Base Load Power Hub (BLPH)

Safety Validation Plan (SVP)

Document Number: 1724000594-IN-PL-00029

Supplier Document Number: E366772C00-SVP

Document Class: 3

ROSETTI MARINO	
1	NO COMMENTS - APPROVED - WORK MAY PROCEED
2	MINOR COMMENTS - REVISE AND RESUBMIT - WORK MAY PROCEED
3	MAJOR COMMENTS – REJECTED – DO NOT PROCEED
4	APPROVAL NOT REQUIRED
NOTE: Approval doesn't relieve the supplier from mandatory compliance with contractual documents and specifications. Comments made do not imply acceptance of any cost or delivery impact.	
Sign	Date
	11/09/2024

SIGNATURES ARE NOT REQUIRED

Rev.	Date	Description	Prepared	Reviewed	Approved
00	14/05/2024	ISSUE FOR INFORMATION (IFI)	MP	AB	Raghavendran

UPDATE THE DATE

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

File: Cover SHeet ADD THE FILE NAME

Revision / Change Log

Rev.	Description
00	Issue for Review (IFR) 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

Base Load Power Hub (BLPH)

Project No. 123A90

CROSSWIND

Crosswind Hollandse Kust Noord

Netherlands

YOKOGAWA

ITALY

Yokogawa Main Automation Contractor Toolkits

GES_A0202_02

DOCUMENT TITLE:

Safety Validation Plan

PO Number CW-I-WP4-2023-05	**Purchaser:** ROSETTI MARINO S.p.A.
Yokogawa Document Number: E366772C00-SVP	**Purchaser Document Number:** 1724000594-IN-PL-00029

REV	DATE	DESCRIPTION	ORIG	CHK	APPR
				AB	Digitally signed by R Raghavendran Date: 2024.08.24 12:40:32 +05'30'
00	23-Aug-2024	Issued for Review	MP	AB	Raghavendran

REVISION DETAILS

Confidentiality Notice: This document and the information contained herein shall not be copied or used for other than the purposes for which it is or has been provided or disclosed in any form or medium to third parties, except as expressly permitted by Yokogawa.

Revision History of this Project Document

Rev.	Date (MM/DD/YY)	Section	Description
0.1	05/14/24	All	Issued for SA Review/Approval (Internal)
0.2	06/10/24	All	Issued for SA Review/Approval (Internal)
0.3	07/30/24	All	Issued for SA Review/Approval (Internal)
00	08/23/24	All	Issued for Client Approval

Copyright © Yokogawa Electric Corporation

Table of Contents

1 Introduction 5
1.1 Purpose and Scope 5
1.2 Reference Documents 5
1.2.1 General 5
1.2.2 Crosswind Hollandse Kust Noord 5
1.2.3 Yokogawa 6
1.3 Definitions, Abbreviations and Acronyms 7
1.4 Product certificate for ProSafe-RS 10
1.5 Hold List 11
2 Functional Safety Management 12
2.1 Introduction 12
2.2 The Safety Life Cycle 12
2.3 Safety Verification, Assessment and Validation 14
2.3.1 Introduction 14
2.3.2 Verification 14
2.3.3 Functional Safety Assessment 14
2.3.4 Validation 14
2.4 Systematic safety integrity 14
2.5 Availability Calculations 15
2.6 Installation and Commissioning 15
2.7 Operation and Maintenance 15
2.8 Modifications 15
2.9 Decommissioning 15
2.10 GMS-600-14-01 Authorization 16
2.11 TÜV Rheinland Certification 18
3 Safety Requirements - Safety Solutions 21
3.1 Introduction 21
3.2 Safety Requirement Specification 21
3.3 System Design 21
3.3.1 System Overview 21
3.3.2 Design Principles 22
3.4 Requirements versus Solutions 23
3.4.1 Safety Instrumented Functions/Loops 24
3.4.2 Safety Parameters 24
3.4.3 Safety Related Parameters 25

Copyright © Yokogawa Electric Corporation

3.4.4 Segregation 26
3.4.5 Sensors 26
3.4.6 Input Field Interfaces 27
3.4.7 LS Input Channels 28
3.4.8 Logic Solver(s) 28
3.4.9 LS Output Channels 29
3.4.10 Output Field Interfaces 30
3.4.11 Final Elements 30
3.4.12 Overrides and Inhibits 31
3.4.13 Environment 32
3.4.14 Communication Interfaces 33
3.4.15 Application Programming 33
3.4.16 Security 34
4 Safety Assessment Notes for the SIS system 35
4.1 Introduction 35
4.2 Safety Architecture 35
4.3 Reliability Calculations 35
4.3.1 Scope 35
4.3.2 Results 35
5 Safety Assessment Notes for FGS Systems 36
5.1 Introduction 36
5.2 Safety Architecture 36
5.3 Reliability Calculations 36
5.3.1 Scope 36
5.3.2 Results 36
6 Miscellaneous 37
7 Modifications 37
End of document 37

Appendix I Availability Calculations
Appendix II Safety Certificates and Safety Manuals
Attachment -1 System Architecture

Copyright © Yokogawa Electric Corporation

1 Introduction

1.1 Purpose and Scope

This document describes the principal activities in the life cycle of the project to be executed by Yokogawa relating to the verification and validation of the functional safety and safety integrity of the Safety Instrumented System. The two objectives of this document are firstly to support that the Safety Instrumented System(s) is realised according to the safety regulations as per international standards IEC 61508 and IEC 61511, and secondly to verify that the required safety integrity level is achieved.
Section 2 describes briefly the verification and validation process of the SIS
Section 3 contains an analysis of the requirements on the SIS
Section 4 contains an assessment of the safety functions.

This document has been prepared by Yokogawa with the assistance and approval of an independent functional safety assessor appointed by GMS-600-14-01-GB. This assessor is responsible for internal safety validation, therefore this assessor has to consider that the project team has correctly stated the specified requirements in this SVP.

Although not being part of Yokogawa's scope and responsibility, inconsistencies and deficiencies within client's safety requirements will be recorded in this SVP as far as they can be identified. It is Yokogawa's policy to present these at an early stage.

In case the SVP is marked as a lifecycle document by the end-user, later (site) modifications might necessitate the update of this document. (IEC: "back to the appropriate phase").

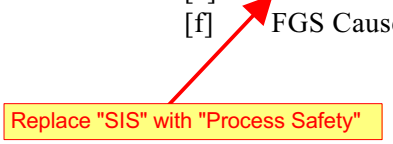
1.2 Reference Documents

1.2.1 General

- IEC 61508 Functional safety of E/E/PES safety related systems (Edition -2)
- IEC 61511 Safety Instrumented Systems for the process industry (Edition -2)
- ISO 9001 Quality management
- Yokogawa Quality Management System

1.2.2 Crosswind Hollandse Kust Noord

Safety Requirement Specification, comprising:
[a] Safety System (ESD, Fire and Gas) Specification (123A90-DDL-IN-SP-40100, Rev 00)
[b] Process Safety Cause & Effect Matrix (123A90-DDL-IN-CE-40000, Rev 00)
[c] Instrument I/O List (123A90-DDL-IN-LIS-40089, Rev 00)
[d] System Specification for Main Automation Contractor (K559-2254-IC-SPE-001, Rev 00)
[e] SIS Cause and Effect (123A90-DDL-IN-CE-40000)
[f] FGS Cause and Effect (123A90-DDL-IN-CE-40002)



Copyright © Yokogawa Electric Corporation

Remove items? already included in 1724000594-IN-MAN-00038

1.2.3 Yokogawa

- ProSafe-RS Safety Manual(IM32P01S10-01EN(7))
- ProSafe-RS Engineering guide Vol. 1 (IM32P01C10-01EN(7))
- ProSafe-RS Engineering guide Vol. 2 (IM32P01C20-01EN(7))
- ProSafe-RS Installation Guidance (TI 32P01J10-01EN(17))
- System Architecture (E366772C00-SA, Rev 01)
- Network Connection Diagram (E366772C00-ND, Rev 00)
- PAS Hardware Functional Design Specification (FDS-HW) (E366772C00-FDS_HW, Rev 00)
- PCS and SAFETY SISTEMS Software Functional Design Specification (FDS-SW) (E366772C00-FDS_SW, Rev 00)
- Bill of Material (E366772C00-BOM, Rev 00)
- PCS and Safety System IO List (HW and SW) (E366772C00-IO, Rev 00)
- Safety Controller loading estimation (E366772C00-SLE, Rev 00)
- Safety Systems Cabinets (SIS And FGS) General Arrangement Drawings And Internal Layout (E366772C00-SIS_CLO, Rev 00)
- Safety Systems Cabinets (SIS And FGS) Wiring Diagrams And Terminal Strips (E366772C00-SIS_WD, Rev 00)
- HW Factory Acceptance Test (Fat) Procedure (E366772C00-HW_FAT, Rev 00)
- Instructions for Operation and Maintenance for ProSafe-RS (E366772C00-SIS_IOM, Rev 00)

GENERAL REMARK:
Please insert Project document number together with Supplier's number

include also recent included documents that have complementary relevance in maintaining Safety / 61511:
- Cybersecurity Risk Assessment & Report
- Cybersecurity Design document
- Cybersecurity SAT Procedure

Copyright © Yokogawa Electric Corporation

1.3 Definitions, Abbreviations and Acronyms

ALARP	As Low As Reasonable Practicable
AMS	Alarm Management System
ATEX	Atmospheres Explosibles (French, Explosive Atmospheres)
BFD	Block Flow Diagram
BLPH	Base Load Power Hub
BPCS	Basic Process Control System
CAP	Critical Action Panel
CCN	Central Control Network
CCR	Central Control Room
PAS	Process Automation System (PCS+EMCS+SIS+F&G)
CHAZOP	Control Systems Hazard Operability Study
COMPANY	Shell Global Solutions International B.V. (SGSI)
CI SERVER	Collaborative Information Server
CW	CrossWind
CWHKN	CrossWind Hollandse Kust Noord
DEM	Design Engineering Manual
DEP	Design Engineering Practice
DoC(FS)	Declaration of Conformance for Functional Safety
EMC	Electromagnetic Compatibility
EMCS	Electrical Monitoring And Control System
EPC	Engineering, Procurement & Construction
ESD	Emergency Shutdown
EU	European Union
EWS	Engineering Workstation
Ex	Explosion Proof
FAT	Factory Acceptance Test
F&G	Fire & Gas
FDS	Functional Design Specification
FGS	Fire & Gas System
FSAC	Functional Safety Assessment Checksheet
FSM	Functional Safety Management
GMS-600-14-01-GB	Yokogawa GMS-600-14-01 Governance Board
HART	Highway Addressable Remote Transducer
HAZID	Hazard Identification
HAZOP	Hazard and Operability Analysis

Copyright © Yokogawa Electric Corporation

HFT	Hardware Fault Tolerance
HKN	Hollandse Kust Noord
HLV	Heavy Lift Vessel
HMI	Human Machine Interface
HRA	Health Risk Assessment
HS(S)E	Health, Safety, (Security) and Environment
HVAC	Heating Ventilation and Air Conditioning
I/O	Input/Output
IACS	Industrial Automation and Control Systems
IAMS	Instrument Asset Management System
ICM	Instructions for Commissioning
IEC	International Electrotechnical Commission
IOM	Instructions for Operation and Maintenance
IP	Ingress Protection / Internet Protocol
IS	Intrinsically Safe
ISO	International Organization for Standardization
ITER	Instrument & Telecoms Equipment Room
LS	Logic Solver
LV	Low Voltage
MAC	Main Automation Contractor
MTTR	Mean Time To Repair
MTBF	Mean Time Between Failure
MW	Mega Watt
n.a.	Not applicable
n.s.	Not specified
NAMUR	Interessengemeinschaft Automatisierungstechnik der Prozessindustrie (User Association of Automation Technology in Process Industries)
NIS	Non-Intrinsically Safe
O&M	Operation & Maintenance
OWNER	Crosswind
OWS	Operator Workstation
P&ID	Piping & Instrumentation Diagram
PSMT	Procedure for Site Modification and Test
RAM	Reliability, Availability & Maintainability (O&M)
RAM	Risk Assessment Matrix (Safety)
RSV	ProSafe-RS Safety Verifier
SA group	Safety Assurance group, Yokogawa's independent

