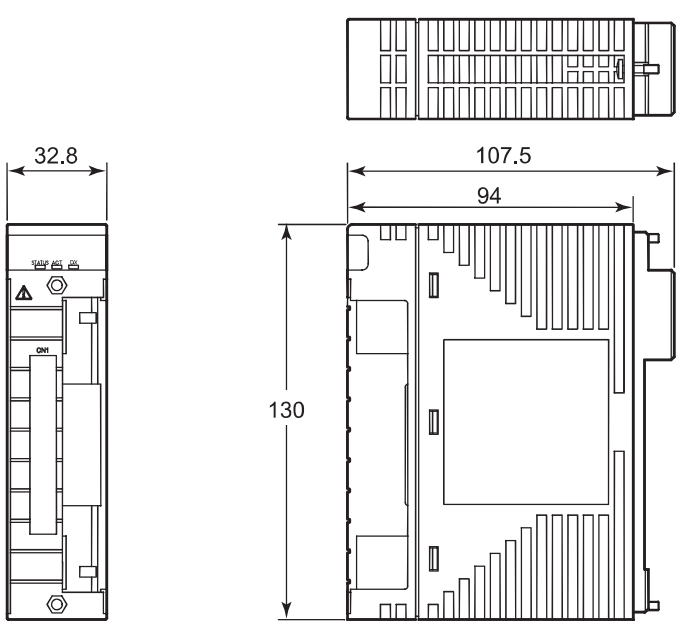
All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

■ EXTERNAL DIMENSIONS

● SAI143, SAV144 and SAI533 Analog Input/Output Modules

For pressure clamp and MIL cable

Unit : mm



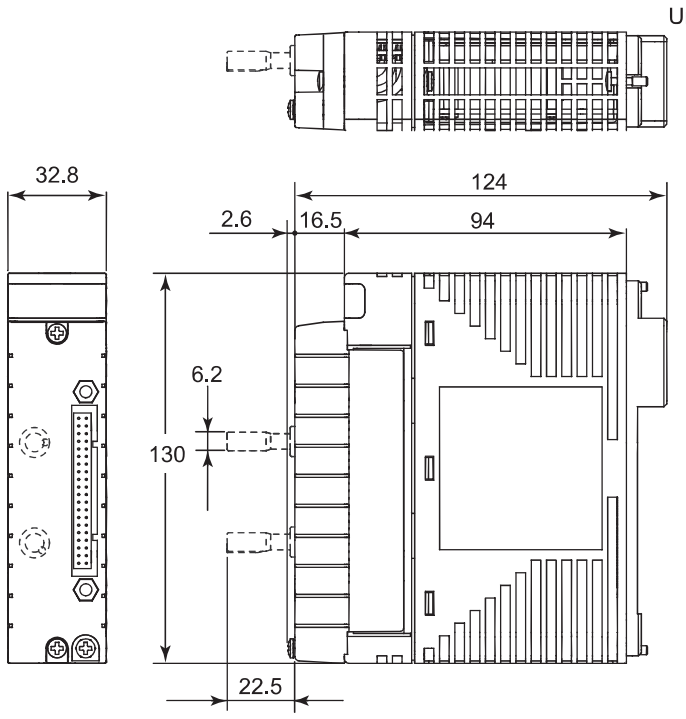
F01E.ai

Nominal tolerance:

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

With signal cable interface adapter

Unit: mm



F02E.ai

Nominal tolerance:

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

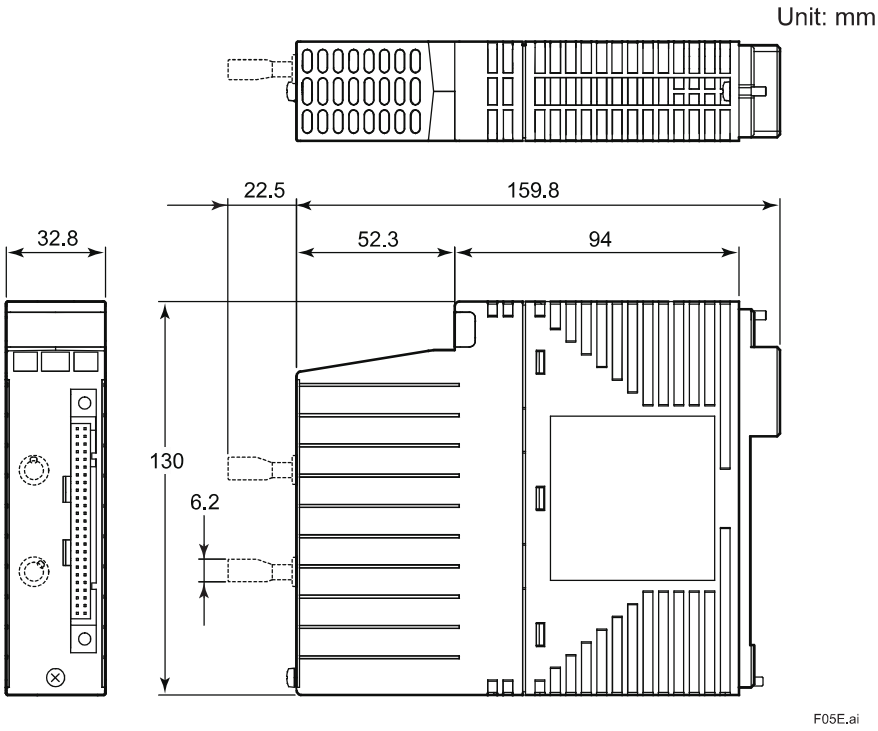
Note: Dash line expresses prevention pin of false insertion. This pin is added if option code /PRP is specified.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

● SAT145, SAR145 Analog Input Modules

With signal cable interface adapter

Unit: mm



Nominal tolerance:

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

Note: Dash line expresses prevention pin of false insertion. This pin is added if option code /PRP is specified.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

■ MODEL AND SUFFIX CODES

		Description
Model	SAI143	Analog Input Module (4 to 20 mA, 16 channels, module isolation)
Suffix Codes	-S	Standard type
	-H	With HART communication [Release: R1.02.00] (*1)
	5	For pressure clamp terminal block or MIL cable with no explosion protection
	6	With signal cable interface adapter and no explosion protection (*2)
	E	For pressure clamp terminal block or MIL cable with explosion protection
	F	With signal cable interface adapter and explosion protection (*2)
	3	With ISA Standard G3 and temperature (-20 to 70 ºC)
	C	With ISA Standard G3 and high-density installation (-20 to 70 ºC) (*5)
Option Codes	/A4S00	With pressure clamp terminal block for analog [Model: STA4S-00]
	/A4S10	With pressure clamp terminal block for analog (with surge absorber) [Model: STA4S-10]
	/A4D00	With dual-redundant pressure clamp terminal block for analog (*3) [Model: STA4D-00]
	/A4D10	With dual-redundant pressure clamp terminal block for analog (with surge absorber) (*3) [Part name: STA4D-10]
	/PRP	With prevention pin of false insertion (*4)
	/CCC01	With connector cover for MIL cable (for flat ribbon cable) [Model: SCCC01]

*1: For dual-redundant pressure clamp terminal block, please do not use STA4D-□0 S1.
*2: When selecting SAI143-□6□ or -□F□, you can not choose the option code of pressure clamp terminal block and MIL cable connector.
*3: When using this module in a dual-redundant configuration, order an additional module with the same specifications but without option codes.
*4: When SAI143-□6□ or -□F□ is selected, you can choose the option code for prevention pin of false insertion. A mechanism to prevent wrong type I/O module insertion is supported with signal cable. The signal cable used with this I/O module must have option code /SAI143.
*5: Suffix code for “With ISA Standard G3 and high-density installation” is available in case of SAI143-H□C. This is not available in case of SAI143-S.

		Description
Model	SAV144	Analog input module (1 to 5 V/1 to 10 V, 16 channels, module isolation)
Suffix Codes	-S	Standard type
	5	For pressure clamp terminal block or MIL cable with no explosion protection
	6	With signal cable interface adapter and no explosion protection (*1)
	E	For pressure clamp terminal block or MIL cable with explosion protection
	F	With signal cable interface adapter and explosion protection (*1)
	3	With ISA Standard G3 and temperature (-20 to 70 ºC)
Option Codes	/A4S00	With pressure clamp terminal block for analog [Model: STA4S-00]
	/A4S10	With pressure clamp terminal block for analog (with surge absorber) [Model: STA4S-10]
	/A4D00	With dual-redundant pressure clamp terminal block for analog (*2) [Model: STA4D-00]
	/A4D10	With dual-redundant pressure clamp terminal block for analog (with surge absorber) (*2) [Part name: STA4D-10]
	/PRP	With prevention pin of false insertion (*3)
	/CCC01	With connector cover for MIL cable (for flat ribbon cable) [Model: SCCC01]

*1: When selecting SAV144-S63 or -SF3, you can not choose the option code of pressure clamp terminal block and MIL cable connector.
*2: When using this module in a dual-redundant configuration, order an additional module with the same specifications but without option codes.
*3: When SAV144-S63 or -SF3 is selected, you can choose the option code for prevention pin of false insertion. A mechanism to prevent wrong type I/O module insertion is supported with signal cable. The signal cable used with this I/O module must have option code /SAV144.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

		Description
Model	SAT145	TC/mV Input Module (16 channels, Isolated Channels)
Suffix Codes	-S	Standard type
	6	With signal cable interface adapter and no explosion protection
	F	With signal cable interface adapter and explosion protection
	3	With ISA Standard G3 and temperature (-20 to 70 ºC)
Option Codes	/PRP	With prevention pin of false insertion (*1)

*1: The signal cable used with this I/O module must have option code /SAT14.

		Description
Model	SAR145	RTD Input Module (16 channels, Isolated Channels)
Suffix Codes	-S	Standard type
	6	With signal cable interface adapter and no explosion protection
	F	With signal cable interface adapter and explosion protection
	3	With ISA Standard G3 and temperature (-20 to 70 ºC)
Option Codes	/PRP	With prevention pin of false insertion (*1)

*1: The signal cable used with this I/O module must have option code /SAR14.

		Description
Model	SAI533	Analog Output Module (4 to 20 mA, 8 channels, module isolation)
Suffix Codes	-H	With HART communication
	5	For pressure clamp terminal block or MIL cable with no explosion protection
	6	With signal cable interface adapter and no explosion protection (*1)
	E	For pressure clamp terminal block or MIL cable with explosion protection
	F	With signal cable interface adapter and explosion protection (*1)
	3	With ISA Standard G3 and temperature (-20 to 70 ºC)
Option Codes	/A4S00	With pressure clamp terminal block for analog [Model: STA4S-00]
	/A4S10	With pressure clamp terminal block for analog (with surge absorber) [Model: STA4S-10]
	/A4D00	With dual-redundant pressure clamp terminal block for analog (*2) [Model: STA4D-00]
	/A4D10	With dual-redundant pressure clamp terminal block for analog (with surge absorber) (*2) [Model: STA4D-10]
	/PRP	With prevention pin of false insertion (*3)
	/CCC01	With connector cover for MIL cable (for flat ribbon cable) [Model: SCCC01]

*1: When selecting SAI533-H63 or -HF3, you can not choose the option code of pressure clamp terminal block and MIL cable connector.
*2: When using this module in a dual-redundant configuration, order an additional module with the same specifications but without option codes.
*3: When SAI533-H63 or -HF3 is selected, you can choose the option code for prevention pin of false insertion.
A mechanism to prevent wrong type I/O module insertion is supported with signal cable. The signal cable used with this I/O module must have option code /SAI533.

■ CONFORMITY STANDARDS

Refer to “Standards Compliant Models” (GS 32P01B60-01EN).

■ ORDERING INFORMATION

Specify the model and suffix codes.

For selecting the right products for explosion protection, please refer to TI 32S01J30-01E without fail.

■ TRADEMARK ACKNOWLEDGMENT

The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation
Subject to change without notice.

Attachment 9.19 Digital Input Module (SDV144-S63)
GS 32Q06K40-31E

General Specifications

ProSafe-RS
Digital I/O Modules (for FIO)

GS 32Q06K40-31E

■ GENERAL

This GS provides the hardware specifications of the digital I/O modules that can be installed in the Safety Node Unit and Safety Control Units.

■ STANDARD SPECIFICATIONS

● Input Module

Input modules accept contact signals from the field. SDV144 can be made dual-redundant.

Item	Specifications
Safety Integrity Level	SIL 3
Model	SDV144
Number of inputs	16 channels, module isolation (*3)
Input signal	No-voltage contact ON: 1 kΩ maximum OFF: 100 kΩ minimum
Input current	6 mA ± 20 % (External power supply, 24 V DC at 0 Ω input)
Contact rating	24 V DC +20 % / -10 % (*4), 10 mA or greater
External power supply	24 V DC +20 % / -10 % (*3) (*4) Current capacity: 200 mA
Instantaneous maximum permissible input voltage	30.0 V DC
Input response time	40 ms maximum
Withstand voltage (*1) (*2)	2 kV AC between input signal and system for 1 minute, 16-input line collectively connected (*5)
Current consumption	290 mA maximum (5 V DC) 140 mA maximum (24 V DC)
Weight	Approx. 0.36 kg (For pressure clamp terminal block or MIL cable) Approx. 0.41 kg (With signal cable interface adapter)
External connection	Pressure clamp terminal MIL cable Dedicated signal cable (AKB331)

*1: These voltages show the case using the field power supply floating. When the field power supply is grounded, the system (functional) ground is connected to the field ground, which is not isolated. For the higher noise immunity, floating the field power supply is recommended.
*2: When the withstanding voltage of the field power supply between the secondary side and the ground is lower than the value shown in the table above, these voltages are adopted as the withstanding voltage of the field power supply.
*3: Number of input channels which a user can use and external power supply are restricted in case of SDV144-S□C. Refer to “ProSafe-RS Outline of I/O Modules (for FIO)” (GS 32P06K60-01EN).
*4: The contact rating and the external power supply of SDV144 style code S1, S2 and S3 are 24 V DC ± 5 %.
*5: When connecting SDV144 and SED4D terminal board using the dedicated signal cable, the withstand voltage is 500 V AC (between input signal lines and system). If MIL connector cables are used, the withstand voltage depends on their cable’s electrical specifications.

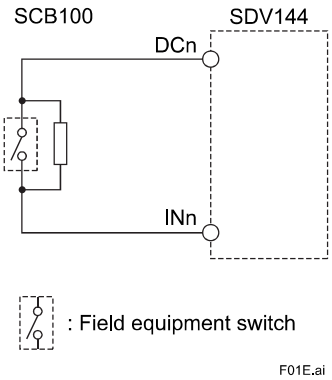
Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan
GS 32Q06K40-31E
©Copyright July 2011 (YK)
12th Edition Dec. 3, 2021 (YK)

If SDV144 field wiring diagnostic functions are used, the following wiring check adapter should be installed for individual channels in the vicinity of the field equipment:

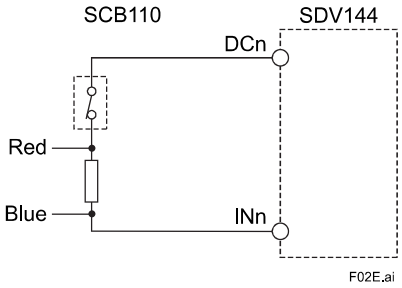
- SCB100 (for defective open circuit detection while accepting off signals) (*1)
- SCB110 (for defective short-circuit detection while accepting on signals) (*2)

*1: Input signals are normally off while in normal operation.
*2: Input signals are normally on while in normal operation.