Copyright © Yokogawa Electric Corporation

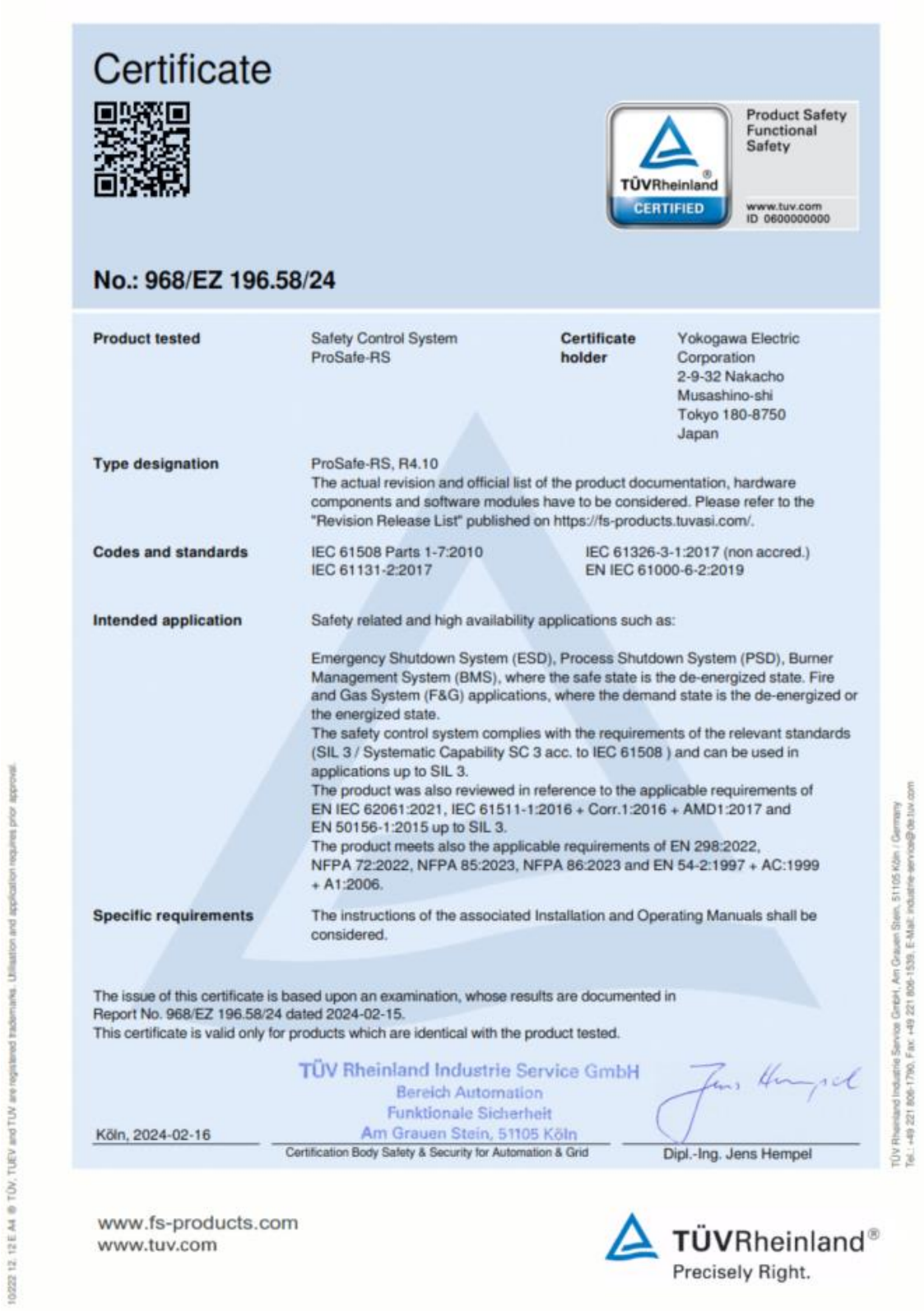
	group of Functional Safety specialists
SC	Systematic Capability
SCADA	Supervisory Control and Data Acquisition
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirements Specification
SN	Safety Network
SVP	Safety Validation Plan
TCP/IP	Transmission Control Protocol/Internet Protocol
UCP	Unit Control Panel
UFD	Utility Flow Diagram
UPS	Uninterrupted Power Supply
PCS	PCS + EMCS
SS	Safety System (SIS + F&G)

For other abbreviations a reference is made to the IEC 61508 standard, part 4.

Copyright © Yokogawa Electric Corporation

1.4 Product certificate for ProSafe-RS

ProSafe-RS is certified by TÜV Rheinland to be used in applications up to and including SIL3 (IEC 61508)



Certificate

Product Safety
Functional Safety

TÜVRheinland
CERTIFIED

www.tuv.com
ID 0600000000

No.: 968/EZ 196.58/24

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, R4.10 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 https://fs-products.tuvasi.com/.		
Codes and standards	IEC 61508 Parts 1-7:2010 IEC 61131-2:2017		IEC 61326-3-1:2017 (non accred.) EN IEC 61000-6-2:2019
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 / Systematic Capability SC 3 acc. to IEC 61508) and can be used in applications up to SIL 3. The product was also reviewed in reference to the applicable requirements of EN IEC 62061:2021, IEC 61511-1:2016 + Corr.1:2016 + AMD1:2017 and EN 50156-1:2015 up to SIL 3. The product meets also the applicable requirements of EN 298:2022, NFPA 72:2022, NFPA 85:2023, NFPA 86:2023 and EN 54-2:1997 + AC:1999 + A1:2006.		
Specific requirements	The instructions of the associated Installation and Operating Manuals shall be considered.		

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/EZ 196.58/24 dated 2024-02-15.
This certificate is valid only for products which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2024-02-16

Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. Jens Hempel

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

Figure 1: TÜV Rheinland certificate for ProSafe-RS

1.5 Hold List

Hold No.	Subject	Reason

Copyright © Yokogawa Electric Corporation

2 Functional Safety Management

2.1 Introduction

The main requirement with respect to Functional Safety Management (FSM) is to assure the execution of all steps of the lifecycle and to record this, so that it can be verified and audited at any time.

- Considering that the IEC 61508 and 61511 standards are internationally accepted in industrial safety nowadays, Yokogawa integrated the standards into the ISO 9001 quality system, which is subject to a periodical audit by a recognised certification body. The result of this integration is the Yokogawa Quality Management System includes an FSM system in accordance with the standards IEC 61508 and 61511.

2.2 The Safety Life Cycle

Requirements on the realisation of safety instrumented systems are given in IEC 61508 part 2 and IEC 61511 Clauses 11, 12 and 13.
Being a system integrator of industrial safety systems, these sections are of most interest in Yokogawa. The needed steps are included in the Yokogawa safety lifecycle model as illustrated in figure 2. This figure presents how Yokogawa has implemented this realisation phase into the organisation. Verification of all steps is done, enabling a continuous monitoring of working practices.

The steps to be taken for the realisation of the project are derived directly from the standard. Following figure 2, the (Basic) Design phase is of most interest. Here the Safety Validation Plan (SVP) will be produced, (this document) which is a comparison between the design and the Safety Requirement Specification (SRS).

The outputs (deliverables) of the realisation steps are called living documents. This means that, when needed, these documents will be updated/revised after any verification (review). After validation the documents are considered as being final.

Include a reference to 61511 par. 8.2.4 - "A Security Risk Assessment shall be carried out [...]". mention the Cybersecurity Risk Assessment performed, the scope and relevance to FSM according to an integrated Security and Safety principle.

Copyright © Yokogawa Electric Corporation

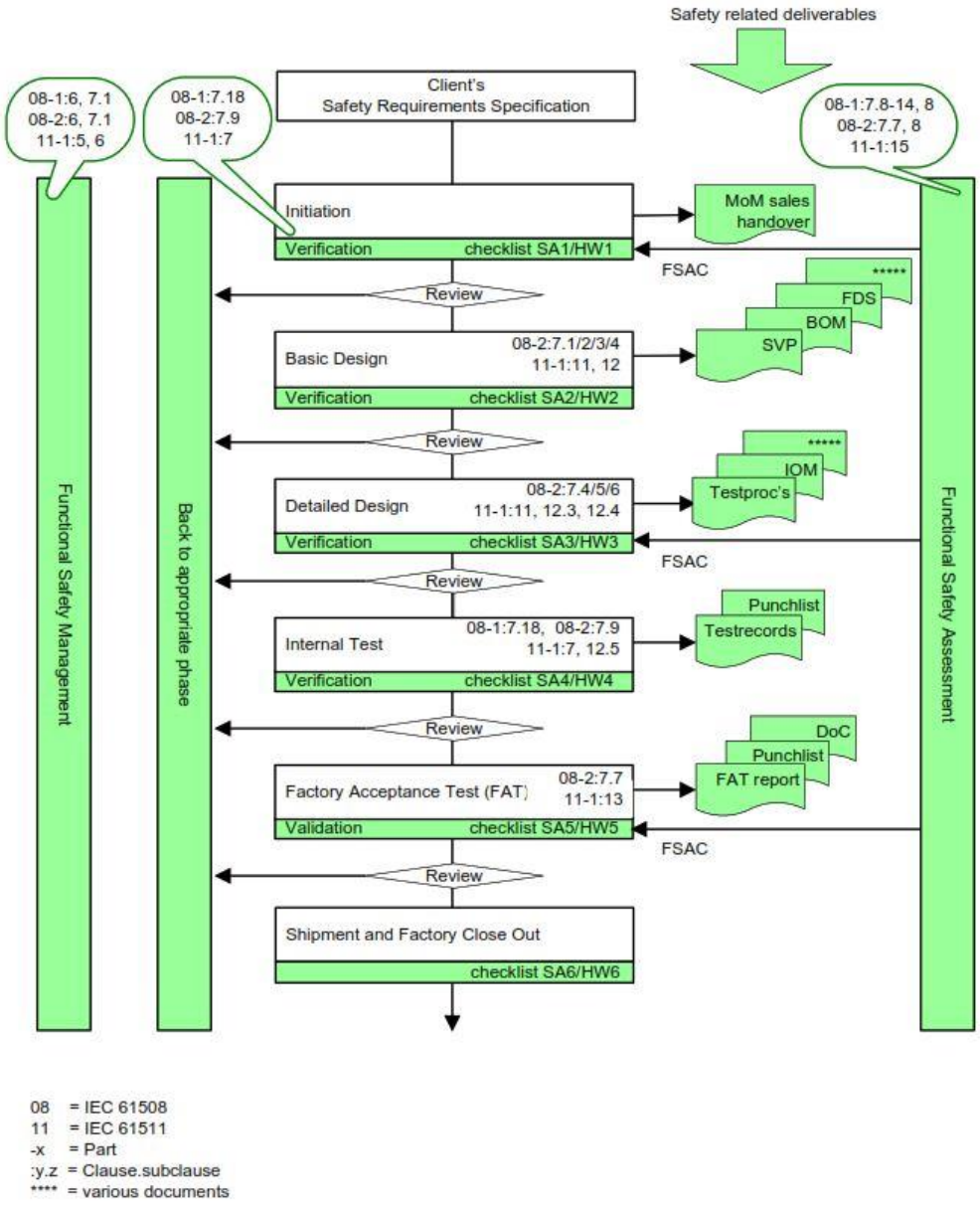


Figure 2: Yokogawa's implementation of the realisation phase of the safety lifecycle

2.3 Safety Verification, Assessment and Validation

2.3.1 Introduction

In accordance with the procedures in the Quality System, safety verification will be an on-going process to fulfil the functional safety requirements during the realisation phase of the project. Because no SIFs and target SILs are provided as part of the SRS or a separate document part of the project specification, no PFDavg calculation will be performed. A table with PFDavg values for the logic solver is provided in section 4.

2.3.2 Verification

Verification will be done by means of document review, visual inspection and system tests. At the end of each project phase a review on deliverables and/or phase-related tests will be carried out. Applicable GES DRCs and phase gate check sheets will used for document reviews and project phase reviews. Verification will be done by a person independent from designer / originator. Details of applicable DRCs and Phase gate check sheets in each phase of the safety lifecycle are referenced in the local FSM procedures. For document review a review log will be kept. Applicable Test Specifications and/or checklists will be used to verify whether the system(s) complies/comply with the design documents.

2.3.3 Functional Safety Assessment

During the realisation of the safety related system usually two safety assessments will be carried out by a functional safety assessor, one after the design phase and one after the FAT. Details depend on the project phase and are defined in the checksheet FSAC. When a check fails, it will be documented in the checksheet. The functional safety assessor will verify the solution of the item during his next assessment.

2.3.4 Validation

The Test procedures combined with applicable test records, and/or checklists will be used to demonstrate the functioning of the system is in accordance with the customer requirement specifications. After the FAT the functional safety assessor carries out a validation assessment to ensure that the system is engineered and tested in accordance with the Quality System and the IEC requirements. At that time, when all outstanding items have been cleared, the FSAC will be signed by the Lead or Project Engineer and the Project Manager and countersigned by the functional safety assessor. Together with the approved SVP, this will be the basis on which the Declaration of Conformance of Functional Safety (DoC(FS)) will be issued. This DoC(FS) will be valid during the life cycle of the system on the condition that the operation and maintenance of the system will be in accordance with the required procedures.
The functional safety assessor is appointed by the GMS-600-14-01-GB and operates independently (which is highly recommended by the IEC 61508 and 61511 standards) from the project execution departments.

2.4 Systematic safety integrity

In IEC 61508 Ed 2 several ways are defined to achieve systematic safety integrity.
Yokogawa will apply Route 1S: avoidance of systematic faults and control of systematic faults.
Yokogawa has their Functional Safety Management system in accordance with the requirements of IEC 61508 and IEC 61511. As such the Yokogawa organisation has a Systematic Capability 3 as per IEC 61508, part 2, 7.4.3.

Copyright © Yokogawa Electric Corporation

2.5 Availability Calculations

As mentioned before, PFDavg calculations are not part of the functional safety assessment. Yokogawa uses the ProSafe-RS Safety Verifier (RSV) to assess the availability of the system. This report provides among others the following assessment results:

- The Mean Time Between Failures: MTBF
- The system (operational) Availability: A

The calculation takes place during the design phase. When necessary, the calculation will be repeated and presented in the re-issued SVP at the next project phases.

2.6 Installation and Commissioning

After delivery the system must be installed and commissioned, after which it can be operated. Yokogawa instructions to be considered for these activities are referred to in 1.2.3.

2.7 Operation and Maintenance

Operation and maintenance is the end-user's responsibility. Yokogawa instructions to be considered for these activities are referred to in 1.2.3. Yokogawa provides the combined document: Instructions for Operation and Maintenance (IOM). This document provides typical maintenance override and system information. The IOM can be used by the client to develop plant maintenance and testing procedures.
The maintenance activities and proof testing shall be executed by safety competent personnel.

2.8 Modifications

For the execution of modifications Yokogawa provides the document: Procedure for Site Modifications and Test (PSMT). The execution of modifications shall be by safety trained and skilled engineers. Safety validation must be done after implementation and testing of the modification on site.

2.9 Decommissioning

De-commissioning will not be Yokogawa's responsibility.

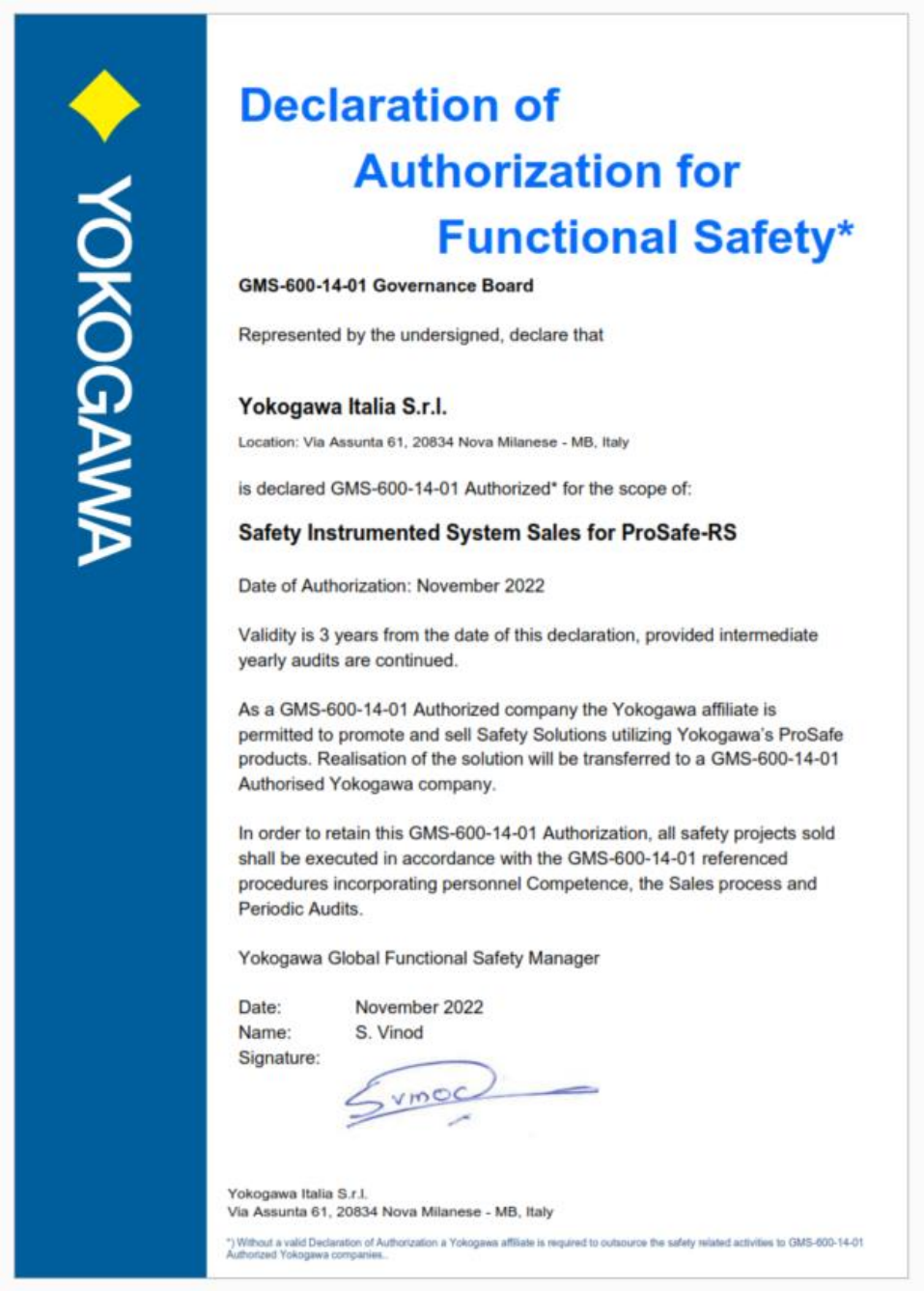
A review of the Cybersecurity Risk Assessment should be mentioned as part of the overall security maintenance lifecycle. Reference eventually to CyberSecurity Design document for specific guidance on relevant systems patching, vulnerability management and other safety-related cybersecurity practice to be considered (as well as Cyber SAT for review and audit security controls).

For modifications, mention the necessity to consider Cybersecurity controls as part of Permit to Work / Management of Change procedures and approval. This should mention which security controls can be disabled or affected by modification tasks.

Copyright © Yokogawa Electric Corporation

2.10 GMS-600-14-01 Authorization

Yokogawa's Governance Board (GMS-600-14-01) has appointed several local Yokogawa Offices worldwide for execution of safety projects. These offices are therefore obliged to have their Local Functional Safety Management System in accordance with IEC 61511 and IEC 61508 and are internally audited every year.
The GMS-600-14-01 Declaration of Authorization for Functional Safety for realization certificate (DoA(FS)R) will indicate which ProSafe products apply to the authorization.
Please note that the FSM system of the local office may be identical to the FSM system of a TÜV Rheinland certified office.



YOKOGAWA

Declaration of Authorization for Functional Safety*

GMS-600-14-01 Governance Board

Represented by the undersigned, declare that

Yokogawa Italia S.r.l.

Location: Via Assunta 61, 20834 Nova Milanese - MB, Italy

is declared GMS-600-14-01 Authorized* for the scope of:

Safety Instrumented System Sales for ProSafe-RS

Date of Authorization: November 2022

Validity is 3 years from the date of this declaration, provided intermediate yearly audits are continued.

As a GMS-600-14-01 Authorized company the Yokogawa affiliate is permitted to promote and sell Safety Solutions utilizing Yokogawa's ProSafe products. Realisation of the solution will be transferred to a GMS-600-14-01 Authorised Yokogawa company.

In order to retain this GMS-600-14-01 Authorization, all safety projects sold shall be executed in accordance with the GMS-600-14-01 referenced procedures incorporating personnel Competence, the Sales process and Periodic Audits.

Yokogawa Global Functional Safety Manager

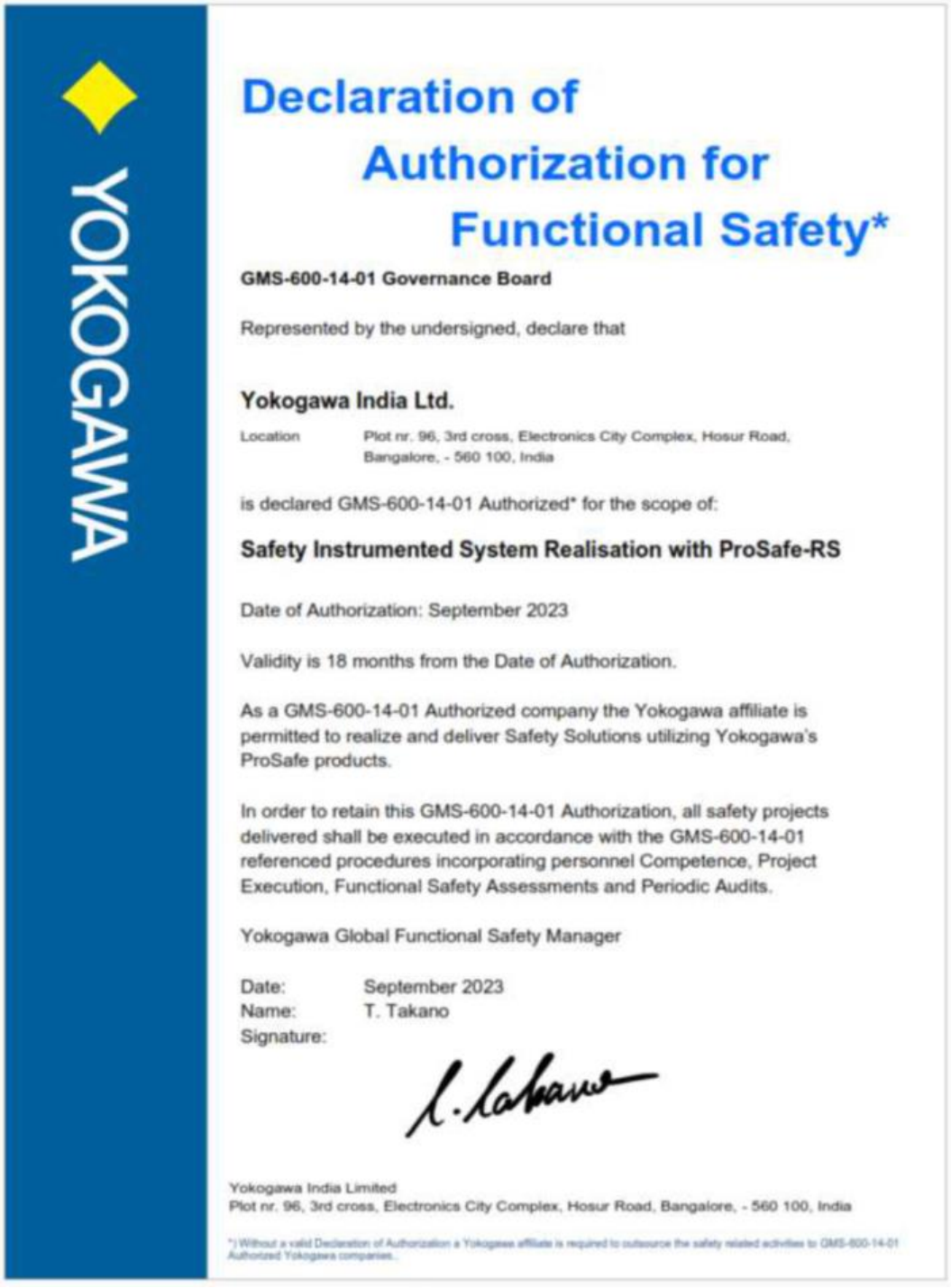
Date: November 2022
Name: S. Vinod
Signature:

Yokogawa Italia S.r.l.
Via Assunta 61, 20834 Nova Milanese - MB, Italy

*) Without a valid Declaration of Authorization a Yokogawa affiliate is required to outsource the safety related activities to GMS-600-14-01 Authorized Yokogawa companies.

Figure 3-A: Declaration of Authorization for Functional Safety certificate (DoA(FS)R)

Copyright © Yokogawa Electric Corporation



YOKOGAWA

Declaration of Authorization for Functional Safety*

GMS-600-14-01 Governance Board

Represented by the undersigned, declare that

Yokogawa India Ltd.

Location Plot nr. 96, 3rd cross, Electronics City Complex, Hosur Road, Bangalore, - 560 100, India

is declared GMS-600-14-01 Authorized* for the scope of:

Safety Instrumented System Realisation with ProSafe-RS

Date of Authorization: September 2023

Validity is 18 months from the Date of Authorization.

As a GMS-600-14-01 Authorized company the Yokogawa affiliate is permitted to realize and deliver Safety Solutions utilizing Yokogawa's ProSafe products.

In order to retain this GMS-600-14-01 Authorization, all safety projects delivered shall be executed in accordance with the GMS-600-14-01 referenced procedures incorporating personnel Competence, Project Execution, Functional Safety Assessments and Periodic Audits.

Yokogawa Global Functional Safety Manager

Date: September 2023
Name: T. Takano
Signature:

Yokogawa India Limited
Plot nr. 96, 3rd cross, Electronics City Complex, Hosur Road, Bangalore, - 560 100, India

*) Without a valid Declaration of Authorization a Yokogawa affiliate is required to outsource the safety related activities to GMS-600-14-01 Authorized Yokogawa companies.