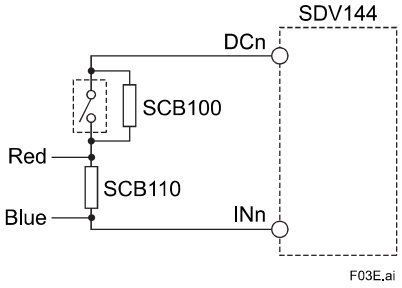
When the input signals are normally off while in normal operation, connect the SCB100 in parallel with the contact output of the field equipment as given below.



When the input signals are normally on while in normal operation, connect the SCB110 in series with the contact output of the field equipment (take care about the polarity taking note of the polarity).



When checking for both defective short and open circuits, connect the SCB100 and SCB110 in parallel and series with the contact outputs of the field equipment respectively, as given below.



All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

● Output Module

Output modules output on/off status signals to field equipment.

The output modules can be made dual-redundant respectively. They incorporate field wiring diagnostic functions, so they require no wiring check adapter.

Item	Specifications
Model	SDV531
Safety Integrity Level	SIL 3
Number of outputs	8 channels, module isolation (*3)
Output voltage	24 V DC
Output voltage drop	1 V maximum
External power supply rating	24 V DC, 5 A minimum
External power supply	24 V DC +20 %/–10 % (*4) Current capacity: 5 A
Maximum leak current at output off status	1.6 mA
Output format	Current source
Maximum load current	0.6 A/output line (4.8 A in total output lines) (*3) (*5)
Minimum load current	35 mA
Load resistance range	40 to 685 Ω (*6)
Output response time	30 ms maximum
Withstand voltage (*1) (*2)	2 kV AC between output signal lines and system for 1 minute, 8-point input lines collectively connected (negative lines) (*7)
Current consumption	280 mA maximum (5 V DC) 140 mA maximum (24 V DC)
Weight	Approx. 0.28 kg (For pressure clamp terminal block or MIL cable) Approx. 0.34 kg (With dedicated signal cable interface adapter)
External connection	Pressure clamp terminal MIL cable Dedicated signal cable (AKB331, AKB651 (*8))

*1: These voltages show the case using the field power supply floating. When the field power supply is grounded, the system (functional) ground is connected to the field ground, which is not isolated. For the higher noise immunity, floating the field power supply is recommended.

*2: When the withstanding voltage of the field power supply between the secondary side and the ground is lower than the value shown in the table above, these voltages are adopted as the withstanding voltage of the field power supply.

*3: Number of output channels which a user can use and maximum load current are restricted in case of SDV531-L□C. Refer to “ProSafe-RS Outline of I/O Modules (for FIO)” (GS 32P06K60-01EN).

*4: External power supply of SDV531-S style code S1 and S2 is 24 V DC ± 5%.

*5: Do not exceed this value, including the case of inrush/variation of the load current.

*6: Resistance value of the load for both ON and OFF state, including the field wiring resistance.

*7: When connecting SDV531 and SED4D terminal board using AKB331 dedicated signal cable, the withstand voltage is 500 V AC (between output signal lines and system). If MIL connector cables are used, the withstand voltage depends on their cable’s electrical specifications.

*8: AKB651 can be used for connection with SDV531-L only.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

Item	Specifications
Model	SDV541
Safety Integrity Level	SIL 3
Number of outputs	16 channels, module isolation (*3)
Output voltage	24 V DC
Output voltage drop	1 V maximum
External power supply rating	24 V DC, 3.4 A minimum
External power supply	24 V DC + 20 % / -10 % (*4) Current capacity: 3.4 A
Maximum leak current at output off status	1.6 mA
Output format	Current source
Maximum load current	0.2 A/output line (3.2 A in total output line) (*3) (*5)
Minimum load current	35 mA
Load resistance range	120 to 685 Ω (*6)
Output response time	30 ms maximum
Withstand voltage (*1) (*2)	2 kV AC between output signal lines and system for 1 minute, 16-point input lines collectively connected (negative lines) (*7)
Current consumption	300 mA maximum (5 V DC) 150 mA maximum (24 V DC)
Weight	Approx. 0.29 kg (For pressure clamp terminal block or MIL cable) Approx. 0.31 kg (With dedicated signal cable interface adapter)
External connection	Pressure clamp terminal MIL cable Dedicated signal cable (AKB331, AKB651)

*1: These voltages show the case using the field power supply floating. When the field power supply is grounded, the system (functional) ground is connected to the field ground, which is not isolated. For the higher noise immunity, floating the field power supply is recommended.
*2: When the withstanding voltage of the field power supply between the secondary side and the ground is lower than the value shown in the table above, these voltages are adopted as the withstanding voltage of the field power supply.
*3: Number of output channels which a user can use and maximum load current are restricted in case of SDV541-S□C. Refer to “ProSafe-RS Outline of I/O Modules (for FIO)” (GS 32P06K60-01EN).
*4: External power supply of SDV541 style code S1 is 24 V DC ± 5%.
*5: Do not exceed this value, including the case of inrush/variation of the load current.
*6: Resistance value of the load for both ON and OFF state, including the field wiring resistance.
*7: When connecting SDV541 and SED4D terminal board using AKB331 dedicated signal cable, the withstand voltage is 500 V AC (between output signal lines and system). If MIL connector cables are used, the withstand voltage depends on their cable’s electrical specifications.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

Item	Specifications
Model	SDV521
Safety Integrity Level	SIL 3
Number of outputs	4 channels, module isolation (*4)
Output voltage	24 V DC
Output voltage drop	1 V maximum
External power supply rating	24 V DC, 10 A minimum
External power supply	24 V DC +20 %/–10 % Current capacity: 8.2 A (*5)
Maximum leak current at output off status	1.6 mA
Output format	Current source
Maximum load current	2 A/output line (8 A in total output lines) (*4)
Minimum load current	100 mA
Load resistance range	12 to 240 Ω (*6)
Maximum lamp load (*1)	1 A/output line
Output response time	30 ms maximum
Withstand voltage (*2) (*3)	2 kV AC between output signal lines and system for 1 minute, 4-point input lines collectively connected (negative lines)
Current consumption	280 mA maximum (5 V DC) 140 mA maximum (24 V DC)
Weight	Approx. 0.36 kg
External connection	Dedicated signal cable (AKB651)

*1: This is the maximum rated load current in the case of a filament lamp. The inrush current of a filament lamp is acceptable up to 10 times of this value.
*2: These voltages show the case using the field power supply floating. When the field power supply is grounded, the system (functional) ground is connected to the field ground, which is not isolated. For the higher noise immunity, floating the field power supply is recommended.
*3: When the withstanding voltage of the field power supply between the secondary side and the ground is lower than the value shown in the table above, these voltages are adopted as the withstanding voltage of the field power supply.
*4: Number of output channels which a user can use and maximum load current are restricted in case of SDV521-S□C. Refer to “ProSafe-RS Outline of I/O Modules (for FIO)” (GS 32P06K60-01EN).
*5: Required capacity when all the channels are loaded with rated load. Please use external source with the capacity most appropriate for load to be applied.
(When it is probable to get inrush load, use power source with the inrush current added.)
*6: Resistance value of the load for both ON and OFF state, including the field wiring resistance.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

Item	Specifications
Model	SDV526 (*1) (*2) (*3) (*4)
Safety Integrity Level	SIL 3
Number of outputs	4 channels, module isolation
Output voltage	100 to 120 V AC
Output voltage drop	1.3 V AC + 0.01 V AC/m minimum 2.5 V AC + 0.04 V AC/m maximum (*5)
External power supply rating	100 to 120 V AC (*6)
External power supply	100 to 120 V AC +10 %/–15 %
Maximum leak current at output off status	2 mA
Output format	Current source (common N side)
Maximum load current	0.5 A/output line
Minimum load current	0.1 A/output line
Load resistance range	5 kΩ (*7)
Output response time	60 ms
Withstand voltage	1500 V AC between output signal lines and system for 1 minute
Current consumption	500 mA maximum (5 V DC) 50 mA maximum (24 V DC)
Weight	Approx. 0.36 kg
External connection	Dedicated signal cable (AKB652) (*8)

*1: SDV526 is not capable to of detecting the following faults.
- short circuit between channels
- output short circuit while output signals are off

*2: When the application logic is designed to continuously change the output state to ON and OFF alternately, at least one of the following conditions must be met.
- every ON state must be kept 1,000ms or longer
- every OFF state must be kept 1,000ms or longer

*3: Acceptable reverse electromotive voltage for output channel is 450 V, 1 ms (The reverse electromotive voltage is caused by the connection with inductive load such as relays or solenoid valves.)

*4: Supported by R2.02.00 or later.

*5: It depends on the length of AKB652.

*6: In order to comply with safety standards, the external power supply connected to the terminal board is supplied from a secondary circuit. The secondary circuit is insulated by a transformer and the primary circuit is MAINS CIRCUITS of overvoltage category II up to 300 V. The insulation must be REINFORCED INSULATION or DOUBLE INSULATION.

*7: Resistance value of the load for OFF state, including the field wiring resistance.

*8: For dual-redundant configuration, two AKB652 cables with the same length should be used.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

Item	Specifications
Model	SDV53A (*3)
Safety Integrity Level	SIL 3
Number of outputs	8 channels, module isolation
Output voltage	48 V DC
Output voltage drop	1 V maximum
External power supply rating	48 V DC, 5 A minimum
External power supply	48 V DC +20 %/–10 % Current capacity: 5 A (*4)
Maximum leak current at output off status	3.2 mA
Output format	Current source
Maximum load current	0.6 A/output line (4.8 A in total output lines) (*5)
Minimum load current	100 mA
Load resistance range	80 to 480 Ω (*6)
Output response time	36 ms maximum
Withstand voltage (*1) (*2)	2 kV AC between output signal lines and system for 1 minute, 8-point input lines collectively connected (negative lines)
Current consumption	290 mA maximum (5 V DC) 150 mA maximum (24 V DC)
Weight	Approx. 0.46 kg
External connection	Dedicated signal cable (AKB331, AKB651)

*1: These voltages show the case using the field power supply floating. When the field power supply is grounded, the system (functional) ground is connected to the field ground, which is not isolated. For the higher noise immunity, floating the field power supply is recommended.
*2: When the withstanding voltage of the field power supply between the secondary side and the ground is lower than the value shown in the table above, these voltages are adopted as the withstanding voltage of the field power supply.
*3: R2.03 or later
*4: Required capacity when all the channels are loaded with rated load. Please use external source with the capacity most appropriate for load to be applied.
(When it is probable to get inrush load, use power source with the inrush current added.)
*5: 0.3 A for filament lamp under the specified conditions. When rush current is over 3 A, the module cannot be connected.
*6: Resistance value of the load for both ON and OFF state, including the field wiring resistance.

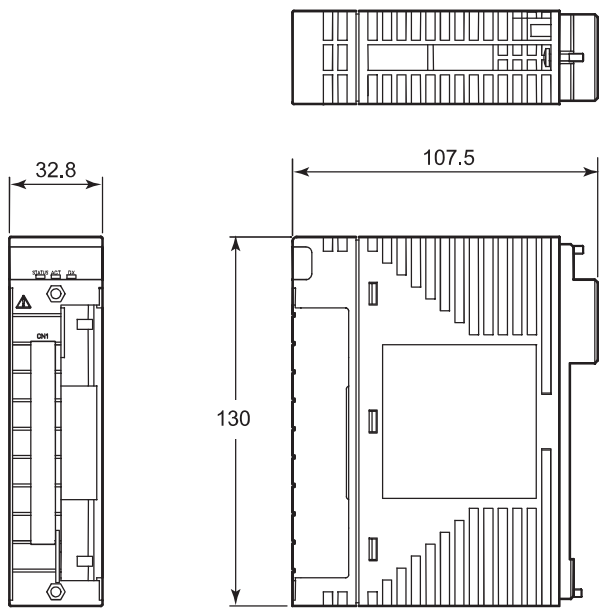
All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

■ EXTERNAL DIMENSIONS

● SDV144 Digital Input Module

For pressure clamp and MIL cable

Unit: mm

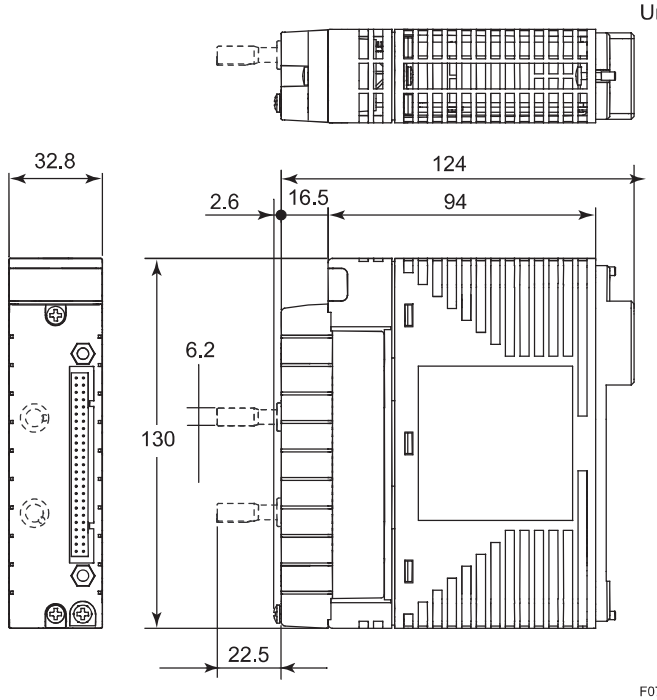


Nominal tolerances :

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominaltolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

With signal cable interface adapter

Unit: mm



Nominal tolerances :

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominaltolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

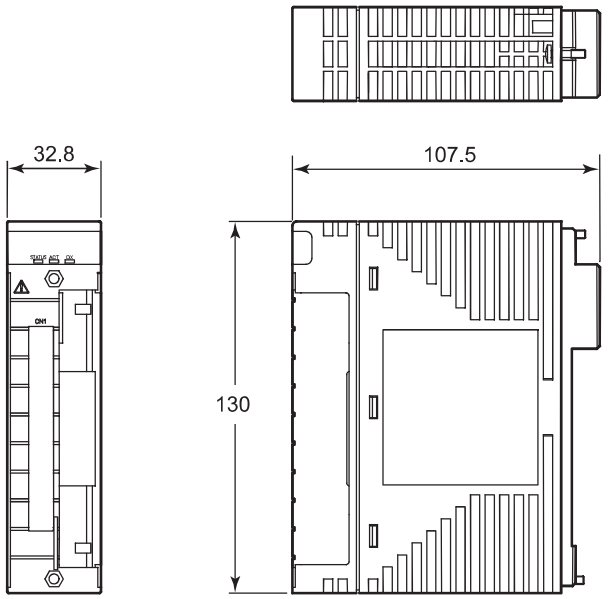
Note: Dash line expresses prevention pin of false insertion. This pin is added if option code /PRP is specified