Figure 3-B: Declaration of Authorization for Functional Safety certificate (DoA(FS)R)

Copyright © Yokogawa Electric Corporation

2.11 TÜV Rheinland Certification

On top of the GMS-600-14-01 authorization, several offices have applied for individual certification by TÜV Rheinland for having their Functional Safety Management system in accordance with IEC 61511 and IEC 61508:

- Yokogawa Europe Solutions B.V, The Netherlands
- Yokogawa Romania, Bucharest
- Yokogawa Industrial Safety Systems Sdn. Bhd., Malaysia
- Yokogawa India Ltd, Bangalore
- Yokogawa Engineering Asia Pte Ltd, Singapore
- Yokogawa Electric International Pte Ltd, Singapore
- Yokogawa Middle East & Africa B.S.C. (c), Kingdom of Bahrain
- Yokogawa Corporation of America
- Yokogawa Electric Korea Co. Ltd.
- Yokogawa Solution Service Corporation, Japan

Information can be found on the TÜV Rheinland website:
https://www.tuv.com/world/en/functional-safety-management-certification.html

Copyright © Yokogawa Electric Corporation



Certificate

Functional Safety Management

FS Management (TÜV Rheinland)
IEC 61511-1:2016 - SIS Integration (Phase 4)
FSM 104

Certificate No. **968/FSM 104.20/22**

Certified Company & Location
Yokogawa Europe Solutions B.V.
Euroweg 2
3825 HD Amersfoort
The Netherlands

YOKOGAWA

Scope of Certification
Safety Instrumented Systems Integration, related to IEC 61511-1:2016 - Phase 4 (Design & Engineering)

The certified company has successfully demonstrated during an audit process that a Functional Safety Management System has been implemented and applied accordingly.

Maturity Level confirmed is **Maturity Level 4 (ML4) - "Improved – Quantitatively Managed"**.

The Scope of Certification **SIS Integration** covers integration of **Safety Instrumented Systems (limited to Logic Solver)** for the **Process Industry** up to and including **Safety Integrity Level 3 (SIL3)** and **Systematic Capability 3 (SC3)**.

The following phase activities are considered: **SIS design, configuration, application programming, assembly** and **test** as well as **safety loop calculations**.

The IEC 61511 is the basic standard for this FSM Certification; however relevant clauses of the **IEC 61508:2010** standard are used complementarily.

As part of the audit process organizational and informational exchange / supply related to other respective Safety Lifecycle Phases between the Certified Company and its customer is considered.
This FSM Certification only refers to the listed company locations and their involved departments, which comply with the organizational FSM requirements for the listed Scope of Certification. It does not replace approval or certification for specific SIS Integrations.

Validity This certificate is valid until 2024-04-30

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Cologne, 2022-06-17

Dipl.-Ing. (FH) Wolf Rückwart

TÜV Rheinland
Industrie Service GmbH
Automation and Functional Safety
Am Grauen Stein
51105 Cologne - Germany

Certification Body Safety & Security for Automation & Grid
Further information referring to the scope of certification, see http://www.tuvasi.com

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

10/222 12.12 E A4 ® TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval.

Figure 4-A: TÜV Rheinland FSM certificate

NOTE: TUV Audit has successfully completed. Renewed Certificate shall be replaced in next revision.



Certificate

Functional Safety Management

FS Management (TÜV Rheinland)
IEC 61511-1:2016 - SIS Integration (Phase 4)
FSM 115

Certificate No. 968/FSM 115.15/21

Certified Company & Location
Yokogawa India Ltd.
Plot No. 96, 3rd Cross Electronics City Complex
Hosur Road
Bangalore 560 100
India

YOKOGAWA

Scope of Certification
Safety Instrumented Systems Integration, related to IEC 61511-1:2016 - Phase 4 (Design & Engineering)

The certified company has successfully demonstrated during an audit process that a Functional Safety Management System has been implemented and applied accordingly.

Maturity Level confirmed is **Maturity Level 4 (ML4) - "Improved – Quantitatively Managed"**.

The Scope of Certification **SIS Integration** covers integration of **Safety Instrumented Systems (limited to Logic Solver)** for the **Process Industry** up to **Systematic Capability (SC3)** and **Safety Integrity Level 3 (SIL3)**.

The following phase activities are considered: **SIS design, configuration, application programming, assembly** and **test** as well as **safety loop calculations**.

The IEC 61511 is the basic standard for this FSM Certification; however relevant clauses of the **IEC 61508:2010** standard are used complementarily.

As part of the audit process organizational and informational exchange / supply related to other respective Safety Lifecycle Phases between the Certified Company and its customer is considered.

This FSM Certification only refers to the listed company locations and their involved departments, which comply with the organizational FSM requirements for the listed Scope of Certification. It does not replace approval or certification for specific SIS Integrations.

Validity This certificate is valid until 2024-11-30

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Cologne, 2021-11-29

Dipl.-Ing. (FH) Wolf Rückwart

TÜV Rheinland
Industrie Service GmbH
Automation and Functional Safety
Am Grauen Stein
51105 Cologne - Germany

Certification Body Safety & Security for Automation & Grid
Further information referring to the scope of certification, see http://www.tuvasi.com

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

Figure 4-B: TÜV Rheinland FSM certificate

Copyright © Yokogawa Electric Corporation

3 Safety Requirements - Safety Solutions

3.1 Introduction

The verification of the system design is carried out by comparing it with the safety requirements, as explained before. The comparison is based on splitting up the safety requirements into a number of significant items, such as logic solver integrity level, field interfaces, etc., which is presented in section 3.4.

3.2 Safety Requirement Specification

IEC61511-1 (2016) requires a description of all the SIFs necessary to achieve the required functional safety. In this case client did not specify any SIFs. The relevant safety requirement items of the system are derived from the specification document refer section 1.2.2 [a].

3.3 System Design

3.3.1 System Overview

BLPH is intended to be a greenfield platform whose purpose is to balance the power supply from HKN wind farm primarily through hydrogen generation and storage. The platform shall provide short-term energy storage through a BESS and long-term energy production and storage by producing and storing green hydrogen through electrolysis.

The facility shall receive power by external means from the Dutch grid (through the HKN wind park) and a floating solar farm. The facility is directly coupled to WTG57 through an inter array cable string that connects to the Dutch grid.

Power production from BLPH will be governed by the real-time forecast out data signals coming from Wind.

Turbine Generator number 57 (WTG57).

Additionally, BLPH shall receive power from an external floating solar farm, by others.

The PACO control system developed for BLPH shall comprise of two (2) interconnected, but independent systems:

- A Central Control System (PCS); and
- A combined Fire and Gas System (FGS) and Safety Instrumented System (SIS), which shall be referred to collectively as the Safety System.

The PCS shall be responsible for the monitoring and control of the facility, whilst the Safety System shall be responsible for the overall safeguarding of BLPH.

The wind farm system is operated by an independent SCADA system called CI Server (Collaborative Information Server). The PCS and the Safety System shall operate independently but shall interface fully with the CI Server. via the Vnet/IP Yokogawa network.

Yokogawa's Integrated Control and Safety System consists of Operator Workstations, Engineering Workstations, Field Control Stations, Safety Control Stations, etc., connected via the Vnet/IP control bus and collectively call a domain. PCS, SIS, FGS and CI server will be in same domains depending on the total number of stations and/or process segregation (or other) requirements.

Copyright © Yokogawa Electric Corporation

Domain segregation is as below,

Domain/Station	System
SCS0110	SIS
SCS0120	FGS

Table 1 – Domain Segregation

Refer Attachment-1 for PACO network configuration and major components is shown in the overall System Architecture Drawing (Doc No - 1724000594-IN-DD-00015).

3.3.2 Design Principles

Safety Instrumented System (SIS) / Fire and Gas (FGS) Design is based on the following principles:

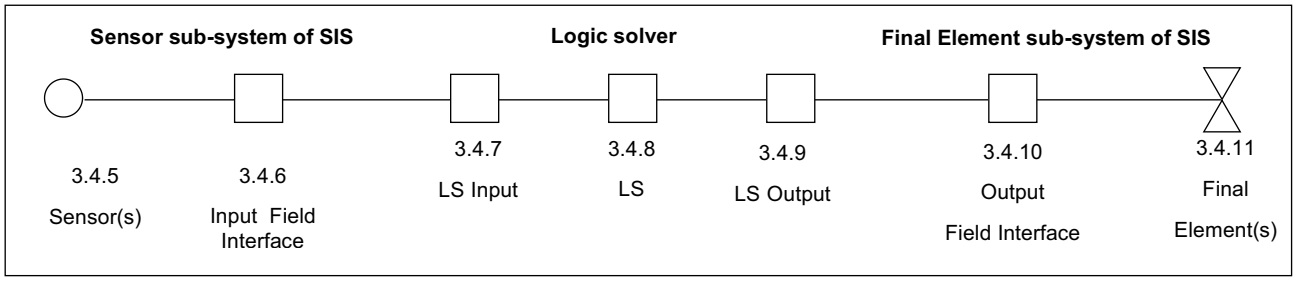
- The scan time of the SIS and FG logic solver shall be a maximum of 300 msec and 500msec.
- Integrated PCS, SIS and FGS with CI server SCADA function.
- Sequence of events (SOE) recording and analysis via CI server (In build Historian) and EWS.
- The SIS shall be fail-safe, normally energized, de-energized to trip and any energise to trip SIS/FGS field circuits shall be continuously line monitored by the system for fault conditions, i.e., device faults, open and short circuit faults, etc. EPC to provide detailed information.
- Proof test will be standardized, the test intervals for proof testing the sensors, logic solver and final elements shall be detailed out by the EPCC contractor.
- SIS/FGS shall create “First up fault” alarm that allow control room operator to quickly interrogate trips through HMI with one Keystroke.
- Each SIS/FGS input shall have the facility for a maintenance inhibit to enable testing without causing a shutdown. The inhibits shall be selected and applied through the operator workstation displays. The inhibit shall only become active when the CAP is enabled. The inhibit state shall be indicated on the SIS/FGS Graphic displays. Input inhibits shall only affect SIS/FGS logic, not input alarming, i.e., inhibited inputs shall alarm to the operator.
- The FGS will be designed as a normally de-energized system with line monitoring (as per input from EPC on requirements of line monitoring functionality, including discrete alarm inputs, such as detector or manual call points).
- All relevant subsystems and Field I/O shall interface with FGS through hardwired signals.
- Any single system fault shall not cause unwanted and unsafe actions, and such faults shall be revealed on occurrence.
- Every possible dangerous failure (fault detected only when the system is called upon to operate), which shall prevent an executive action from taking place in the event of a genuine trip input, shall be identified and exterminated.
- No single fault shall prevent the entire system from working normally i.e. no common mode failures.

Copyright © Yokogawa Electric Corporation

- Replacement of I/O modules shall not require any kind of bypassing, either in hardware or software. To achieve such capability, it shall not be necessary to externally wire inputs and outputs to multiple I/O modules. Programming must be for the single I/O point only. Explicit programming of voting and module replaceability shall be unacceptable.
- Input and output signals shall be voted independently. The output-voting network shall be automatically tested at a regular interval.
- Maintenance inhibits, with only one input to any voted system being allowed to be overridden at any one time (Maintenance overrides shall not be provided on output devices).
- The FGS shall have the capability of on-line software download from the programming terminal without shutdown of the process. This capability shall be approved by EPC for class SIL 3 applications. Live/On-line download shall require security password to avoid unauthorized access.
- The FGS shall be provided with redundant communication and processor architecture to provide uninterrupted automatic Fire & Gas Detection and Protection and increased reliability.
- The FGS shall seamlessly interface with the PCS system. This will allow the operator to monitor the Fire & Gas detection status of the entire OGP Complex via PCS operator consoles located in the CCR.
- Fire protection operator commands (e.g. starting fire water pumps, initiating extinguishing agent discharge, deluge system, etc.) that may be required in case of black out of all operator workstations.
- The FGS system hardware will be separated from all other control and safety systems (PCS, SIS, etc.) and will not require the correct operation of any other system to fulfil its own function. However, to optimize facilities spare inventory and ease maintenance, the FGS shall use the same hardware as the SIS system.

Further detailed information on the system is given in the FDS (E366772C00-FDS_SW).

3.4 Requirements versus Solutions



Model to clarify the used terms

3.4.1 Safety Instrumented Functions/Loops

Requirement	Solution
No Safety Instrumented Functions (SIFs) with SIL targets are specified by the client.	A quantitative assessment (PFDavg calculation) is not carried out as there is no customer specified safety requirement for the project. General PFDavg values for the logic solver can be found in section 4.