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

● SDV531 and SDV541 Digital Output Module

For pressure clamp and MIL cable

Unit: mm

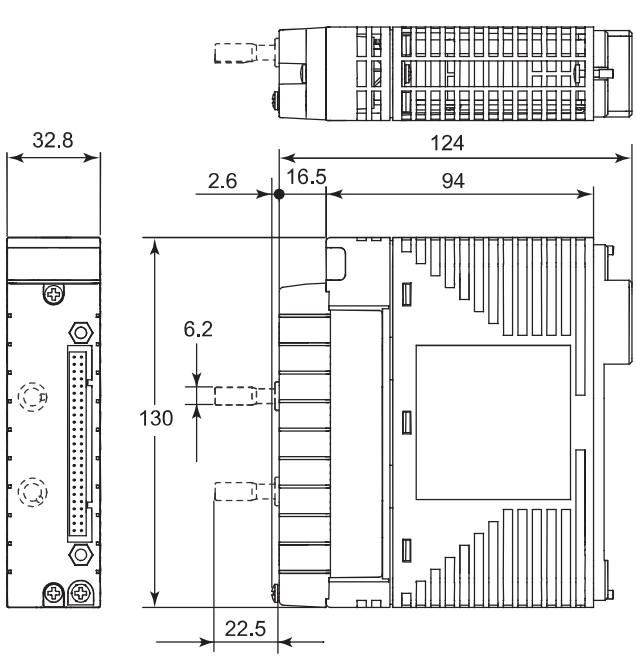


Nominal tolerances :

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominaltolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

With signal cable interface adapter

Unit: mm



Nominal tolerances :

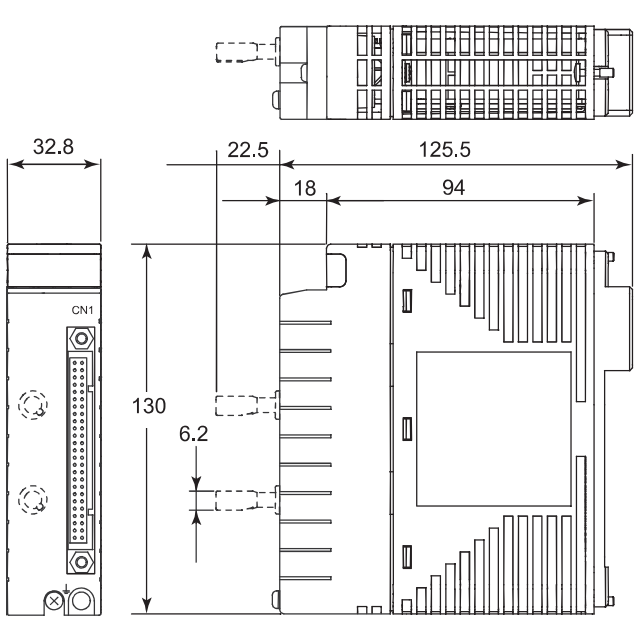
Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominaltolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

Note: Dash line expresses prevention pin of false insertion. This pin is added if option code /PRP is specified

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

● SDV521 Digital Output Module

Unit: mm



F09E.ai

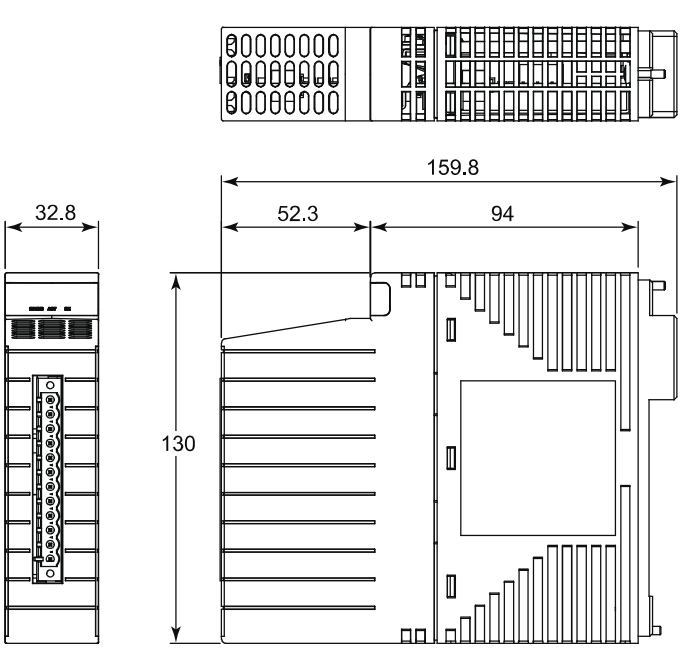
Nominal tolerances :

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominaltolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

Note: Dash line expresses prevention pin of false insertion.

● SDV526 Digital Output Module

Unit: mm



F10E.ai

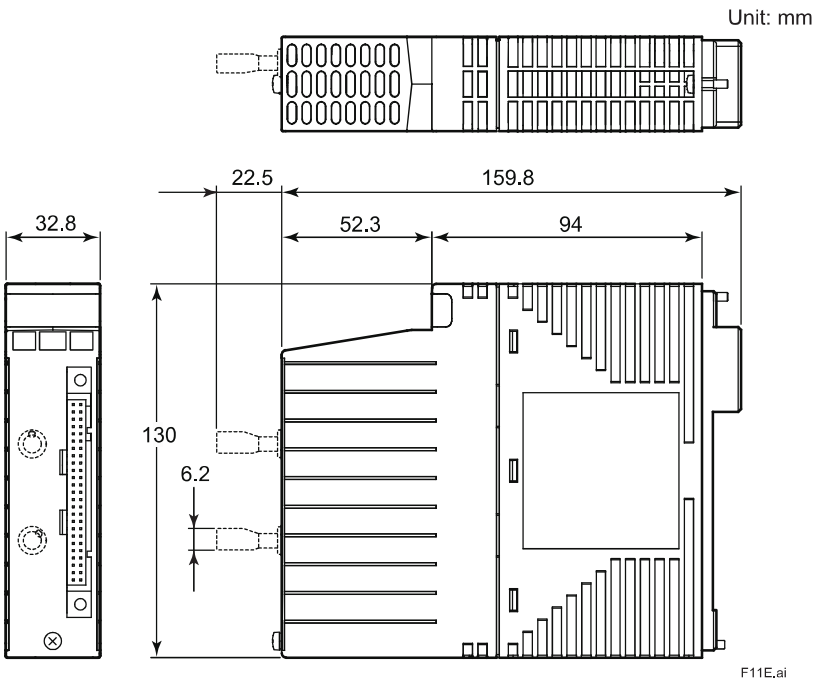
Nominal tolerances :

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominaltolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

● SDV53A Digital Output Module

Unit: mm

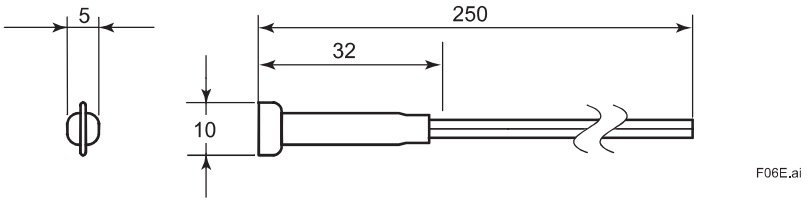


Nominal tolerances :

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominaltolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

● SCB100 and SCB110 Wiring Check Adapter

Unit: mm



Nominal tolerances :

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominaltolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

■ MODEL AND SUFFIX CODES

Digital Input Module

		Description
Model	SDV144	Digital Input Module (24 V DC, 16 channels, module isolation)
Suffix Codes	-S	Standard type
	5	For pressure clamp terminal block or MIL cable with no explosion protection
	6	With signal cable interface adapter and no explosion protection (*1)
	E	For pressure clamp terminal block or MIL cable with explosion protection
	F	With signal cable interface adapter and explosion protection (*1)
	3	With ISA Standard G3 and temperature (-20 to 70 °C)
	C	With ISA Standard G3 and high-density installation (-20 to 70 °C)
Option Codes	/B4S00	With pressure clamp terminal block for digital input (without surge absorber) [Model: STB4S-00]
	/B4S10	With pressure clamp terminal block for digital input (with surge absorber) [Model: STB4S-10]
	/B4D00	With dual-redundant pressure clamp terminal block for digital input (without surge absorber) (*2) [Model: STB4D-00]
	/B4D10	With dual-redundant pressure clamp terminal block for digital input (with surge absorber) (*2) [Model: STB4D-10]
	/PRP	With prevention pin of false insertion (*3)
	/CCC01	With connector cover for MIL cable (for flat ribbon cable) [Model: SCCC01]
	/CCC02	With connector cover for MIL cable (for discrete wire) [Model: SCCC02]

*1: When SDV144-S6☐ or -SF☐ is selected, you cannot choose the option code for a pressure clamp terminal block and MIL cable connector.
*2: When this module is used in dual-redundant configuration, order an additional module with the same specification but without option codes.
*3: When SDV144-S6☐ or -SF☐ is selected, you can choose the option code for prevention pin of false insertion.
A mechanism to prevent wrong type I/O module insertion is supported with signal cable. The signal cable used with this I/O module must have option code /SDV144.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

Digital Output Module

		Description
Model	SDV531	Digital output module (24 V DC, 8 channels, module isolation)
Suffix Codes	-L	Long distance type
	-S	Standard type
	5	For pressure clamp terminal block or MIL cable with no explosion protection
	6	With signal cable interface adapter and no explosion protection (*1)
	E	For pressure clamp terminal block or MIL cable with explosion protection
	F	With signal cable interface adapter and explosion protection (*1)
	3	With ISA Standard G3 and temperature (-20 to 70 °C)
	C	With ISA Standard G3 and high-density installation (-20 to 70 ºC) (*4)
Option Codes	/B4S00	With pressure clamp terminal block for digital output (without surge absorber) [Model: STB4S-00]
	/B4S10	With pressure clamp terminal block for digital output (with surge absorber) [Model: STB4S-10]
	/B4D00	With dual-redundant pressure clamp terminal block for digital output (without surge absorber) (*2) [Model: STB4D-00]
	/B4D10	With dual-redundant pressure clamp terminal block for digital output (with surge absorber) (*2) [Model: STB4D-10]
	/PRP	With prevention pin of false insertion (*3)
	/CCC01	With connector cover for MIL cable (for flat ribbon cable) [Model: SCCC01]
	/CCC02	With connector cover for MIL cable (for discrete wire) [Model: SCCC02]

*1: When SDV531-□6□ or -□F□ is selected, you cannot choose the option code for a pressure clamp terminal block and MIL cable connector.
*2: When this module is used in dual-redundant configuration, order an additional module with the same specification but without option codes.
*3: When SDV531-□6□ or -□F□ is selected, you can choose the option code for prevention pin of false insertion.
A mechanism to prevent wrong type I/O module insertion is supported with signal cable. The signal cable used with this I/O module must have option code /SDV531, /SDV53L or /DV53L.
*4: Suffix Code for “With ISA Standard G3 and high-density installation” is available in case of SDV531-L□C. This is not available in case of SDV531-S.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

		Description
Model	SDV541	Digital Output Module (24 V DC, 16 channels, module isolation)
Suffix Codes	-S	Standard type
	5	For pressure clamp terminal block or MIL cable with no explosion protection
	6	With signal cable interface adapter and no explosion protection (*1)
	E	For pressure clamp terminal block or MIL cable with explosion protection
	F	With signal cable interface adapter and explosion protection (*1)
	3	With ISA Standard G3 and temperature (-20 to 70 °C)
	C	With ISA Standard G3 and high-density installation (-20 to 70 °C)
Option Codes	/B4S00	With pressure clamp terminal block for digital output (without surge absorber) [Model: STB4S-00]
	/B4S10	With pressure clamp terminal block for digital output (with surge absorber) [Model: STB4S-10]
	/B4D00	With dual-redundant pressure clamp terminal block for digital output (without surge absorber) (*2) [Model: STB4D-00]
	/B4D10	With dual-redundant pressure clamp terminal block for digital output (with surge absorber) (*2) [Model: STB4D-10]
	/PRP	With prevention pin of false insertion (*3)
	/CCC01	With connector cover for MIL cable (for flat ribbon cable) [Model: SCCC01]
	/CCC02	With connector cover for MIL cable (for discrete wire cable) [Model: SCCC02]

*1: When SDV541-S6☐ or -SF☐ is selected, you cannot choose the option code for a pressure clamp terminal block and MIL cable connector.
*2: When this module is used in dual-redundant configuration, order an additional module with the same specification but without option codes.
*3: When SDV541-S6☐ or -SF☐ is selected, you can choose the option code for prevention pin of false insertion. A mechanism to prevent wrong type I/O module insertion is supported with signal cable. The signal cable used with this I/O module must have option code /SDV541 or /DV541.

		Description
Model	SDV521	Digital Output Module (24 V DC/2 A, 4 channels, module isolation)
Suffix Codes	-S	Standard type
	6	With signal cable interface adapter and no explosion protection
	F	With signal cable interface adapter and explosion protection
	3	With ISA Standard G3 and temperature (-20 to 70 °C)
	C	With ISA Standard G3 and high-density installation (-20 to 70 °C)
Option Codes	/PRP	With prevention pin of false insertion (*1)

*1: The signal cable used with this I/O module must have option code /SDV521.

		Description
Model	SDV526	Digital Output Module (4 channels, module isolation)
Suffix Codes	-S	Standard type (*1)
	3	With signal cable interface adapter
	3	With ISA Standard G3 and temperature (-20 to 70 °C)

*1: with prevention of false insertion

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

		Description
Model	SDV53A	Digital Output Module (48 V DC, 8 channels, module isolation)
Suffix Codes	-S	Standard type
	6	With signal cable interface adapter and no explosion protection
	F	With signal cable interface adapter and explosion protection
	3	With ISA Standard G3 and temperature (-20 to 70 °C)
Option Codes	/PRP	With prevention pin of false insertion (*1)

*1: The signal cable used with this I/O module must have option code /SDV53A or /DV53A.

Wiring Check Adapter

		Description
Model	SCB100	Wiring Check Adapter for Digital Input (for defective open circuit detection while accepting off signals with ISA Standard G3) (*1)
Suffix Codes	-S	Standard type
	0	Always 0

*1: Eight pcs/set

		Description
Model	SCB110	Wiring Check Adapter for Digital Input (for defective short-circuited detection while accepting on signals with ISA Standard G3) (*1)
Suffix Codes	-S	Standard type
	0	Always 0

*1: Eight pcs/set

■ STANDARD ACCESSORIES

The fuse for SDV144 style code S1, S2 and S3 are replaceable.

SDV144 style code S4 contains the fuse but it is not replaceable.

Accessory	Part number	Quantity	Remark
Fuse	A1327EF	1	Mounted

■ CONFORMITY STANDARDS

Refer to “Standards Compliant Models” (GS 32P01B60-01EN).

■ ORDERING INFORMATION

Specify the model and suffix codes when ordering.