3.4.2 Safety Parameters

Requirement	Solution
Logic solver ▪ SIL = 3 (Refer section 1.2.2. [a])	The ProSafe-RS is certified by TÜV Rheinland for use in applications up to and including SIL3 according to IEC 61508. See 1.4.
▪ Proof test interval T = n.s.	Proof test interval of 1 year is assumed for the calculation purpose.
Overall ▪ System life time T_L = n.s	System Life Time TL of 10 year is assumed for the calculation purpose.

Copyright © Yokogawa Electric Corporation

3.4.3 Safety Related Parameters

Requirement	Solution
▪ System availability A = n.s ▪ MTTR = n.s ▪ MTBF = n.s ▪ LS scan time = n.s ▪ LS response time = n.s ▪ Process safety time = n.s	See section 4.3 for the availability calculation result. MTTR of 8 hours is assumed for the calculation purpose. The SIS & FGS ProSafe-RS scan time is set to 300msec and 500msec respectively. The SIS ProSafe-RS response time is (worst case) twice the scan time, being 300 msec scan time, LS Response time is 600 msec. The FGS ProSafe-RS response time is (worst case) twice the scan time, being 500 msec scan time, LS Response time is 1000 msec. For SIS to FGS SCS Link transmission safety communication, Transmission delay is 100 ms. The LS response time is (Considering Link transmission communication) Sender Tscan x 2 + Receiver Tscan x 2 + Transmission Delay, which is 300 x 2 + 500 x 2 + 100 = 1700 msec For FGS to SIS SCS Link transmission safety communication, Transmission delay is 100 ms. The LS response time is (Considering Link transmission communication) Sender Tscan x 2 + Receiver Tscan x 2 + Transmission Delay, which is 500 x 2 + 300 x 2 + 100 = 1700 msec Yokogawa is only responsible for the SIF response time with respect to logic solver and interfaces. However this SIF response time is mostly determined by the selection of the sensors and final elements. It is client responsibility to check the SIF response time with the inclusion of sensors and valves against the process safety time.

Copyright © Yokogawa Electric Corporation

3.4.4 Segregation

Requirement	Solution
Functional separation: ▪ Subsystems: n.s ▪ BPCS: Yokogawa Centum VP	SIS and FGS Systems are implemented in separate controllers. The Prosafe-RS is integrated over Vnet/IP network with Centum-VP, EMCS and CI serve. CI server is used to control and monitor the status on SCADA.
Galvanic isolation: ▪ I/O-groups: n.s ▪ SIS I/O channels: n.s ▪ FGS I/O channels: Yes (Refer section 1.2.2. [e]))	For FGS - AI IS signal barriers (Smoke Detector Signals) are used & For SIS - DO VFC IO's are used. Barriers and Relays are assigned based on customer Instrument I/O List (123A90-DDL-IN-LIS-40089) requirement. Based on FGS C&E, voting has segregated with different channel/module.
▪ Power supplies: Power supplies shall be considered for system, IS barriers and field instruments.	SIS and FGS Marshalling Cabinets are equipped with external 24VDC Redundant Power Supply units which serve as external source for Terminal Boards.

3.4.5 Sensors

Requirement	Solution
▪ Analogue: 4-20mA with HART ▪ Digital: VFC and NO/NC contacts ▪ Type transmitters: Pressure	The sensors are not in the scope of supply and not included in the safety assessment.
▪ FGS Safety architecture: Yes	Based on FGS, Refer section 1.2.2. [f], voting signals has segregated.
▪ SIS Safety architecture: n.s	

Copyright © Yokogawa Electric Corporation

3.4.6 Input Field Interfaces

Requirement	Solution
▪ IS isolators/barriers: Yes (Refer section 1.2.2.[d])	Following IS Barriers are used for FGS system: Make: P&F Model: P+F - HIC2025 IS barrier for AI
▪ Signal splitters: n.s	No Signal Splitters are used.
▪ HART interfaces: n.s ▪ Interposing relays: n.s	
▪ Line monitoring: Yes	Diagnostics included: Yes Line Monitoring will be achieved for IS and NIS signal up to the System from Field. Isolators used for DI and AI have pass through capability for line monitoring. For SIS & FGS Line monitoring has enabled based on customer Instrument I/O List (123A90-DDL-IN-LIS-40089) Safety certificates and/or safety manuals of the applied interfaces are included in Appendix II.

Copyright © Yokogawa Electric Corporation

3.4.7 LS Input Channels

Requirement	Solution
▪ Analogue: 4-20mA with HART	SAI143-H is used for all Analogue Inputs. Analogue inputs module SAI143-H are HART compatible. Analogue Input barriers used are HART compatible.
▪ Digital: VFC and NO/NC contacts	SDV144 is used as Digital Input Card. All Digital Inputs to the system are potential free contacts.
▪ Line monitoring: Yes	Line Monitoring for AI is enabled at IO Parameter builder using Detect IOP. Line Monitoring for DI enabled at IO Parameter for NO signals using Detect disconnection and Detect short Circuit. Diagnostics included: Yes For Analog inputs, line monitoring shall be provided by configuring over and under range using ProSafe-RS IO parameter builder. For Non-IS digital inputs, line monitoring shall be provided by using Yokogawa SCB100 and SCB110 end of line devices. For SIS & FGS Line monitoring has enabled based on customer Instrument I/O List (123A90-DDL-IN-LIS-40089)
▪ Fusing: n.s	Fuse terminal provided for the field input (NIS signal) for AI 250 mA and for DI 250 mA fuse.

3.4.8 Logic Solver(s)

Requirement	Solution
▪ Dual Inputs ▪ Dual CPU ▪ Dual Outputs	ProSafe-RS is used in a configuration with dual Inputs, dual CPU and dual Outputs. The safety manuals of the ProSafe-RS are included in the Workbench installation package.

Copyright © Yokogawa Electric Corporation

3.4.9 LS Output Channels

Requirement	Solution
▪ Power: 24VDC ▪ Lamp driver: n.s	SDV541 module is used for the DOs of the Safety Systems.
▪ VFC:Yes (Refer section 1.2.2. [a] and [c])	Relays are used to provide volt free contact to interface signals.
▪ Line monitoring: Yes	Diagnostics included: Yes Line diagnostics (detect disconnection / short circuit) will be enabled for Normally De-energized DO signals. Field DO's are Line monitored up to the field Device. For SIS & FGS Line monitoring has enabled based on customer Instrument I/O List (123A90-DDL-IN-LIS-40089) Wherever relays are used for any Digital Outputs, then Line Monitoring shall be provided only up to Relay Coil and not up to the field device.
▪ Fusing: n.s	

Copyright © Yokogawa Electric Corporation

3.4.10 Output Field Interfaces

Requirement	Solution
▪ IS isolators/barriers: n.s	Interposing relay used for SIS Interface signals. Make: P&F Model: KFD0-RSH-1.4S.PS2
▪ Interposing relays: Yes	Relays are used to provide volt free contact to interface signals.
▪ Line monitoring: Yes	Diagnostics included: Yes Line diagnostics (detect disconnection / short circuit) will be enabled for Normally De-energized DO signals. Field DO's are Line monitored up to the field Device. Wherever relays are used for any Digital Outputs, then Line Monitoring shall be provided only up to Relay Coil and not up to the field device. Safety certificates and/or safety manuals of the applied interfaces are included in Appendix II
▪ Fusing: n.s ▪ Surge protection: n.s	

3.4.11 Final Elements

Requirement	Solution
▪ Solenoid(s): Yes Safety architecture: n.s ▪ Valve(s): Yes Safety architecture: n.s Is Partial Stroke testing applied: NO ▪ Contactors: n.s Safety architecture: n.s ▪ Alarms indicators: n.s Safety architecture: n.s	The final elements are not in the scope of supply and not included in the safety assessment.

Copyright © Yokogawa Electric Corporation

3.4.12 Overrides and Inhibits

Requirement	Solution
▪ Input overrides: Yes (Refer section 1.2.2. [a]),section 6.5) ▪ Input inhibits: n.s ▪ Output overrides: n.s	**MAINTENANCE OVERRIDE FUNCTION**: 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 with only one and not for output signals. Maintenance overrides should not prevent actual input status from being alarmed.
▪ Start up override: Yes ▪ (Refer section 1.2.2. [a]), section 6.5)	**START UP OVERRIDE:** The start-up overrides shall normally be automatic reset type. Some services will require manual start up overrides. Failure of a start-up override to reset shall be alarmed to the operator. Whenever an override is placed the safety function in question no longer offers protection. Operational precautions must be taken in line with the requirements of the standards. This is not in Yokogawa's scope or responsibility.
▪ Override groups: n.s ▪ HW override: …n.s ▪ Override from BPCS: n.s ▪ Override enable: n.s	

Copyright © Yokogawa Electric Corporation

3.4.13 Environment

Requirement	Solution
Environmental conditions and EMC requirements, as per client specification. In the event of a failure of the HVAC system the conditions will be more severe. The equipment shall therefore be designed to operate under the following conditions: • Design Temperature range: 5 to 45 ºC • Design Relative Humidity :10 to 93% RH	ProSafe-RS modules are Compliant with the requirements (Refer Hardware FDS). ProSafe-RS Hardware: Temperature: -20 to 70˚C and Relative humidity: 5 to 95% EMC Compliance meets EN55011, Class A, Group 1, EN61000-6-2, EN61000-3-2, EN61000-3-3 - RFI is 10 V/m maximum (80 MHz to 1 GHz) Power supply and Diode unit: Puls:Temperature: -25 to 70˚C (>60 derating) Relative Humidity: < 95% (at 25˚C, no condensation) Isolator: Temperature: -40 to 70˚C and Relative humidity: 5 to 95% (at 25˚C, no condensation) EMC Compliance: EN61326 Safety Relay: Temperature: -20 to 60˚C Relative humidity: 5 to 95% (at 25˚C, no condensation) The SIS & FGS System and Marshalling cabinets are designed to operate at an optimal temperature of 26°C. In the event of HVAC failure, internal temperature exceeds this threshold, a temperature alarm will be triggered, requiring immediate attention and corrective action by the operator to restore safe operating conditions.

Copyright © Yokogawa Electric Corporation

3.4.14 Communication Interfaces

Requirement	Solution
▪ BPCS communication: Yes (Refer section 1.2.2. [a]), section 6.7)	All the stations on the V-net/IP platform will be connected and communication with each other via redundant Vnet/IP. No safety related information will be communicated over this connection.
	No subsystem interface via Modbus communication is applicable in this project
	Remote I/O Communication is not used in this project
	Critical Action Panel (CAP) IO's are provided as software based IO's as part of SCADA/HMI (CI View). It consists of soft signals pushbutton, switches and lamps.
▪ Comm. between sub-systems: n.s ▪ Remote I/O communication: n.s ▪ Matrix panels: n.s ▪ Mimic panels: n.s	

3.4.15 Application Programming

Requirement	Solution
▪ Ladder diagram, acc. IEC 61131-3: n.s	The ProSafe-RS engineering tools and application programming (Ladder diagram, Function block and Structured text), are approved by TÜV Rheinland (ref. ProSafe-RS Safety Manual and Engineering guide) and are in accordance with IEC 61131. In this system FB programming is used.
▪ Function blocks, acc. IEC 61131-3: Yes (Refer section 1.2.2. [a]), section 6.4)	For the obvious non-safety related application logic function blocks/parts may be used which is not part of the SIL3 certified function block library. Examples of obvious non-safety related application logic are: Totalizers, Alarms, Diagnostics, Matrix panel outputs etc.
▪ Structured text, acc. IEC 61131-3: n.s	

Copyright © Yokogawa Electric Corporation

3.4.16 Security

Requirement	Solution
To protect against cyber-attacks it is required to	
▪ Install a switch to inhibit downloads: Yes	A hardwired (key) switch has been implemented to inhibit changing the security level of the SIS so that an unauthorised download to a ProSafe-RS controller is prevented
▪ Install a virus scanner: Yes	Virus scanner provided in all PC.
▪ Install a firewall:Yes (Refer section 1.2.2. [a]), section 7)	Firewall deployed between control (PCS) and safety(SIS and FGS) network.

Copyright © Yokogawa Electric Corporation

4 Safety Assessment Notes for the SIS system

4.1 Introduction

In 3.4.1 and 3.4.2 it was concluded that no Safety Instrumented Functions are specified.

One of the few safety related specifications is “Safety PLC to be SIL 3 compliant”
The ProSafe-RS logic solver meets that specification (see 1.4).

4.2 Safety Architecture

As no SIFs are specified Yokogawa has no possibilities to assess the hardware fault tolerance. Whenever certain SIL requirements arise the hardware fault tolerance has to be re-assessed.

4.3 Reliability Calculations

4.3.1 Scope

As no SIFs are specified Yokogawa has no possibilities to assess the PFDavg in detail.

For reference, typical values for the PFDavg of the logic solver can be found in 4.3.2

Based on the assumptions and restrictions as indicated in this SVP the Availability of the logic solver has been calculated using the Yokogawa RSV tool.

4.3.2 Results

Typical values for the PFDavg of the logic solver, based on one year proof test interval, can be found in the table below.

Loop structure	Input	CPU	Output	PFDavg
DI－CPU－DO	SDV144	S2CP471	SDV541	6.623E-07
AI－CPU－DO	SAI143-H	S2CP471	SDV541	6.754E-06

The results of the Availability calculations can be found in the calculation report (appendix 1)

Availability of logic solver (excluding field interfaces): 99.99996
Availability of logic solver (including field interfaces): 99.99991

Copyright © Yokogawa Electric Corporation

5 Safety Assessment Notes for FGS Systems

5.1 Introduction

In 3.4.1 and 3.4.2 it was concluded that no Safety Instrumented Functions for FGS are specified.

Since FGS are mainly mitigation systems, where both sensor coverage and human factor are dominant, no assumed loops are considered for calculation purposes.

One of the few safety related specifications is “Safety PLC to be SIL 3 compliant”
The ProSafe-RS logic solver meets that specification (see 1.4).

5.2 Safety Architecture

As no SIFs are specified Yokogawa has no possibilities to assess the hardware fault tolerance. Whenever certain SIL requirements arise the hardware fault tolerance has to be re-assessed.

5.3 Reliability Calculations

5.3.1 Scope

As no SIFs are specified Yokogawa has no possibilities to assess the PFDavg in detail.

For reference, typical values for the PFDavg of the logic solver can be found in 5.3.2

Because no target for Availability has been specified, calculations have not been performed.

5.3.2 Results

Typical values for the PFDavg of the logic solver, based on one year proof test interval, can be found in the table below.

Loop structure	Input	CPU	Output	PFDavg
DI－CPU－DO	SDV144	S2CP471	SDV541	6.623E-07
AI－CPU－DO	SAI143-H	S2CP471	SDV541	6.754E-06

The results of the Availability calculations can be found in the calculation report (appendix 1)

Availability of logic solver (excluding field interfaces): 99.99993
Availability of logic solver (including field interfaces): 99.99680

Copyright © Yokogawa Electric Corporation

Appendix I

Availability Calculation results for SIS

Number of pages that follow: 2

Copyright © Yokogawa Electric Corporation

6 Miscellaneous

Reliability Data
Yokogawa's independent group of Functional Safety specialists has assessed the reliability data from manufacturers of devices and prepared a Reliability Datasheet per device with reliability data to be used in the calculations performed by Yokogawa.
Yokogawa's approach is to use the reliability data provided by manufacturers of devices in a conservative way, thus minimizing the chance of a too optimistic calculation.

Installation
All installation instructions as stated in the Installation Manuals, Instructions for Operation and Maintenance Manuals and/or Safety Manuals have to be followed up to ensure the validity of their associated failure rates.

Proof Testing
Procedures for testing of Yokogawa's logic solver can be found in the Instructions for Operation and Maintenance. It is end-user's responsibility to execute the tests and to keep records thereof.

System alarms
System alarms like line fault message, module failures, etc. have to be followed up by operators and/or maintenance engineers. Procedures for this must be developed by the end-user, some guidance for the Yokogawa equipment can be found in the Instructions for Operation and Maintenance.

Configurable system parts
For all configurable system parts, such as transmitters (HART), protection against unauthorised modification should be used at all times.

Life time restrictions
An overall life time has been specified in section 3.4.2. For certain, mostly mechanical, devices a shorter life time might apply. It is end-user's responsibility to identify and replace these devices at the end of their specified life time to ensure the validity of their associated failure rates. The Yokogawa Power supply modules in the rack have an expected life time of 8 years. The replacement of devices within the expected life time will not affect the associated failure rates and the overall life time of the SIS.

Overrides
The human factor will not be included in the Yokogawa reliability calculations. As a consequence unsafe operating of overrides as far as they may be caused by mistake and/or wrong procedures are not part of the safety assessment.

7 Modifications

This section is not applicable yet.

End of document

Copyright © Yokogawa Electric Corporation

ProSafe-RS Reliability Calculation

tool info : revision 16

Project: Base Load Power Hub (BLPH)
SCS0110

Rev: 00

Date: 23-08-2024

Author: Manojkumar P

1. Availability

System configuration

Model name	Model type	Single	Duplex
		Number of modules	Number of Duplex sets (=1/2 # of modules)
Digital Input Module	SDV144		5
Digital Output Module (8ch, 24VDC)	SDV531-S/L		
Digital Output Module (8ch, 48VDC)	SDV53A		
Digital Output Module (16ch, 24VDC)	SDV541		4
Digital Output Module (4ch, 24VDC)	SDV521		
Digital Output Module (4ch, 100VAC)	SDV526		
Analog Input Module (4～20mA)	SAI143-S		
Analog Input Module (4～20mA, with HART)	SAI143-H		1
Analog Input Module (1-5V/1-10V)	SAV144		
Analog Input Module (mV/TC)	SAT145		
Analog Input Module (RTD)	SAR145		
Analog Output Module (4～20mA, with HART)	SAI533		
Analog Digital I/O Module (Analog Input 2-wire)	S2MMM843 AI 2Wire		
Analog Digital I/O Module (Analog Input 4-wire)	S2MMM843 AI 4Wire		
Analog Digital I/O Module (Analog Output)	S2MMM843 AO		
Analog Digital I/O Module (Digital Input)	S2MMM843 DI		
Digital I/O Module (Digital Input)	S2MDV843 DI		
Analog Digital I/O Module (Digital Output)	S2MMM843 DO		
Digital I/O Module (Digital Output)	S2MDV843 DO		
Fire and Gas Communication Module	S2LP131		
Safety Control Unit (Single CPU for V net)	SSC10S		
Safety Control Unit (Dual redundant CPU for V net)	SSC10D		
Safety Control Unit (Single CPU for Vnet/IP)	SSC50S		
Safety Control Unit (Dual redundant CPU for Vnet/IP)	SSC50D		
Safety Control Unit (Single CPU for Vnet/IP)	SSC57S		
Safety Control Unit (Dual redundant CPU for Vnet/IP)	SSC57D		
Safety Control Unit (Single CPU for Vnet/IP)	SSC60S / S2SC70S (SCP461)		
Safety Control Unit (Dual redundant CPU for Vnet/IP)	SSC60D / S2SC70D (SCP461)		
Safety Control Unit (Single CPU for Vnet/IP)	SSC60S / S2SC70S (S2CP471)		
Safety Control Unit (Dual redundant CPU for Vnet/IP)	SSC60D / S2SC70D (S2CP471)	1	
Safety Node Unit	SNB10D / S2NN30D	2	
Unit for Optical Bus Repeater Module	SNT10D		
Optical ESB Bus Repeater Master Module (! Enter 1/2 #of Mdl) *1	SNT401/411		

*1 Failure rates of SNT501/511 are automatically calculated.

Parameters

Proof test interval (T) : 1 **years** 8760 **hours**

Mean Time To Restoration (MTTR) : 8 **hours**

Results

Availability: 99.99996 **%**

MTBFspurious: 2534.78 **years**

General Reliability Configurator™ for SIS
DTS: De-energize To Safe state

YOKOGAWA
Safety Assurance and Consultancy

tool info : revision 18.4
custodian: SA
© 2019 Yokogawa Europe B.V.

project no.:	E366772C00	system:	SCS0110
project name:	Base Load Power Hub (BLPH)	sub-system:	SIS System
	SCS0110	scope:	Overall System Availability
client name:	ROSETTI MARINO S.p.A	revision no.:	00
client P.O. no.:	CW-I-WP4-2023-05	executed by:	Manojkumar P
end user name:	Crosswind Hollandse Kust Noord	date:	23-08-2024

assumptions:

legend

MTBF = mean time between failure
MTTR = mean time to restoration
FTR = false trip rate
I/O = input / output
SE = sensor element
LS = logic solver
FE = final element

Normally sensors and final elements are not included in availability calculations unless specified.

calculation scope

- ☐ sensor(s)
- ☐ SE interface(s)
- ☑ LS incl. I/O module(s)
- ☑ FE interface(s)
- ☐ final element(s)

inputs

result from ext. calc.
MTBF (year)

ProSafe-RS availability
99.99996 %

	FTR		MTBF		availability	
targets		1/year		year		%
set MTTR	8	hour				

results

	FTR		MTBF		availability	
	0.00	1/year	992.35	year	99.99991	%
	1.150E-01	E-6/hr				
targets met?	n.a		n.a		n.a	

manufacturer	model	Type (A/B)	failure rates per circuit (E-6/hr)			total number of circuits for SIS Availability calculation, based on below voting principles					
			λ_S	λ_{Dd}	λ_{Du}	1oo1	1oo2	1oo3	2oo2	2oo3	2oo4
Final Element Interface Modules											
P&F	KFD0-RSH-1.4S.PS2 (1oo1)	A	3.50E-02	0.00E+00	1.83E-03	2					

Availability Calculation results for FGS

Number of pages that follow: 2

Copyright © Yokogawa Electric Corporation

ProSafe-RS Reliability Calculation

tool info : revision 16

Project: Base Load Power Hub (BLPH)
SCS0120

Rev: 00

Date: 23-08-2024

Author: Manojkumar P

1. Availability

System configuration

Model name	Model type	Single	Duplex
		Number of modules	Number of Duplex sets (=1/2 # of modules)
Digital Input Module	SDV144		5
Digital Output Module (8ch, 24VDC)	SDV531-S/L		
Digital Output Module (8ch, 48VDC)	SDV53A		
Digital Output Module (16ch, 24VDC)	SDV541		6
Digital Output Module (4ch, 24VDC)	SDV521		
Digital Output Module (4ch, 100VAC)	SDV526		
Analog Input Module (4～20mA)	SAI143-S		
Analog Input Module (4～20mA, with HART)	SAI143-H		9
Analog Input Module (1-5V/1-10V)	SAV144		
Analog Input Module (mV/TC)	SAT145		
Analog Input Module (RTD)	SAR145		
Analog Output Module (4～20mA, with HART)	SAI533		
Analog Digital I/O Module (Analog Input 2-wire)	S2MMM843 AI 2Wire		
Analog Digital I/O Module (Analog Input 4-wire)	S2MMM843 AI 4Wire		
Analog Digital I/O Module (Analog Output)	S2MMM843 AO		
Analog Digital I/O Module (Digital Input)	S2MMM843 DI		
Digital I/O Module (Digital Input)	S2MDV843 DI		
Analog Digital I/O Module (Digital Output)	S2MMM843 DO		
Digital I/O Module (Digital Output)	S2MDV843 DO		
Fire and Gas Communication Module	S2LP131		
Safety Control Unit (Single CPU for V net)	SSC10S		
Safety Control Unit (Dual redundant CPU for V net)	SSC10D		
Safety Control Unit (Single CPU for Vnet/IP)	SSC50S		
Safety Control Unit (Dual redundant CPU for Vnet/IP)	SSC50D		
Safety Control Unit (Single CPU for Vnet/IP)	SSC57S		
Safety Control Unit (Dual redundant CPU for Vnet/IP)	SSC57D		
Safety Control Unit (Single CPU for Vnet/IP)	SSC60S / S2SC70S (SCP461)		
Safety Control Unit (Dual redundant CPU for Vnet/IP)	SSC60D / S2SC70D (SCP461)		
Safety Control Unit (Single CPU for Vnet/IP)	SSC60S / S2SC70S (S2CP471)		
Safety Control Unit (Dual redundant CPU for Vnet/IP)	SSC60D / S2SC70D (S2CP471)	1	
Safety Node Unit	SNB10D / S2NN30D	5	
Unit for Optical Bus Repeater Module	SNT10D		
Optical ESB Bus Repeater Master Module (! Enter 1/2 #of Mdl) *1	SNT401/411		

*1 Failure rates of SNT501/511 are automatically calculated.