For selecting the right products for explosion protection, please refer to the TI “Explosion Protection” (TI 32S01J30-01E) without fail.

■ TRADEMARK ACKNOWLEDGMENT

The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation
Subject to change without notice.

Attachment 9.20 Enhanced Serial Bus Cable (YCB301)
GS 32Q06M10-31E

General Specifications

ProSafe-RS/ProSafe-RS Lite
Cables

GS 32Q06M10-31E

GENERAL

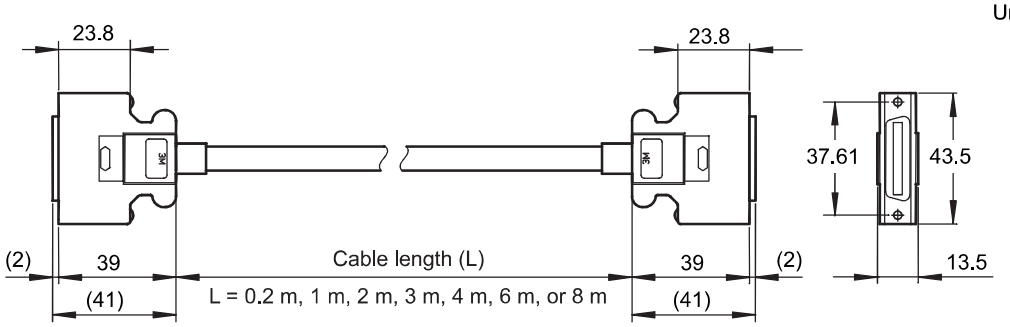
This GS provides the specifications for cables used in the ProSafe-RS/ProSafe-RS Lite system.

DIMENSIONS

Cables

YCB301 ESB Bus Cable

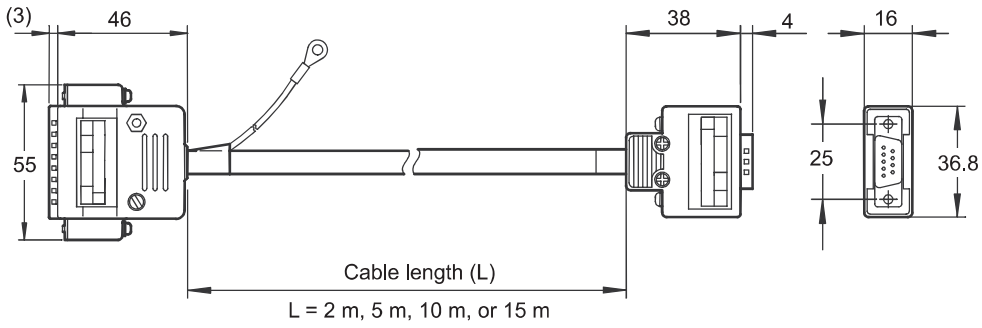
Unit: mm



F01E.ai

AKB131, AKB132, AKB135, AKB136 RS-232C Cables for Start-Stop Asynchronous Communications (for ALR111 Communications Module)

Unit: mm



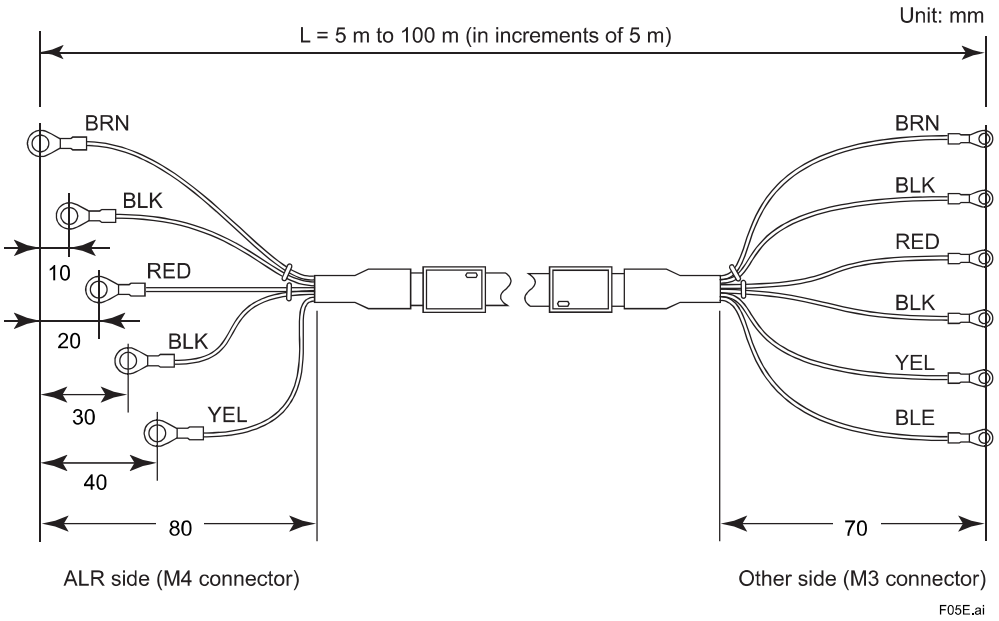
F04E.ai

Note: An FG connection wire is attached to the other side connector of the AKB131 and AKB132 cables.

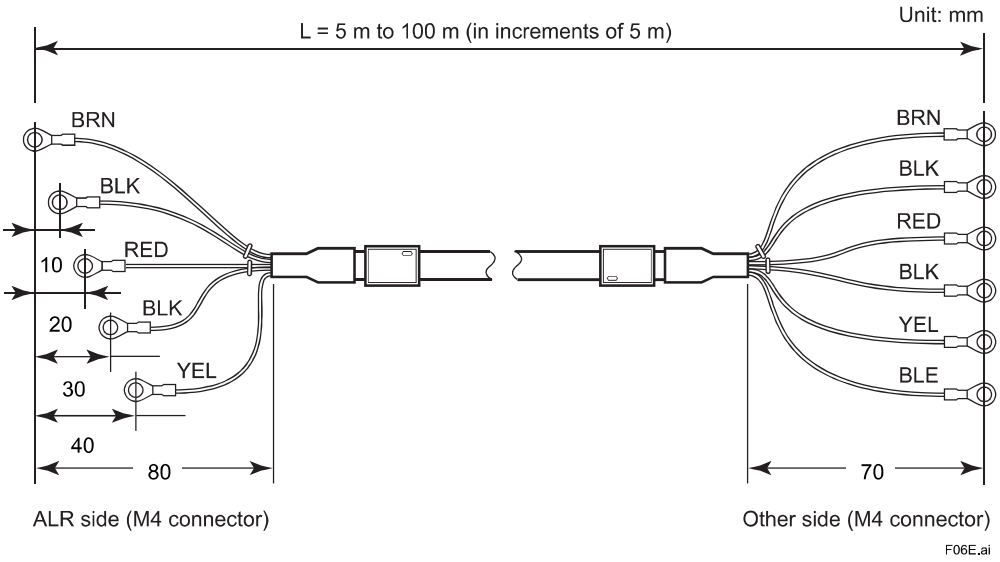
Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

GS 32Q06M10-31E
©Copyright July 2011 (YK)
8th Edition Jan. 22, 2021 (YK)

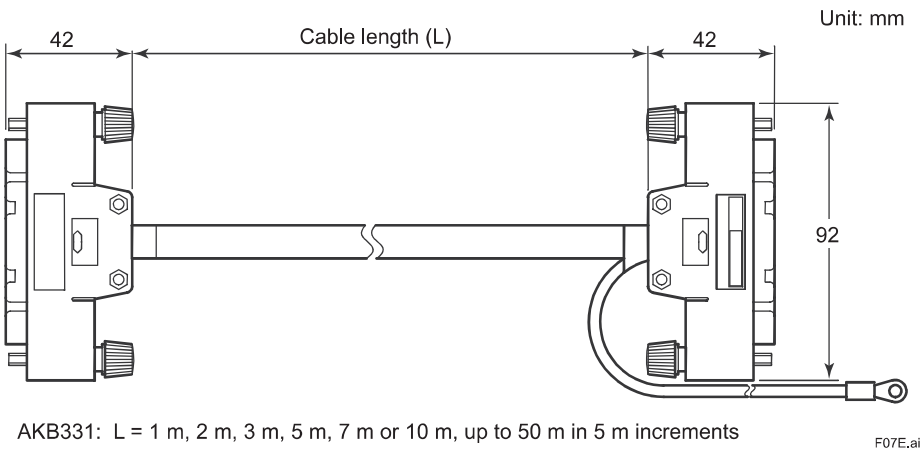
AKB161 RS-422/RS-485 Cable (for ALR121 Communications Module)



AKB162 RS-422/RS-485 Cable (for ALR121 Communications Module)



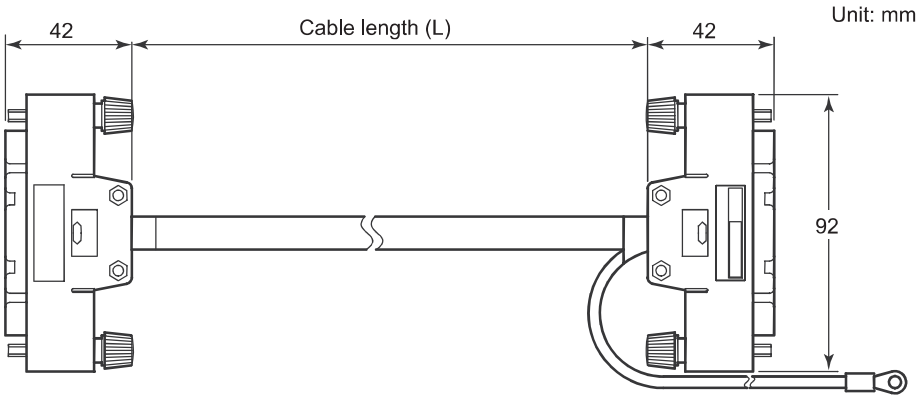
AKB331 Signal Cable (50-50 pins)



All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

AKB611 Signal Cable (50-50 pins)

Unit: mm

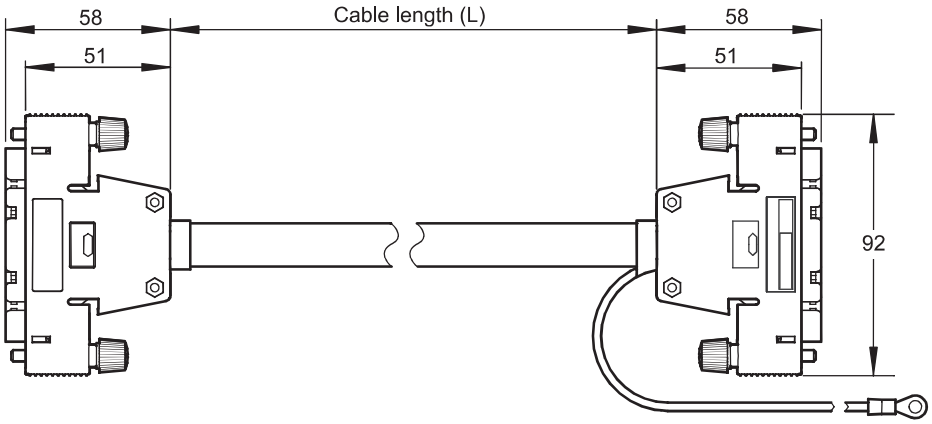


AKB6111: L = 2 m, 5 m

F17E.ai

AKB651 Signal Cable (50-50 pins)

Unit: mm

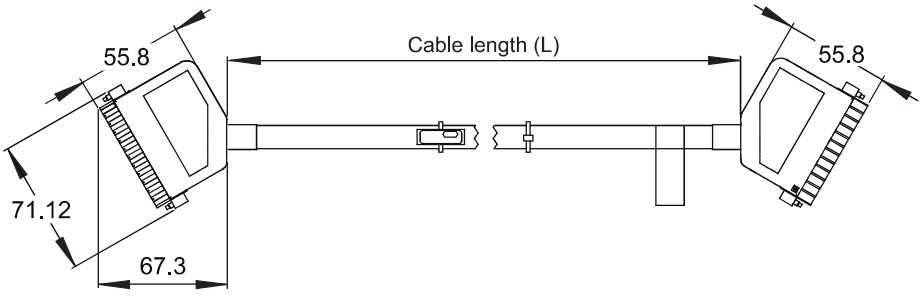


AKB651: L = 1 m, 2 m, 3 m, 5 m, 7 m or 10 m, up to 30 m in 5 m increments

F15E.ai

AKB652 Signal Cable (12 pins)

Unit: mm

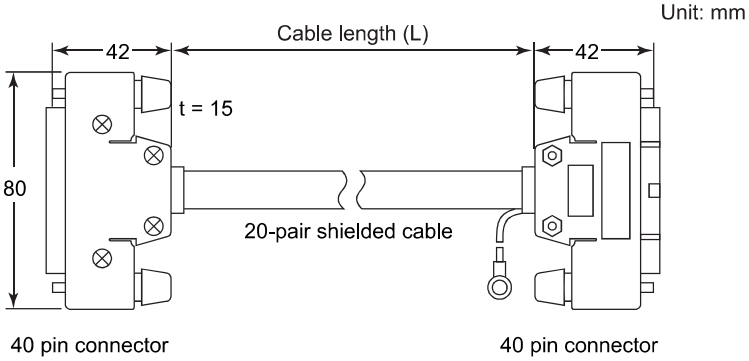


AKB652: L = 1 m, 2 m, 3 m, 5 m, 7 m, 10 m, 15 m, 20 m, 25 m, or 30 m

F16E.ai

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

KS1 Cable (40-40 pins)



KS1: L = 1 m, 2 m, 3 m, 5 m, 7 m or 10 m, up to 50 m in 5 m increments

F08E.ai

Nominal tolerances:

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominaltolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

Nominal tolerances of cable length:

When the reference dimension is less than or equal to 3000 mm, its nominal tolerance is +5%, -0%.
When the reference dimension is over 3000 mm, its nominal tolerance is +3% or +1m(whichever is smaller), -0%.