Parameters

Proof test interval (T) : 1 **years** 8760 **hours**

Mean Time To Restoration (MTTR) : 8 **hours**

Results

Availability: 99.99993 **%**

MTBFspurious: 1281.70 **years**

General Reliability Configurator™ for SIS
DTS: De-energize To Safe state

YOKOGAWA
Safety Assurance and Consultancy

tool info : revision 18.4
custodian: SA
© 2019 Yokogawa Europe B.V.

project no.:	E366772C00	system:	SCS0120
project name:	Base Load Power Hub (BLPH)	sub-system:	FGS System
	SCS0120	scope:	Overall System Availability
client name:	ROSETTI MARINO S.p.A	revision no.:	00
client P.O. no.:	CW-I-WP4-2023-05	executed by:	Manojkumar P
end user name:	Crosswind Hollandse Kust Noord	date:	23-08-2024

assumptions:

legend

MTBF = mean time between failure
MTTR = mean time to restoration
FTR = false trip rate
I/O = input / output
SE = sensor element
LS = logic solver
FE = final element

calculation scope

- ☐ sensor(s)
- ☑ SE interface(s)
- ☑ LS incl. I/O module(s)
- ☐ FE interface(s)
- ☐ final element(s)

Normally sensors and final elements are not included in availability calculations unless specified.

inputs

result from ext. calc.
MTBF (year)

ProSafe-RS availability
99.99993 %

	FTR		MTBF		availability	
targets		1/year		year		%
set MTTR	8	hour				

results

	FTR		MTBF		availability	
	0.04	1/year	28.53	year	99.99680	%
	4.001E+00	E-6/hr				
targets met?	n.a		n.a		n.a	

manufacturer	model	Type (A/B)	failure rates per circuit (E-6/hr)			total number of circuits for SIS Availability calculation, based on below voting principles					
			λ_S	λ_{Dd}	λ_{Du}	1oo1	1oo2	1oo3	2oo2	2oo3	2oo4
Sensor Interface Modules											
P&F	HiC2025 (1oo1)	A	0.00E+00	1.63E-01	4.09E-02	24					

Attachment -1

System Architecture

1724000594-IN-DD-00015_Rev 02 Update to rev. 03

Number of pages that follow: 4

Copyright © Yokogawa Electric Corporation

Base Load Power Hub (BLPH)

System Architecture

Document Number: 1724000594-IN-DD-00015

Supplier Document Number: E366772C00-SA

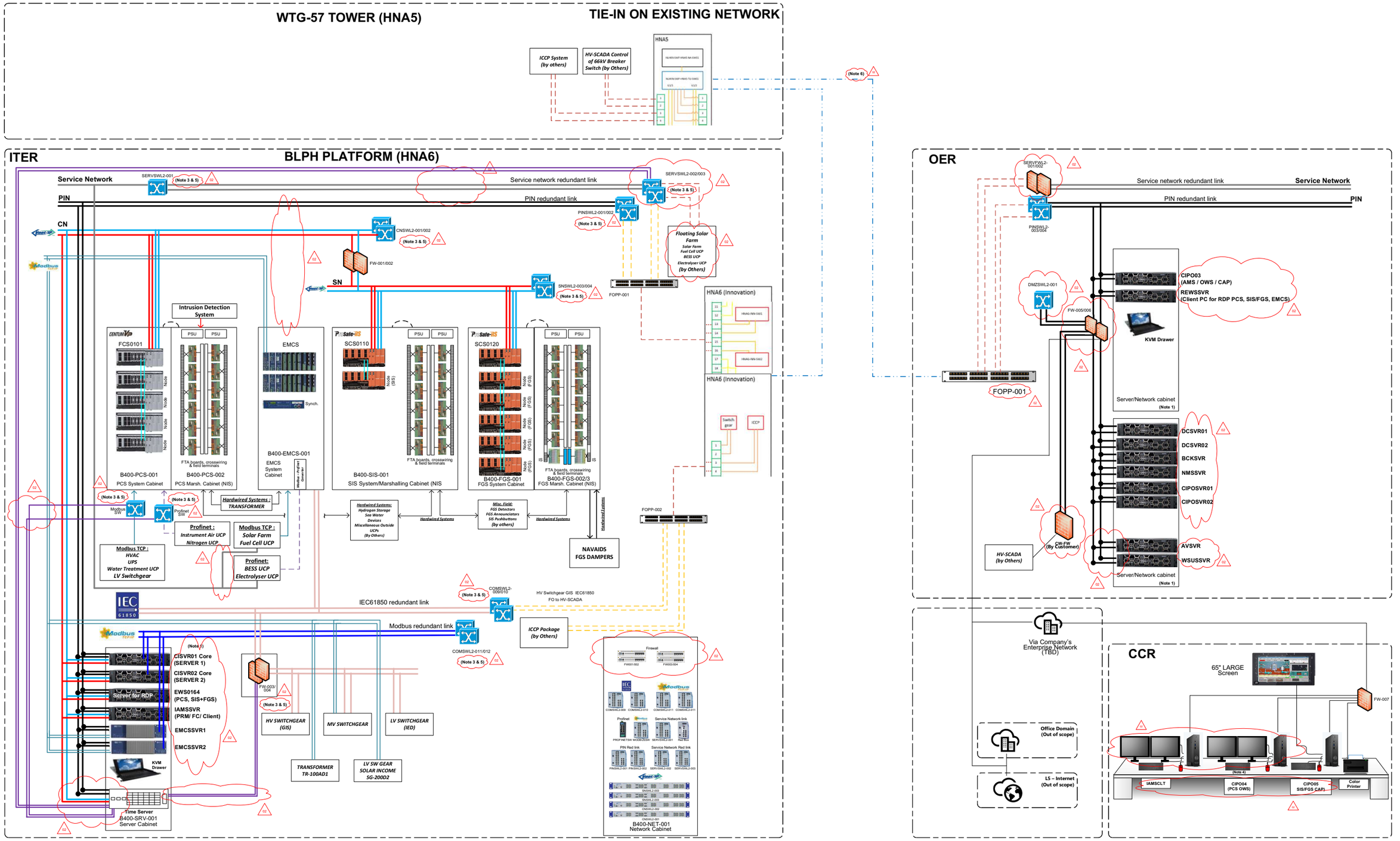
Document Class: 2

02	28/06/2024	Issue for Approval (IFA)	SKR	MP/AB	SC
01	24/05/2024	Issue for Review (IFR)	SKR	MP/AB	SC
00	23/04/2024	Issue for Review (IFR)	SKR	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

CROSSWIND BLPH PROJECT - SYSTEM ARCHITECTURE



AMS	: Alarm Management System	FCS	: Field Control Station
AV	: Anti-virus	FGS	: Fire & Gas System
BCK	: Backup Server	FO	: Fiber Optic
BESS	: Battery Energy Storage System	FOPP	: Fiber Optic Patch Panel (by others)
BLPH	: Base Load Power Hub	FTA	: Field Termination Assembly
CAP	: Critical Alarm Panel	HIST	: Historian
CCR	: Central Control Room	HKN	: Hollandse Kust Noord
CI	: Collaborative Information	IAMS	: Instrument Asset Management System
CN	: Control Network	ITER	: Instrument & Telecom Equipment Room
DC	: Domain Controller	LHVS	: Land High Voltage Station
DMZ	: De-militarized Zone	MCC	: Motor Control Center
ESB	: IO communication bus	MODB	: Modbus
EWS	: Engineering Work Station	MQTT	: Message Queuing Telemetry Transport
FC	: Field Communication (Vnet/IP)	NMS	: Network Management System
OER	: Onshore Equipment Room		
OHVS	: Offshore High Voltage Station		
OWS	: Operator Work Station		
PIN	: Plant Information Network		
PKG	: Package		
RDP	: Remote Desktop Protocol		
SCS	: Safety Control Station		
SIS	: Safety Instrumented System		
SN	: Safety Network		
SW	: Switch		
UCP	: Unit Control Panel (3rd party systems)		
VM	: Virtual Machine		
Vnet/IP	: Yokogawa's Control network		
WSUS	: Windows Security Update Services		

LEGEND:

- PIN (Plant Information Network)
- Vnet/IP BUS 1 PCS
- Vnet/IP BUS 2 PCS
- Vnet/IP BUS 1 SIS/FGS
- Vnet/IP BUS 2 SIS/FGS
- ESB bus connection
- IEC61850 connection
- MODBUS TCP/IP connection
- Service Network connection
- Modbus TCP connection
- Profinet (non redundant)
- Fiber Optic Patch Cords
- Fiber Optic connection (core by Crosswind)
- Fiber Optic backbone (by Crosswind)
- System Cable connection
- NTP Connection

Note 1 : Exact assignment of Servers per cabinet to be defined in cabinet General Arrangement Drawing.
Note 2 : Interface with HV SCADA, WIND FARM and SOLAR FARM to be finalized with Crosswind.
Note 3 : All Network Components will be installed in Network Cabinet.
Note 4 : Supply of Console Desk in CCR is in Customer Scope.
Note 5 : All Network Switches and Firewall is configured in VLAN.
Note 6 : Intermediate FO Connection between HNA5 and OER Intentionally not shown.

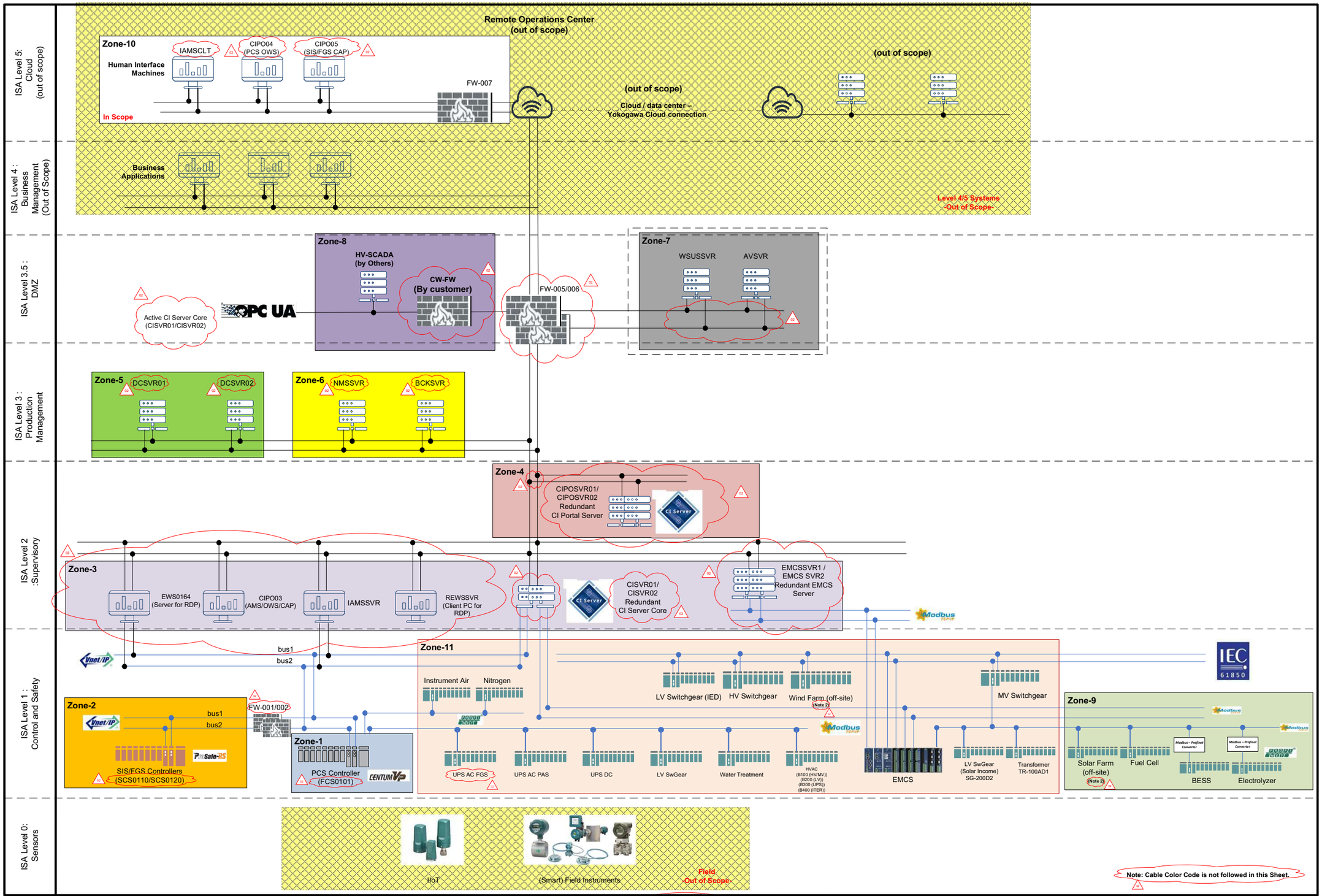
Zone-1 : PCS Control Zone
Zone-2 : Safety Control Zone
Zone-3 : PCS Zone
Zone-4 : Application Server Facility Zone
Zone-5 : Security Management Zone-1
Zone-6 : Security Management Zone-2
Zone-7 : Demilitirized Zone
Zone-8 : Croswind Zone
Zone-9 : Service Network Zone
Zone-10: Application Server Facility Zone-OD
Zone-11: Third Party System Zone
: Out of Scope