■ MODEL AND SUFFIX CODES

EBS Bus Cable

		Description
Model	YCB301	ESB Bus Cable
Suffix Codes	-C020	Length: 20 cm
	-C100	Length: 1 m
	-C200	Length: 2 m
	-C300	Length: 3 m
	-C400	Length: 4 m
	-C600	Length: 6 m
	-C800	Length: 8 m

RS-232C Modem Cable (for connection between ALR111 and modem)

		Description
Model	AKB131	For connecting RS circuit isolated devices; RS-232C modem cable for start-stop asynchronous communications (9-25 pins)(for connection between ALR111 and modem)
Suffix Codes	-M002	Length: 2 m
	-M005	Length: 5 m
	-M010	Length: 10 m
	-M015	Length: 15 m

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

RS-232C Null Modem Cable (for connection between ALR111 and RS-232C device)

		Description
Model	AKB132	RS-232C null modem cable for start-stop asynchronous communications (9-25 pins)(for connection between ALR111 and RS-232C device)
Suffix Codes	-M002	Length: 2 m
	-M005	Length: 5 m
	-M010	Length: 10 m
	-M015	Length: 15 m

RS-232C Modem Cable (for connection between ALR111 and modem)

		Description
Model	AKB135	RS-232C modem cable for start-stop asynchronous communications (9-25 pins)(for connection between ALR111 and modem)
Suffix Codes	-M002	Length: 2 m
	-M005	Length: 5 m
	-M010	Length: 10 m
	-M015	Length: 15 m

RS-232C Null Modem Cable (for connection between ALR111 and RS-232C device)

		Description
Model	AKB136	RS-232C null modem cable for start-stop asynchronous communications (9-25 pins)(for connection between ALR111 and RS-232C device)
Suffix Codes	-M002	Length: 2 m
	-M005	Length: 5 m
	-M010	Length: 10 m
	-M015	Length: 15 m

Signal Cables

		Description
Model	AKB161	RS-422/RS-485 Cable Used between ALM side (M4 terminal) and other side (M3 terminal)
Suffix Code	-M □□□	Enter multiples of 5 in the □□□ (the cable comes in 5-m increments). Maximum length: 100 m (suffix code: -M100)

		Description
Model	AKB162	RS-422/RS-485 Cable Used between ALR side (M4 terminal) and other side (M4 terminal)
Suffix Code	-M □□□	Enter multiples of 5 in the □□□ (the cable comes in 5-m increments). Maximum length: 100 m (suffix code: -M100)

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

		Description
Model	AKB331	Signal Cable (50-50 pins) (for connection between SDV144/L1DV144, SDV531/L1DV531, SDV53A/L1DV53A, SDV541/L1DV541, or SAT145/L1AT145 and Terminal Board)
Suffix Codes	-M001	Length: 1 m
	-M002	Length: 2 m
	-M003	Length: 3 m
	-M005	Length: 5 m
	-M007	Length: 7 m
	-M010	Length: 10 m
	-M015	Length: 15 m
	-M020	Length: 20 m
	-M025	Length: 25 m
	-M030	Length: 30 m
	-M035	Length: 35 m
	-M040	Length: 40 m
	-M045	Length: 45 m
	-M050	Length: 50 m
Option Codes	/SDV144	Special cable for SDV144/L1DV144
	/SDV53L	Special cable for SDV531-L/L1DV531
	/SDV53A	Special cable for SDV53A/L1DV53A
	/SDV541	Special cable for SDV541/L1DV541
	/SAT14	Special cable for SAT145/L1AT145

Note: When connecting AKB331 with SDV531, SDV53A or SDV541, check if the cable length of AKB331 is proper or not, referring to “Terminal Board is connected” of “■ LIMITATIONS ON DIGITAL OUTPUT MODULE CONNECTIONS” in “ProSafe-RS Outline of I/O Modules (for FIO)” (GS 32P06K60-01EN).

Note: When connecting AKB331 with L1DV531, L1DV53A or L1DV541, check if the cable length of AKB331 is proper or not, referring to “Terminal Board is connected” of “■ LIMITATIONS ON DIGITAL OUTPUT MODULE CONNECTIONS” in “ProSafe-RS Lite Outline of I/O Modules” (GS 32P56K60-01EN).

Note: A mechanism to prevent wrong type I/O module insertion is supported. When you select option code /SDV144, /SDV53L, /SDV53A, /SDV541 and /SAT14, the same model I/O module with /PRP prevention pin of false insertion option can be used. For example, AKB331-M003/SDV144 can be used only with SDV144 or L1DV144 that have /PRP prevention pin of false insertion option.

		Description
Model	AKB611	Signal Cable (for connections between SAR145/L1AR145 and Terminal Board)
Suffix Code	-M002	Cable length : 2 m
	-M005	Cable length : 5 m
Option Code	/SAR14	Special cable for SAR145 /L1AR145

Note: A mechanism to prevent wrong type I/O module insertion is supported.
When you select option code /SAR14, SAR145 or L1AR145 with /PRP prevention pin of false insertion option can be used.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

		Description
Model	AKB651	Signal Cable (50-50 pins) (for connections between SDV521/L1DV521,SDV531/L1DV531, SDV53A/L1DV53A, or SDV541/L1DV541 and Terminal Board)
Suffix Codes	-M001	Length: 1 m
	-M002	Length: 2 m
	-M003	Length: 3 m
	-M005	Length: 5 m
	-M007	Length: 7 m
	-M010	Length: 10 m
	-M015	Length: 15 m
	-M020	Length: 20 m
	-M025	Length: 25m
	-M030	Length: 30 m
Option Codes	/SDV521	Special cable for SDV521/L1DV521
	/DV53L	Special cable for SDV531-L/L1DV531
	/DV53A	Special cable for SDV53A/L1DV53A
	/DV541	Special cable for SDV541/L1DV541

Note: When connecting AKB651 with SDV521, SDV531-L, SDV53A or SDV541, check if the cable length of AKB651 is proper or not, referring to “Terminal Board is connected” of “■ LIMITATIONS ON DIGITAL OUTPUT MODULE CONNECTIONS” in “ProSafe-RS Outline of I/O Modules (for FIO)” (GS 32P06K60-01EN).
Note: When connecting AKB651 with L1DV521, L1DV531, L1DV53A or L1DV541, check if the cable length of AKB651 is proper or not, referring to “Terminal Board is connected” of “■ LIMITATIONS ON DIGITAL OUTPUT MODULE CONNECTIONS”in “ProSafe-RS Lite Outline of I/O Modules ” (GS 32P56K60-01EN).
Note: A mechanism to prevent wrong type I/O module insertion is supported. When you select option code /SDV521, /DV53L, /DV53A and /DV541, the same model I/O module with /PRP prevention pin of false insertion option can be used. For example, AKB651-M003/DV53L can be used only with SDV531-L or L1DV531 that have /PRP prevention pin of false insertion option.

		Description
Model	AKB652	Signal Cable (for connections between SDV526/L1DV526 and Terminal Board)
Suffix Codes	-M001	Length: 1 m
	-M002	Length: 2 m
	-M003	Length: 3 m
	-M005	Length: 5 m
	-M007	Length: 7 m
	-M010	Length: 10 m
	-M015	Length: 15 m
	-M020	Length: 20 m
	-M025	Length: 25 m
	-M030	Length: 30 m
Option Code	/SDV526	Special cable for SDV526/L1DV526

Note: When connecting AKB652 with SDV526, check if the cable length of AKB652 is proper or not, referring to “Terminal Board is connected” of “■ LIMITATIONS ON DIGITAL OUTPUT MODULE CONNECTIONS” in “ProSafe-RS Outline of I/O Modules (for FIO)” (GS 32P06K60-01EN).
Note: When connecting AKB652 with L1DV526, check if the cable length of AKB652 is proper or not, referring to “Terminal Board is connected” of “■ LIMITATIONS ON DIGITAL OUTPUT MODULE CONNECTIONS”in “ProSafe-RS Lite Outline of I/O Modules” (GS 32P56K60-01EN).

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

		Description
Model	KS1	Signal Cable (40-40 pins) (for connections between SAI143/L1AI143, SAV144/L1AV144, or SAI533/L1AI533 and Terminal Board)
Suffix Codes	-01	Length: 1 m
	-02	Length: 2 m
	-03	Length: 3 m
	-05	Length: 5 m
	-07	Length: 7 m
	-10	Length: up to 10 m (*1)
	-15	Length: 15 m
	-20	Length: 20 m
	-25	Length: 25 m
	-30	Length: 30 m
	-35	Length: 35 m
	-40	Length: 40 m
	-45	Length: 45 m
	-50	Length: 50 m
Style Code	*B	Style B
Option Codes	/SAI143	Special cable for SAI143/L1AI143
	/SAI533	Special cable for SAI533/L1AI533
	/SAV144	Special cable for SAV144/L1AV144

*1: "Length: up to 10 m" means the customer can specify the cable length that is not exceeding the 10 meters. For example, 8 m or 9 m can be specified when KS1-10*B is selected.

Note: A mechanism to prevent wrong type I/O module insertion is supported. When you select option code /SAI143, /SAI533 and /SAV144, the same model I/O module with /PRP prevention pin of false insertion option can be used. For example, KS1-03/SAI143 can be used only with SAI143/L1AI143 that have /PRP prevention pin of false insertion option.

■ CONFORMITY STANDARDS

Refer to "Standards Compliant Models" (GS 32P01B60-01EN).

■ ORDERING INFORMATION

Specify the model, suffix code(s), and option code(s).

■ TRADEMARK ACKNOWLEDGMENT

The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation
Subject to change without notice.

Attachment 9.21 TB for Analog Modules (SBA4D-06)

GS 32Q06L20-31E

General Specifications

ProSafe-RS/ProSafe-RS Lite
Terminal Boards/Relay Boards

GS 32Q06L20-31E

■ GENERAL

This GS describes the hardware specifications of the terminal boards used for the ProSafe-RS/ProSafe-RS Lite system.

■ STANDARD SPECIFICATIONS

● Terminal Board

19-inch Rack Mountable Type

Application	Model	Number of connection channels	Terminal	SIL (*1)	Connection module (*2)	Connection cable	Weight	Withstand voltage	Insulation resistance
For analog signals (single/ dual-redundant configuration)	SEA4D	16 channels x 2	M4 screw	SIL3	SAI143/ L1AI143	KS1	1.5 kg	500 V AC (for 1 minute) (*6)	100 MΩ minimum (500 V DC)
					SAV144/ L1AV144	KS1			
					SAI533/ L1AI533	KS1			
For digital signals (single/ dual-redundant configuration)	SED2D	4 channels x 4	M4 screw	SIL3	SDV521/ L1DV521	AKB651	2.3 kg	2000 V AC (for 1 minute) (*6)	100 MΩ minimum (500 V DC)
	SED3D	8 channels x 4	M4 screw	SIL3	SDV53A/ L1DV53A	AKB331 (*4)	2.0 kg	2000 V AC (for 1 minute) (*6)	
	SED4D	16 channels x 2 (*3)	M4 screw	SIL3	SDV144/ L1DV144	AKB331	1.5 kg	500 V AC (for 1 minute) (*6)	
					SDV531-S	AKB331			
					SDV531-L/ L1DV531-L	AKB331			
					SDV541/ L1DV541	AKB331			
	SWD2D (*5)	4 channels x 4	M4 screw	SIL3	SDV526/ L1DV526	AKB652	2.9 kg	1500 V AC (for 1 minute) (*6)	

Note: Connector covers must be mounted on connectors that do not have cables connected to them, to protect them from dust, and also to protect the connector pins.

*1: SIL (Safety Integrity level) of the terminal board alone.
*2: When connecting terminal boards with input/output modules, refer to following GS.
"ProSafe-RS Field Device Connection (for FIO)" (GS 32Q06J10-31E)
"ProSafe-RS Lite Field Device Connection" (GS 32P56J10-01EN)
*3: 8 channels × 2 for SDV531/L1DV531 connection
*4: Use AKB331 of style code S3 or later.
*5: Contact rating between ALM terminals when any fuse is blown
Meet all the following requirements.
Rated output voltage: 125 V AC or less, 125 V DC or less
Rated output current: 0.3 A or less
Rated power: 25 VA or less
*6: Between each signal terminal, and between all signal terminals and grounding terminal

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan
GS 32Q06L20-31E
©Copyright July2011 (YK)
11th Edition Jan. 22, 2021 (YK)

DIN Rail Mount Type

Application	Model	Number of connection channels	Terminal	SIL (*1)	Connection module (*2)	Connection cable	Weight	Withstand voltage	Insulation resistance
For analog signals (single/ dual-redundant configuration)	SBA4D	16 channels x 1	Pressure clamp	SIL3	SAI143/ L1AI143	KS1	0.2 kg	NA	NA
					SAV144/ L1AV144	KS1			
					SAI533/ L1AI533	KS1			
	S1BB4D (*3) (*4)	16 channels x 1	Pressure clamp	SIL3	SAI143/ L1AI143	KS1	0.5 kg	2000 V AC (for 1 minute) (*5)	20 MΩ minimum (500 V DC)
	SBT4D	16 channels x 1	Pressure clamp	SIL3	SAT145/ L1AT145	AKB331	0.3 kg	200 V AC (for 1 minute) (*6)	10 MΩ minimum (200 V DC)
	SBR4D	16 channels x 1	Pressure clamp	SIL3	SAR145/ L1AR145	AKB611	0.3 kg		
For digital signals (single/ dual-redundant configuration)	SBD2D (*3)	4 channels x 1	Pressure clamp	SIL3	SDV521/ L1DV521	AKB651	0.3 kg	2000 V AC (for 1 minute) (*5)	10 MΩ minimum (500 V DC)
	SBD3D (*3)	8 channels x 1	Pressure clamp	SIL3	SDV531-L/ L1DV531-L	AKB331 (*7), AKB651	0.3 kg	2000 V AC (for 1 minute) (*5)	
					SDV531-S	AKB331 (*7)			
					SDV53A/ L1DV53A	AKB331 (*7), AKB651			
	SBD4D (*3)	16 channels x 1	Pressure clamp	SIL3	SDV144/ L1DV144	AKB331 (*7)	0.3 kg	2000 V AC (for 1 minute) (*5)	
					SDV541/ L1DV541	AKB331 (*7), AKB651			

Note: Connector covers must be mounted on connectors that do not have cables connected to them, to protect them from dust, and also to protect the connector pins.

*1: SIL (Safety Integrity level) of the terminal board alone.
*2: When connecting terminal boards with input/output modules, refer to following GS.
"ProSafe-RS Field Device Connection (for FIO)" (GS 32Q06J10-31E)
"ProSafe-RS Lite Field Device Connection" (GS 32P56J10-01EN)
*3: The READY contact rating shows below.
125 V AC or less and 0.3 A or less
60 V DC or less and 1 A or less
*4: Rated power supply current for field devices is 0.35 A per channel. Inrush current must be 0.7 A or less for the first 2 seconds.
*5: Between power terminal and READY terminal
*6: Between channels
*7: Use AKB331 of style code S3 or later.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

● Relay Board

19-inch Rack Mountable Type

Item	Specifications	
Model	SRM53D	SRM54D
Safety integrity level	SIL 2 (*1)	SIL 2 (*1)
Type of input/output and number of I/O channels	Contact output/8 channels x 2 (dry contact outputs)	Contact output/16 channels x 1 (dry contact outputs)
Terminals	M4 screws, 16 poles x 2 (outputs) M4 screws, 2 poles x 1 (power)	
Connection module	SDV531/L1DV531, SDV144 /L1DV144 (read-back) (*2) Dual-redundant possible	SDV541/L1DV541, SDV144/L1DV144 (read-back) (*2) Dual-redundant possible
External connection	Dedicated signal cable AKB331	
Withstanding voltage	Between field device terminals and case: 2 kV for 1 minute Between 24 V power terminal and case: 500 V for 1 minute Between 24 V power terminal and field device terminals: 2.5 kV for 1 minute	
Insulation resistance	10 MΩ minimum (500 V DC)	
External supply voltage/current	24 V DC +5 %, -3.1 % (*3) Up to 1500 mA (24 V DC)	24 V DC +5 %, -1.2 % (*3) Up to 1500 mA (24 V DC)
Rated output voltage/current (current/channel)	250 V AC / 2 A 125 V DC / 0.4 A 30 V DC / 2 A	
Ambient temperature (during operation)	-20 to 70 °C	
Ambient humidity (both during operation and in transit/storage conditions)	5 to 85 % RH	
Weight	2.7 kg	

*1: SRM53D, SRM54D complies with SIL2 when used as DTS (De-energized-To-Safe) outputs under “low demand mode of operation” (the frequency of demands is no greater than one per year), which is defined in the IEC 61508.

*2: When connecting relay boards with output modules, refer to following GS.
“ProSafe-RS Field Device Connection (for FIO)” (GS 32Q06J10-31E)
“ProSafe-RS Lite Field Device Connection” (GS 32P56J10-01EN)

*3: This is the tolerance of the external supply voltage when the signal cable of 10 m (AKB331-M010) is used. The voltage loss of the external power supply varies with the length of the signal cable. For details, refer to following GS.
“ProSafe-RS Outline of I/O Modules (for FIO)” (GS 32Q06K20-31E)
“ProSafe-RS Lite Outline of I/O Modules” (GS 32P56K20-01EN)
Moreover, the maximum length of the signal cable (AKB331) used for connecting to the relay board is 20 m.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

DIN Rail Mount Type

Item	Specifications
Model	SBM54D (*1)
Safety integrity level	SIL 2 (*2)
Type of input/output and number of I/O channels	Contact output/16 channels x 1 (dry contact outputs)
Terminals	Pressure clamp
Connection module (*3)	SDV541/L1DV541 (*4) Dual-redundant possible
External connection	Dedicated signal cable AKB331
Withstanding voltage	Between field device terminal and case: 2 kV for 1 minute Between 24 V power terminal and case: 2 kV for 1 minute Between 24 V power terminal and field device terminals: 2.5 kV for 1 minute Between READY terminal and case: 2 kV for 1 minute Between READY terminal and 24 V power terminal: 2 kV for 1 minute Between READY terminal and field device terminals: 2.5 kV for 1 minute
Insulation resistance	10 MΩ minimum (500 V DC)
External supply voltage/current	24 V DC +20 %, -10% Up to 500 mA (24 V DC)
Rated output voltage/current (current/channel)	30 V DC/4 A 240 V AC/4 A
Ambient temperature (during operation)	-20 to 70 °C
Ambient humidity (both during operation and in transit/storage conditions)	5 to 85 % RH
Weight	0.6 kg

*1: Dual power supply is available.
In case of power supply is normal operation, LED keeps ON. In the other case LED turns OFF.
The READY contact outputs the condition which power supply and all fuses is normal operation.
The READY contact rating shows below.
125 V AC or less and 0.3 A or less
60 V DC or less and 1 A or less

*2: SBM54D style code S3 or later complies with SIL2 when used as DTS (De-energized-To-Safe) outputs under “low demand mode of operation” (the frequency of demands is no greater than one per year), which is defined in the IEC 61508.

*3: When connecting relay boards with output modules, refer to following GS.
“ProSafe-RS Field Device Connection (for FIO)” (GS 32Q06J10-31E)
“ProSafe-RS Lite Field Device Connection” (GS 32P56J10-01EN)

*4: The style code and firmware revision numbers of SDV541 must be used following revision or later.
SDV541 S3, F1: 1 F2: 1

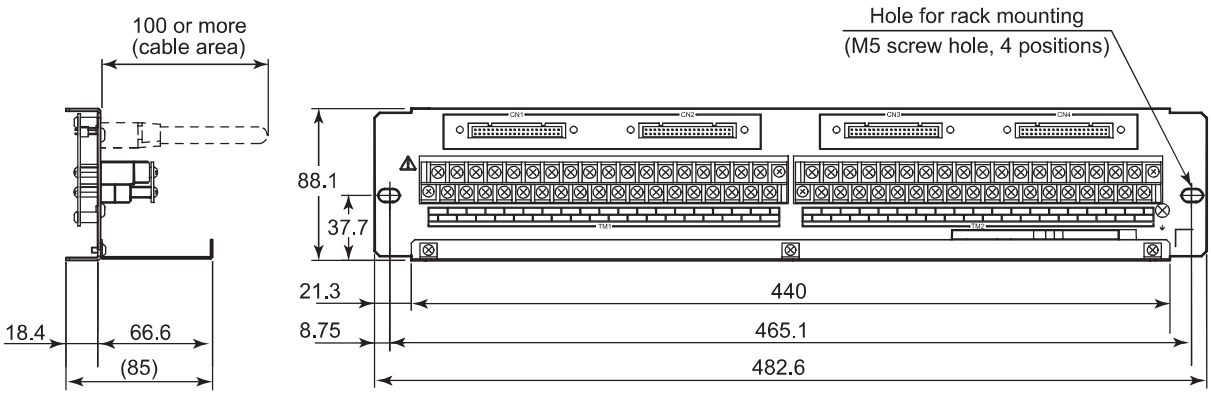
All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

■ EXTERNAL DIMENSIONS

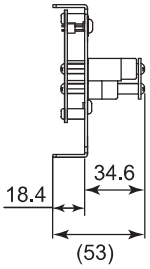
● Terminal Boards

SEA4D

Unit: mm



When option code is “/NTRY”



F01E.ai

Nominal tolerance:

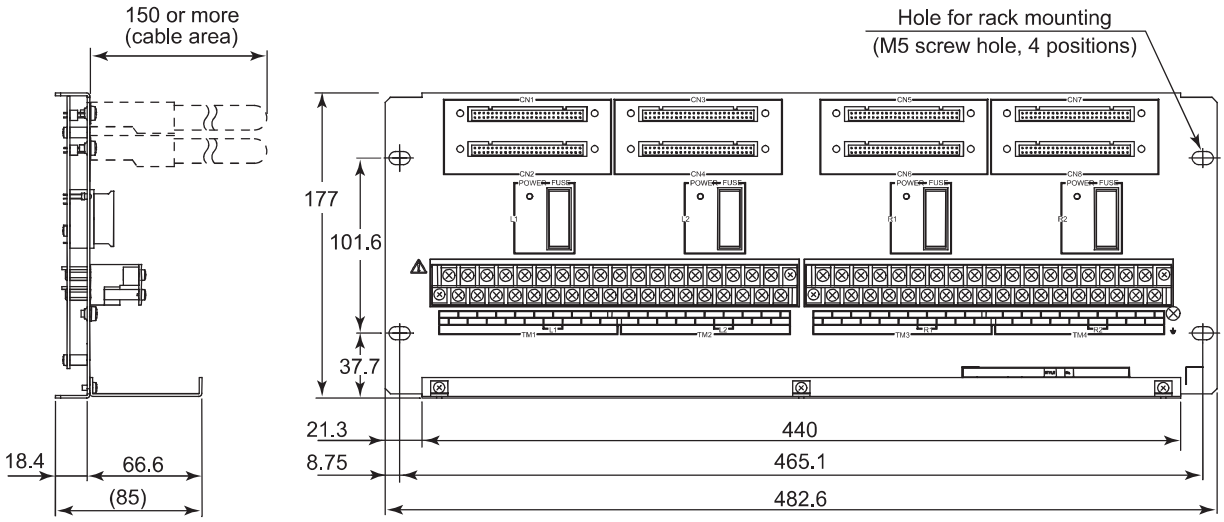
Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

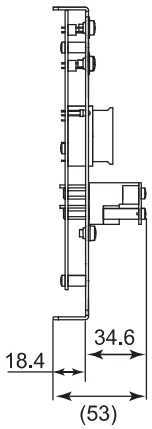
All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

SED2D

Unit: mm



When option code is "/NTRY"



F07E.ai

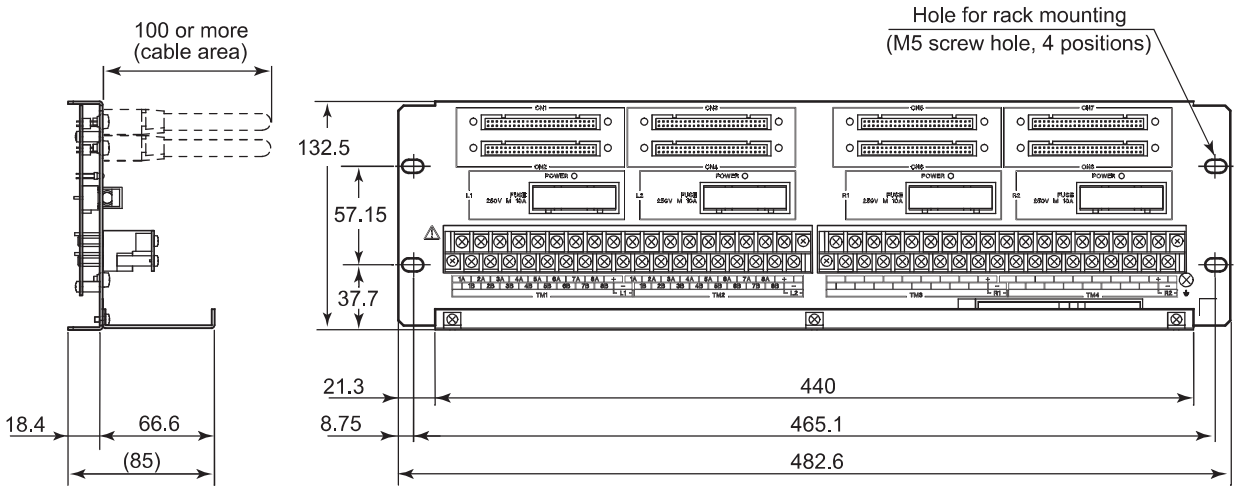
Nominal tolerance:

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

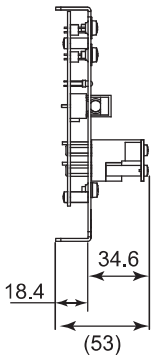
All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

SED3D

Unit: mm



When option code is “/NTRY”



F09E.ai

Nominal tolerance:

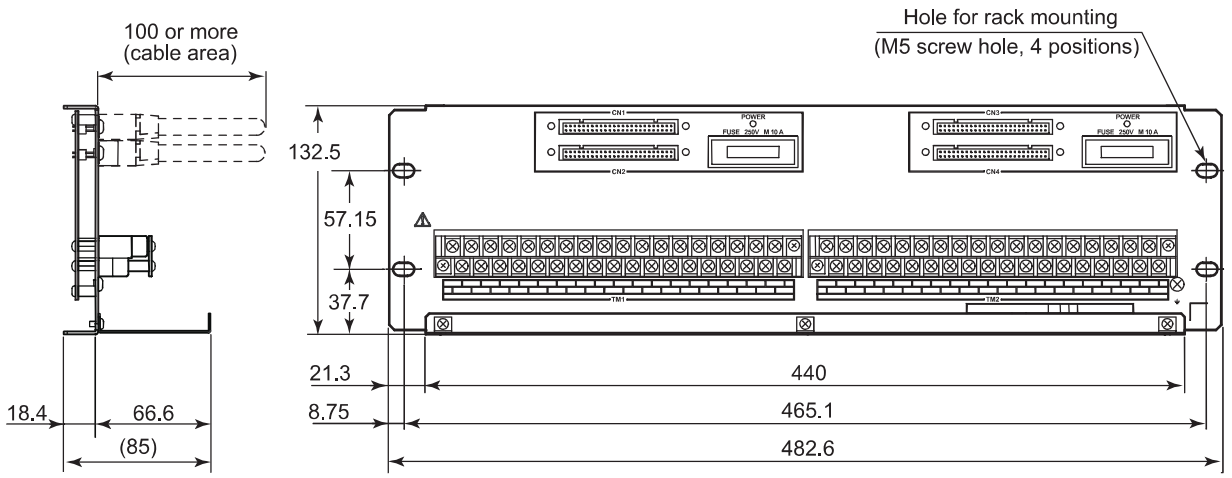
Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

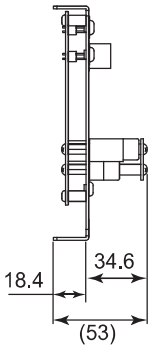
All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

SED4D

Unit: mm



When option code is “/NTRY”



F02E.ai

Nominal tolerance:

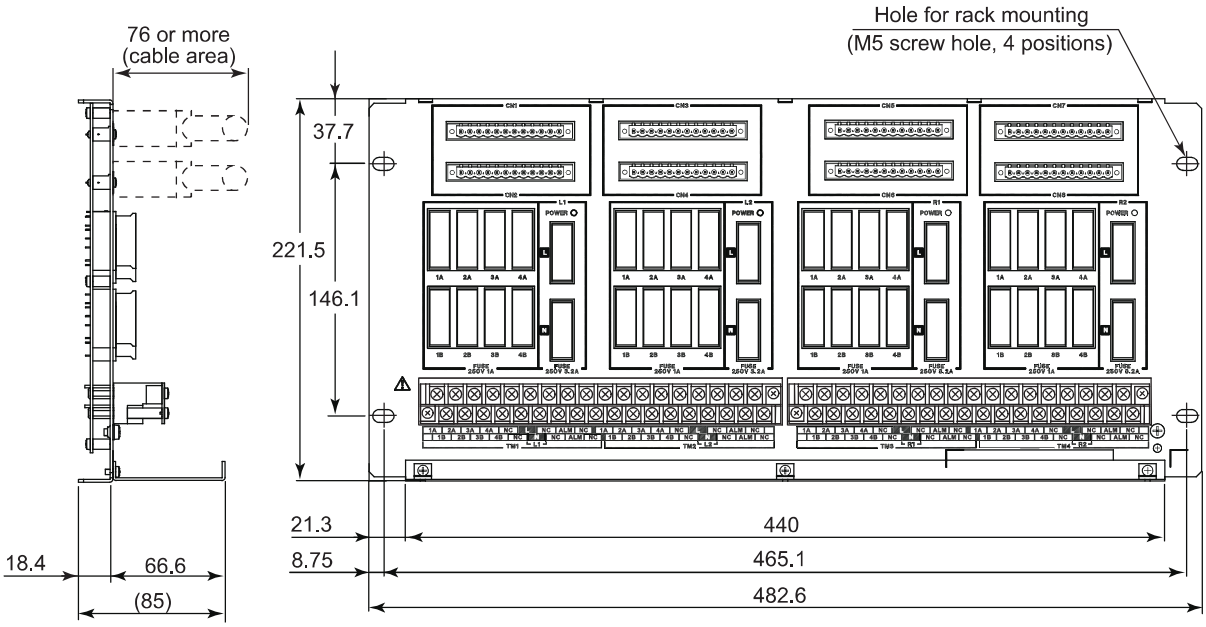
Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

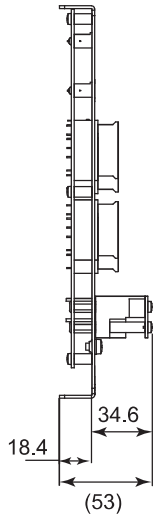
All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

SWD2D

Unit: mm



When option code is “/NTRY”



F08E.ai

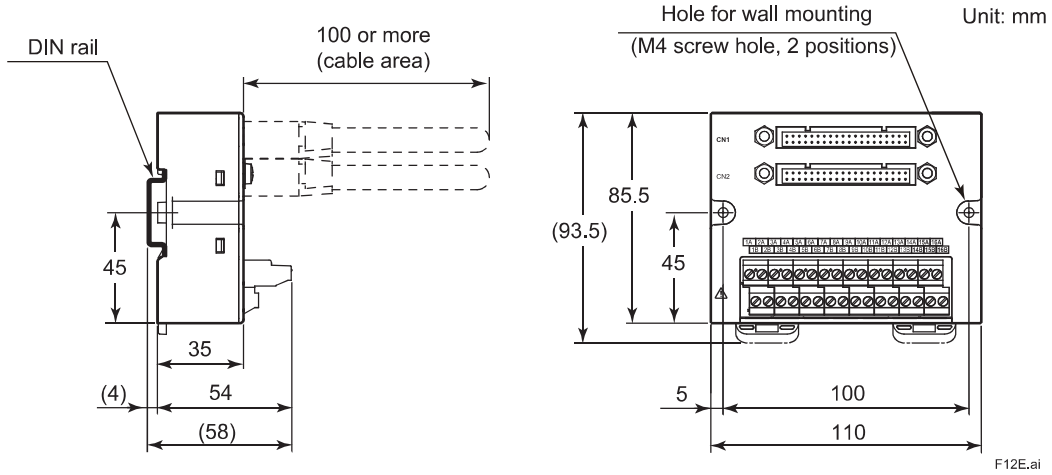
Nominal tolerance:

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

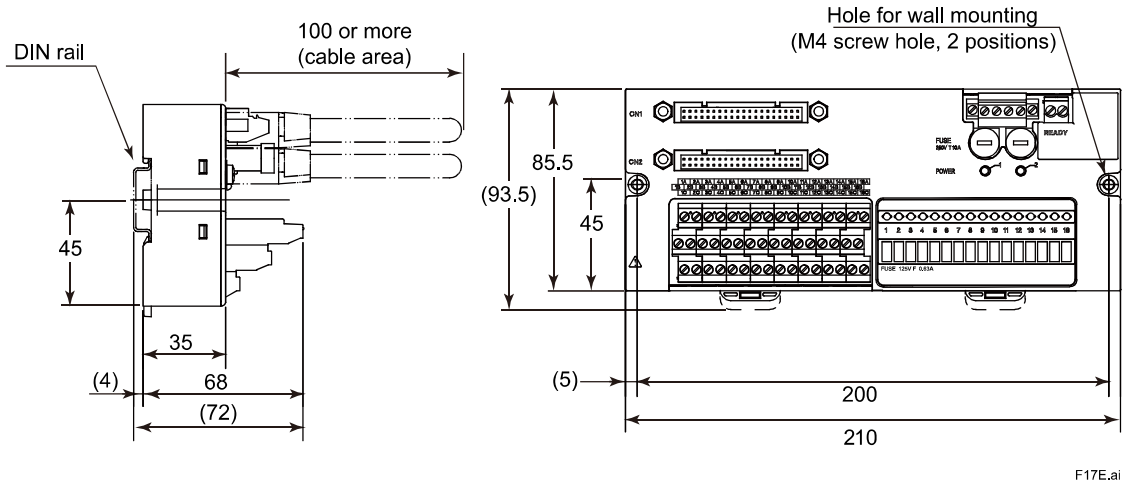
All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

SBA4D



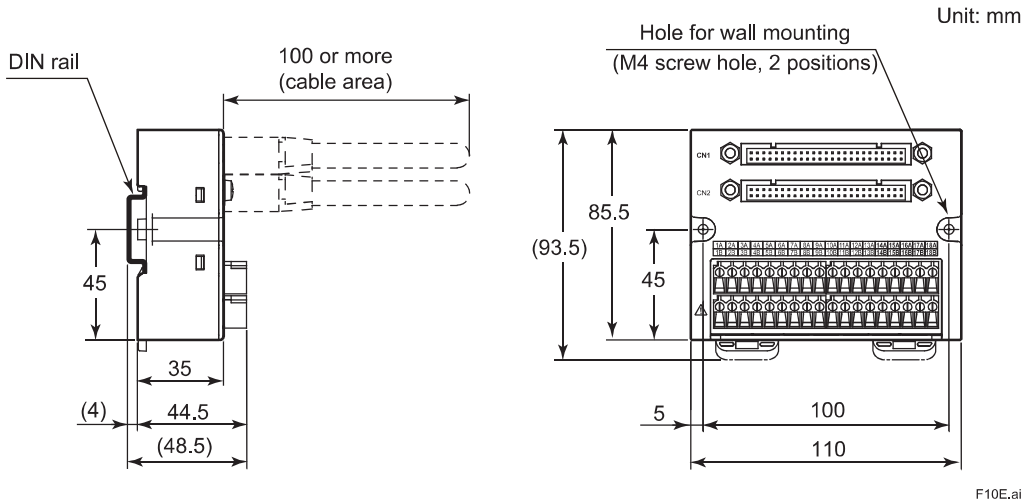
S1BB4D

Unit: mm



SBT4D

Unit: mm



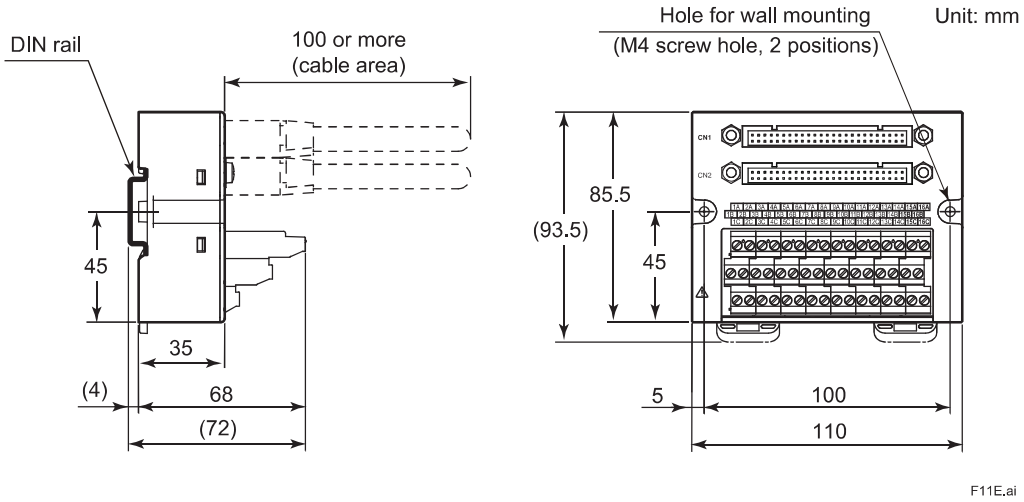
Nominal tolerance:

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

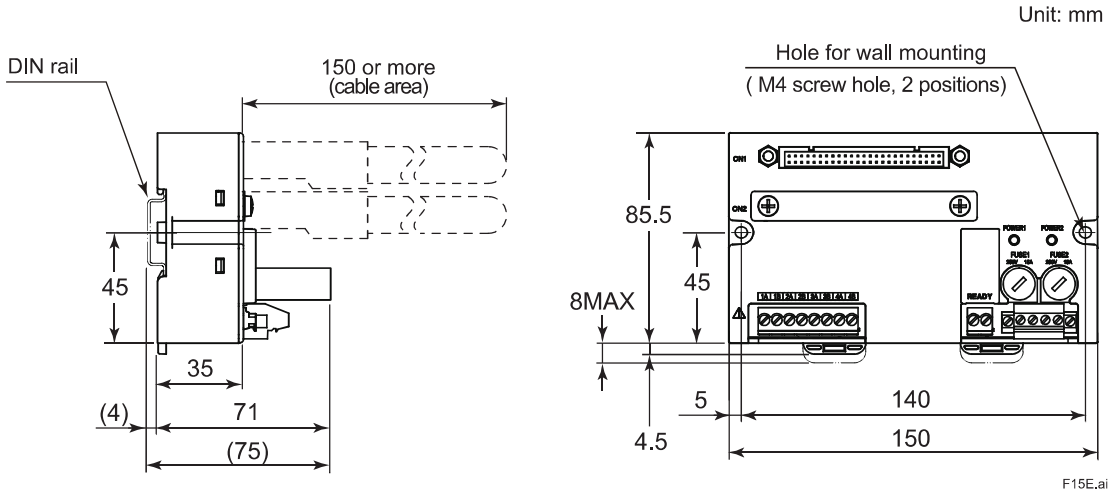
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

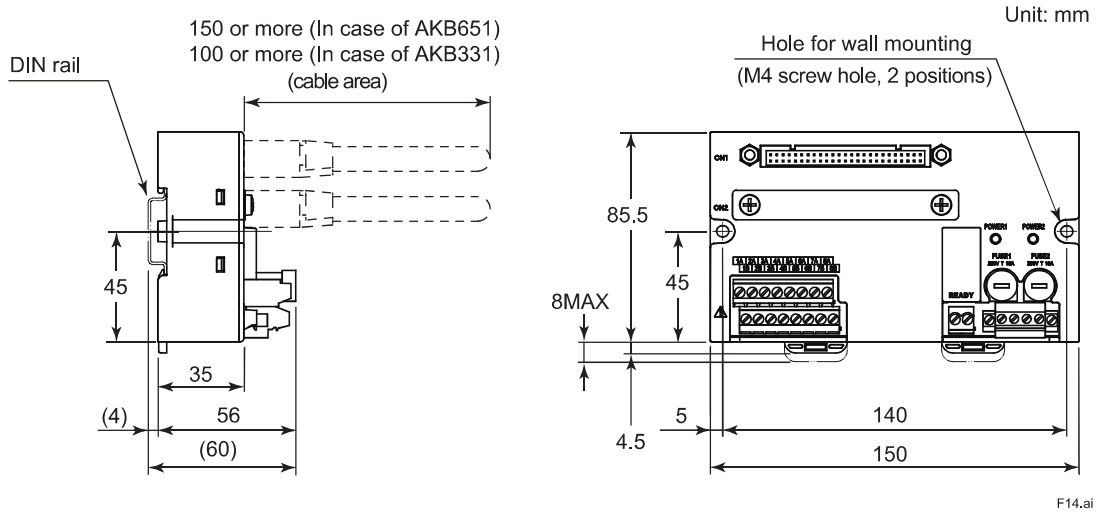
SBR4D



SBD2D



SBD3D



Nominal tolerance:

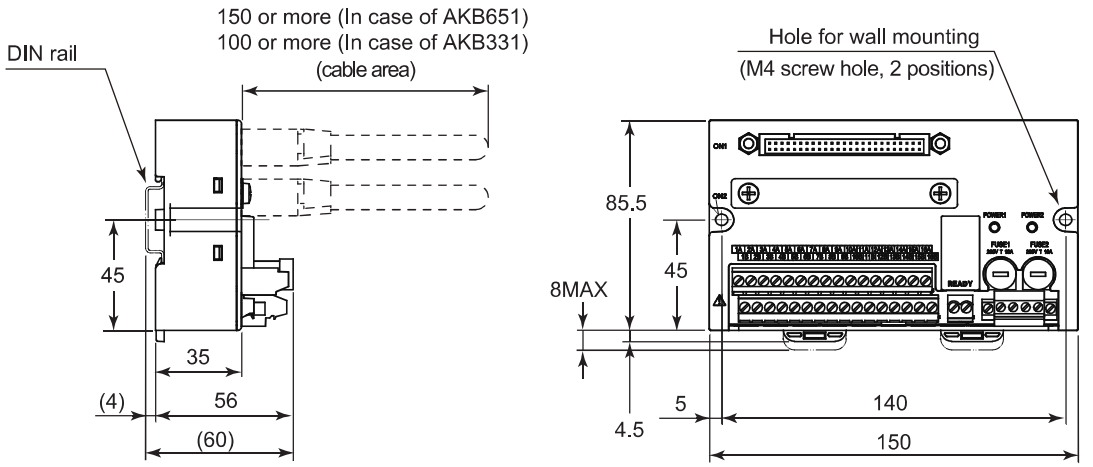
Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

SBD4D

Unit: mm



F13.ai

Nominal tolerance:

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

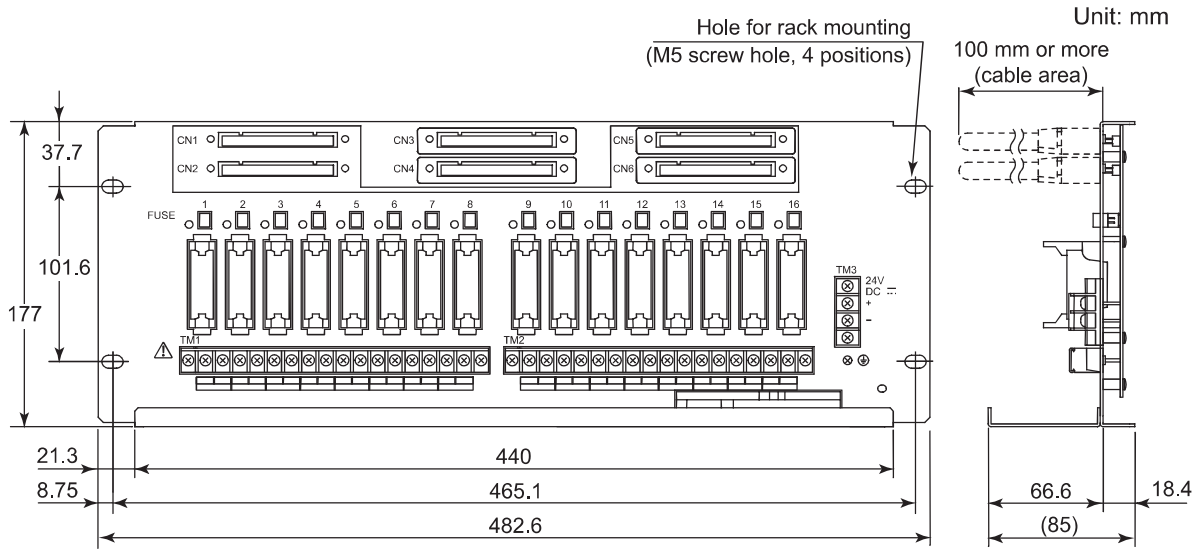
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

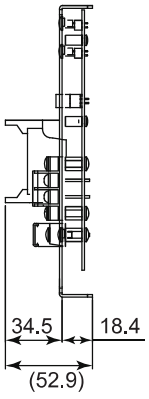
● Relay Board

SRM53D

Other than /BR4



When option code is “/NTRY”



F03E.ai

Nominal tolerance:

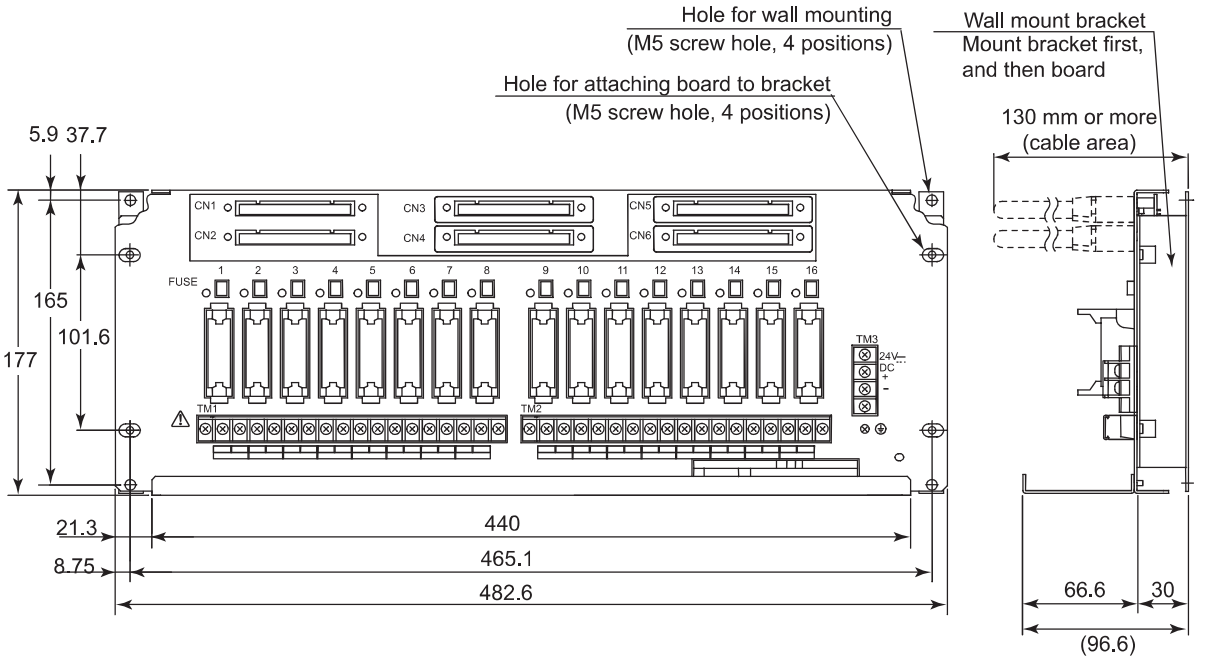
Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

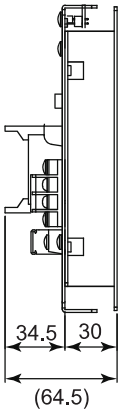
All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

For /BR4

Unit: mm



When option code is “/NTRY”



F04E.ai

Nominal tolerance:

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

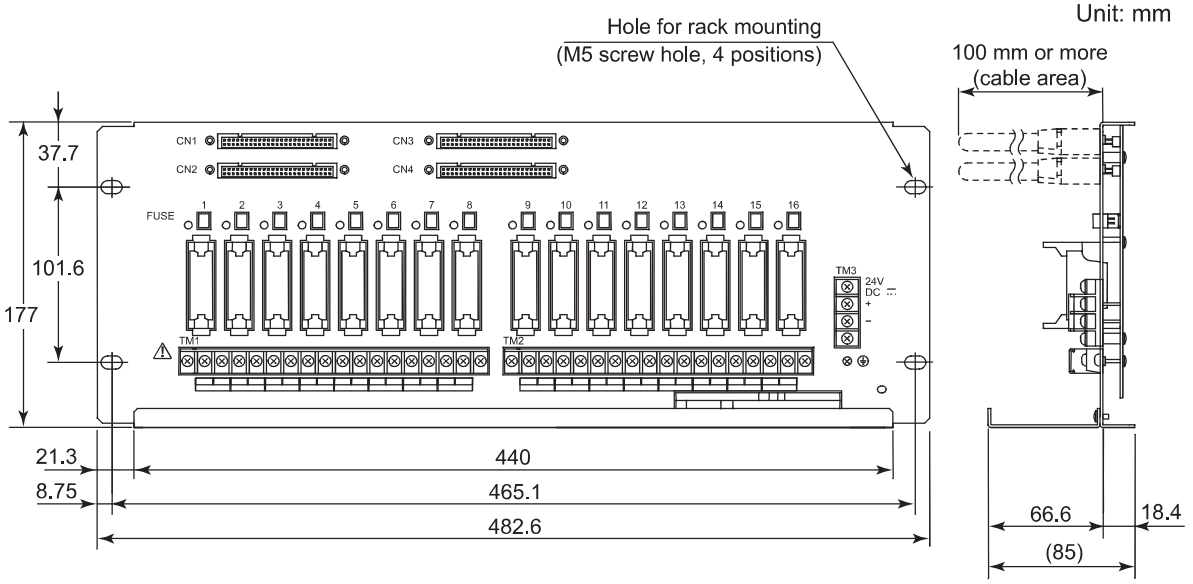
The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

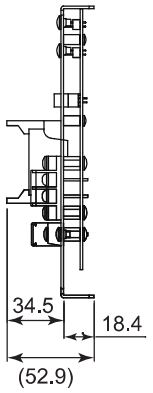
SRM54D

Other than /BR4

Unit: mm



When option code is “/NTRY”



F05E.ai

Nominal tolerance:

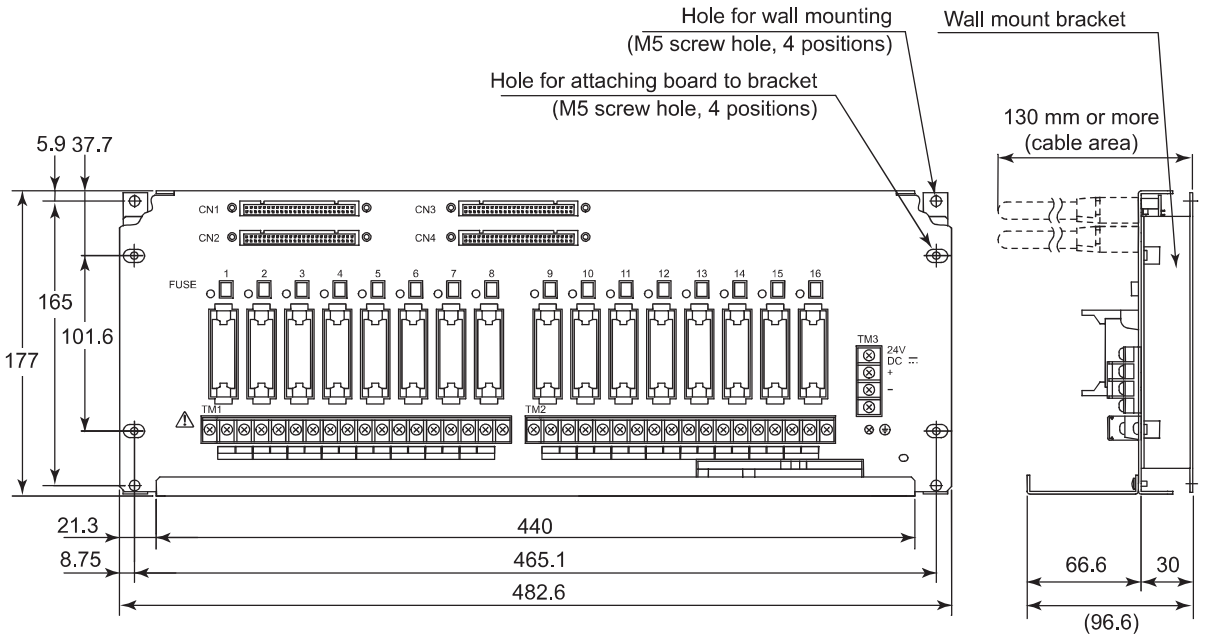
Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

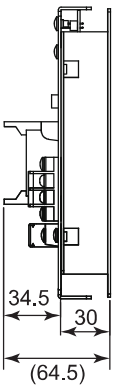
All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

For /BR4

Unit: mm



When option code is "/NTRY"



F06E.ai

Nominal tolerance:

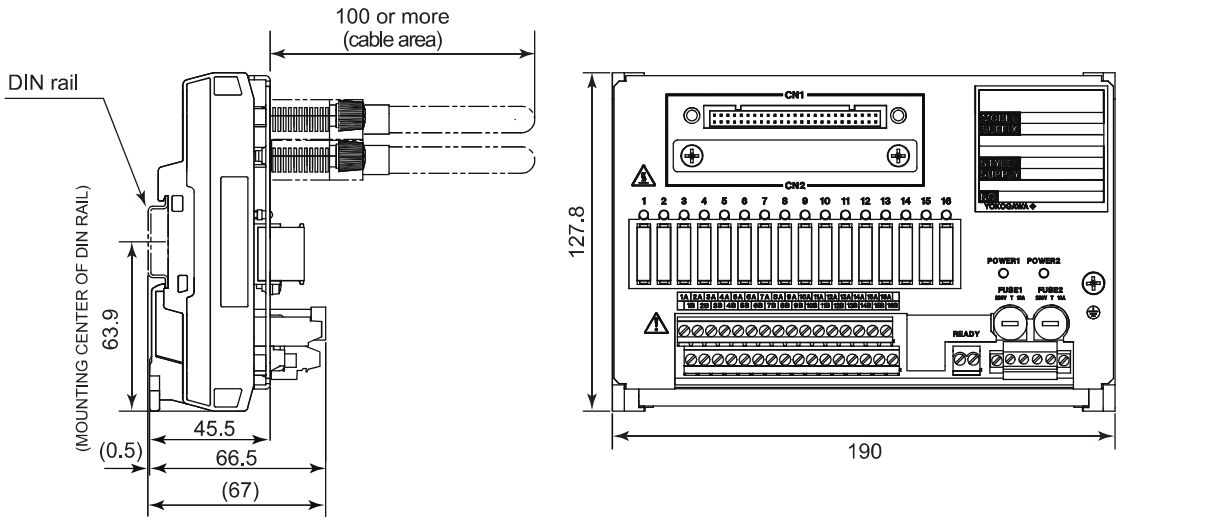
Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

SBM54D

Unit: mm



F16E.ai

Nominal tolerance:

Nominal tolerance is ± 0.8 mm for the dimensions of 0.5 mm or more and 120 mm or less, and the combined nominal tolerance is ± 1.5 mm.

The nominal tolerance is in accordance with JEM 1459 for the dimensions over 120 mm.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

■ MODEL AND SUFFIX CODES

Analog terminal board for single/dual-redundant configuration

		Description
Model	SEA4D	Analog Terminal Board (Single and Dual-Redundant, 16 channels x 2)
Suffix Codes	-0	Without surge absorber
	-1	With surge absorber
	6	With ISA Standard G3 and no explosion protection
	F	With ISA Standard G3 and explosion protection
Option Code	/NTRY	Without cable tray

		Description
Model	SBA4D	Terminal Board for Analog: DIN rail mount type (Single and Dual-redundant, 16 channels x 1)
Suffix Codes	-0	Always 0
	6	With ISA Standard G3 and no explosion protection
	F	With ISA Standard G3 and explosion protection

		Description
Model	S1BB4D	Terminal Board for Analog Input, 3-wire : DIN rail mount type
Suffix Codes	-0	Always 0
	6	With ISA Standard G3 and no explosion protection
	F	With ISA Standard G3 and explosion protection

		Description
Model	SBT4D	Terminal Board for TC/mV: DIN rail mount type (Single and Dual-redundant, 16 channels x 1)
Suffix Codes	-0	Without surge absorber
	6	With ISA Standard G3 and no explosion protection
	F	With ISA Standard G3 and explosion protection

		Description
Model	SBR4D	Terminal Board for RTD Input: DIN rail mount type (Single and Dual-redundant, 16 channels x 1)
Suffix Codes	-0	Without surge absorber
	6	With ISA Standard G3 and no explosion protection
	F	With ISA Standard G3 and explosion protection

Digital terminal board for single/dual-redundant configuration

		Description
Model	SED2D	Digital Terminal Board (Single and Dual-Redundant, 4 channels x 4)
Suffix Codes	-0	Without surge absorber
	-1	With surge absorber
	6	With ISA Standard G3 and no explosion protection
	F	With ISA Standard G3 and explosion protection
Option Code	/NTRY	Without cable tray

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

		Description
Model	SED3D	Digital Terminal Board (Single and Dual-Redundant, 8 channels x 4)
Suffix Codes	-A	For 48 V DC output, without surge absorber
	6	With ISA Standard G3 and no explosion protection
	F	With ISA Standard G3 and explosion protection
Option Code	/NTRY	Without cable tray

		Description
Model	SED4D	Digital Terminal Board (Single and Dual-Redundant, 16 channels x 2)
Suffix Codes	-0	Without surge absorber
	-1	With surge absorber
	6	With ISA Standard G3 and no explosion protection
	F	With ISA Standard G3 and explosion protection
Option Code	/NTRY	Without cable tray

		Description
Model	SWD2D	Digital Terminal Board (Single and Dual-Redundant, 100 to 120 V AC, 4 channels x 4)
Suffix Codes	-2	For 100 to 120 V AC output
	1	With ISA Standard G3
Option Code	/NTRY	Without cable tray

		Description
Model	SBD2D	Terminal Board for Digital Output: DIN rail mount type (Single and Dual-redundant, 4 channels x 1, for SDV521/L1DV521)
Suffix Codes	-0	Always 0
	6	With ISA Standard G3 and no explosion protection
	F	With ISA Standard G3 and explosion protection

		Description
Model	SBD3D	Terminal Board for Digital Output: DIN rail mount type (Single and Dual-redundant, 8 channels x 1, for SDV53☐/L1DV53☐)
Suffix Codes	-0	24 V DC (for SDV531/L1DV531)
	-A	48 V DC (for SDV53A/L1DV53A)
	6	With ISA Standard G3 and no explosion protection
	F	With ISA Standard G3 and explosion protection

		Description
Model	SBD4D	Terminal Board for Digital: DIN rail mount type (Single and Dual-redundant, 16 channels x 1, for SDV144/L1DV144 and SDV541/L1DV541)
Suffix Codes	-0	Always 0
	6	With ISA Standard G3 and no explosion protection
	F	With ISA Standard G3 and explosion protection

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation

Single or dual-redundant relay board with digital output

		Description
Model	SRM53D	Relay Board (8 × 2 Dry Contact Output)
Suffix Codes	-0	Always 0
	0	19-inch Rack mountable
	0	Basic
Option Codes	/BR4	Wall-mount bracket
	/NTRY	Without cable tray

		Description
Model	SRM54D	Relay Board (16 × 1 Dry Contact Output)
Suffix Codes	-0	Always 0
	0	19-inch Rack mountable
	0	Basic
Option Codes	/BR4	Wall-mount bracket
	/NTRY	Without cable tray

		Description
Model	SBM54D	Relay Board for Digital Output: DIN rail mount type (Single and Dual-redundant, 16 channels x 1, for SDV541/L1DV541)
Suffix Codes	-0	Always 0
	0	Always 0
	0	Standard type

■ CONFORMITY STANDARDS

Refer to “Standards Compliant Models (GS 32P01B60-01EN).”

■ ORDERING INFORMATION

Specify the model, suffix code(s), and option code(s).

For selecting the right products for explosion protection, please refer to TI 32S01J30-01E without fail.

■ TRADEMARK ACKNOWLEDGMENT

The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

All Rights Reserved. Copyright © 2011, Yokogawa Electric Corporation
Subject to change without notice.