Doc No : 1724000594-IN-DD-00015
Doc Name : System Architecture

REV	DWG BY	CHK BY	APP BY	DATE
02	SKR	MP/AB	SC	28-Jun-24
01	SKR	MP/AB	SC	24-May-24
00	SKR	AB	SC	23-Apr-24

ROSETTI MARINO | HOLLANDSE KUST NOORD WIND PART Project | CROSSWIND | YOKOGAWA

CROSSWIND BLPH PROJECT - CYBER ARCHITECTURE



AMS	: Alarm Management System	FCS	: Field Control Station
AV	: Anti-virus	FGS	: Fire & Gas System
BCK	: Backup Server	FO	: Fiber Optic
BESS	: Battery Energy Storage System	FOPP	: Fiber Optic Patch Panel (by others)
BLPH	: Base Load Power Hub	FTA	: Field Termination Assembly
CAP	: Critical Alarm Panel	HIST	: Historian
CCR	: Central Control Room	HKN	: Hollandse Kust Noord
CI	: Collaborative Information	IAMS	: Instrument Asset Management System
CN	: Control Network	ITER	: Instrument & Telecom Equipment Room
DC	: Domain Controller	LHVS	: Land High Voltage Station
DMZ	: De-militarized Zone	MCC	: Motor Control Center
ESB	: IO communication bus	MODB	: Modbus
EWS	: Engineering Work Station	MQTT	: Message Queuing Telemetry Transport
FC	: Field Communication (Vnet/IP)	NMS	: Network Management System
OER	: Onshore Equipment Room		
OHVS	: Offshore High Voltage Station		
OWS	: Operator Work Station		
PIN	: Plant Information Network		
PKG	: Package		
RDP	: Remote Desktop Protocol		
SCS	: Safety Control Station		
SIS	: Safety Instrumented System		
SN	: Safety Network		
SW	: Switch		
UCP	: Unit Control Panel (3rd party systems)		
VM	: Virtual Machine		
Vnet/IP	: Yokogawa's Control network		
WSUS	: Windows Security Update Services		

LEGEND:

- PIN (Plant Information Network)
- Vnet/IP BUS 1 PCS
- Vnet/IP BUS 2 PCS
- Vnet/IP BUS 1 SIS/FGS
- Vnet/IP BUS 2 SIS/FGS
- ESB bus connection
- IEC61850 connection
- MODBUS TCP/IP connection
- Service Network connection
- Modbus TCP connection
- Profinet (non redundant)
- Fiber Optic Patch Cords
- Fiber Optic connection (core by Crosswind)
- Fiber Optic backbone (by Crosswind)
- System Cable connection
- NTP Connection

Note 1 : Exact assignment of Servers per cabinet to be defined in cabinet General Arrangement Drawing.
Note 2 : Interface with HV SCADA, WIND FARM and SOLAR FARM to be finalized with Crosswind.
Note 3 : All Network Components will be installed in Network Cabinet.
Note 4 : Supply of Console Desk in CCR is in Customer Scope.
Note 5 : All Network Switches and Firewall is configured in VLAN.
Note 6 : Intermediate FO Connection between HNA5 and OER Intentionally not shown.

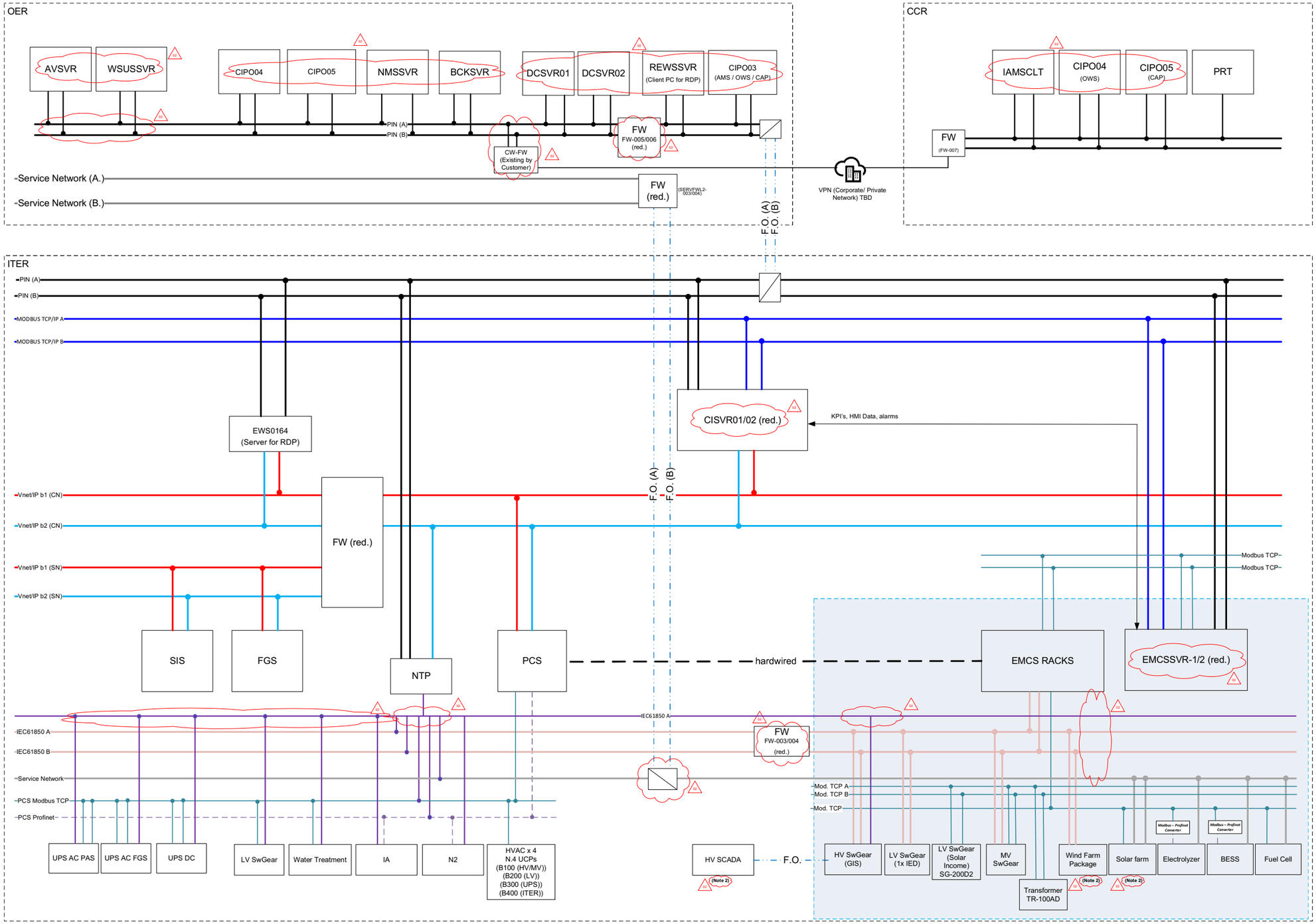
Zone-1 : PCS Control Zone
Zone-2 : Safety Control Zone
Zone-3 : PCS Zone
Zone-4 : Application Server Facility Zone
Zone-5 : Security Management Zone-1
Zone-6 : Security Management Zone-2
Zone-7 : Demilitirized Zone
Zone-8 : Croswind Zone
Zone-9 : Service Network Zone
Zone-10: Application Server Facility Zone-OD
Zone-11: Third Party System Zone
: Out of Scope

REV	DWG BY	CHK BY	APP BY	DATE
02	SKR	MP/AB	SC	28-Jun-24
01	SKR	MP/AB	SC	24-May-24
00	SKR	AB	SC	23-Apr-24

Doc No : 1724000594-IN-DD-00015
Doc Name : System Architecture

ROSETTI MARINO | HOLLANDSE KUST NOORD WIND PART Project | CROSSWIND | YOKOGAWA

CROSSWIND BLPH PROJECT - SYSTEM BLOCK DIAGRAM



AMS	: Alarm Management System	FCS	: Field Control Station
AV	: Anti-virus	FGS	: Fire & Gas System
BCK	: Backup Server	FO	: Fiber Optic
BESS	: Battery Energy Storage System	FOPP	: Fiber Optic Patch Panel (by others)
BLPH	: Base Load Power Hub	FTA	: Field Termination Assembly
CAP	: Critical Alarm Panel	HIST	: Historian
CCR	: Central Control Room	HKN	: Hollandse Kust Noord
CI	: Collaborative Information	IAMS	: Instrument Asset Management System
CN	: Control Network	ITER	: Instrument & Telecom Equipment Room
DC	: Domain Controller	LHVS	: Land High Voltage Station
DMZ	: De-militarized Zone	MCC	: Motor Control Center
ESB	: IO communication bus	MODB	: Modbus
EWS	: Engineering Work Station	MQTT	: Message Queuing Telemetry Transport
FC	: Field Communication (Vnet/IP)	NMS	: Network Management System

OER	: Onshore Equipment Room		
OHVS	: Offshore High Voltage Station		
OWS	: Operator Work Station		
PIN	: Plant Information Network		
PKG	: Package		
RDP	: Remote Desktop Protocol		
SCS	: Safety Control Station		
SIS	: Safety Instrumented System		
SN	: Safety Network		
SW	: Switch		
UCP	: Unit Control Panel (3rd party systems)		
VM	: Virtual Machine		
Vnet/IP	: Yokogawa's Control network		
WSUS	: Windows Security Update Services		

LEGEND:

- PIN (Plant Information Network)
- Vnet/IP BUS 1 PCS
- Vnet/IP BUS 2 PCS
- Vnet/IP BUS 1 SIS/FGS
- Vnet/IP BUS 2 SIS/FGS
- ESB bus connection
- IEC61850 connection
- MODBUS TCP/IP connection
- Service Network connection
- Modbus TCP connection
- Profinet (non redundant)
- Fiber Optic Patch Cords
- Fiber Optic connection (core by Crosswind)
- Fiber Optic backbone (by Crosswind)
- System Cable connection
- NTP Connection

Note 1 : Exact assignment of Servers per cabinet to be defined in cabinet General Arrangement Drawing.
Note 2 : Interface with HV SCADA, WIND FARM and SOLAR FARM to be finalized with Crosswind.
Note 3 : All Network Components will be installed in Network Cabinet.
Note 4 : Supply of Console Desk in CCR is in Customer Scope.
Note 5 : All Network Switches and Firewall is configured in VLAN.
Note 6 : Intermediate FO Connection between HNA5 and OER Intentionally not shown.

Zone-1 : PCS Control Zone
Zone-2 : Safety Control Zone
Zone-3 : PCS Zone
Zone-4 : Application Server Facility Zone
Zone-5 : Security Management Zone-1
Zone-6 : Security Management Zone-2
Zone-7 : Demilitirized Zone
Zone-8 : Croswind Zone
Zone-9 : Service Network Zone
Zone-10: Application Server Facility Zone-OD
Zone-11: Third Party System Zone
: Out of Scope

REV	DWG BY	CHK BY	APP BY	DATE
02	SKR	MP/AB	SC	28-Jun-24
01	SKR	MP/AB	SC	24-May-24
00	SKR	AB	SC	23-Apr-24

Doc No : 1724000594-IN-DD-00015
Doc Name : System Architecture

ROSETTI MARINO
HOLLANDSE KUST NOORD WIND PART Project
CROSSWIND
YOKOGAWA

Appendix II

Safety Certificates and Safety Manuals

Number of pages that follow: 44

Copyright © Yokogawa Electric Corporation

Reliability Data Sheet: Rev. 4

Pepperl+Fuchs - SMART Transmitter Power Supply				
Device Type No. KCD2-STC-(Ex)1(.SP) and HiC2025(A)				
Doc. ref.	Document name	Date	Revision	Institute
DOCT-6393A	Functional Safety Manual	04-2020	-	P+F

Yokogawa's independent group of Safety Experts has assessed the reliability data in the attached report and proposes to use these data as follows (values in E-06/hr):

Manufacturer	Model	Type	λ_S (*)	λ_{DD} (*)	λ_{DU} (*)
Pepperl+Fuchs	KCD2-STC-(Ex)1(.SP) HiC2025(A)	A	0	1.63E-01	4.09E-02

(*) The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60541-1 class C (sheltered location) with an average temperature of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied by 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

Yokogawa's approach is to use the reliability data in a conservative way, thus minimizing the chance of a too optimistic calculation. On request the calculation can always be repeated with less conservative data.

Manufacturer claims compliance to Systematic Capability: SC3(*)
(*) DOCT-6393A, P+F (or more recent)

Considerations

Values are only valid for Route 1H.

Values are taken from the attached safety manual without change.

Amersfoort, 08 – 12 – 2020
Rob van der Harst
Functional Safety Specialist
FS Eng (TÜV Rheinland, #13190 / 16 - SIS)

Amersfoort, 08 – 12 – 2020
Arjan Kroon
Functional Safety Specialist
FS Exp (TÜV Rheinland, #308 / 2020 - SIS/FSM)

Functional Safety

SMART Transmitter Power Supply KCD2-STC-(Ex)1(.SP), HiC2025(A)

Manual

SIL

IEC 61508/61511

ISO9001

CE SIL 2

Your automation, our passion.

PEPPERL+FUCHS

With regard to the supply of products, the current issue of the following document is applicable:
The General Terms of Delivery for Products and Services of the Electrical Industry, published by the Central Association of the Electrical Industry (Zentralverband Elektrotechnik und Elektroindustrie (ZVEI) e.V.) in its most recent version as well as the supplementary clause: "Expanded reservation of proprietorship"

Worldwide

Pepperl+Fuchs Group

Lilienthalstr. 200

68307 Mannheim

Germany

Phone: +49 621 776 - 0

E-mail: info@de.pepperl-fuchs.com

North American Headquarters

Pepperl+Fuchs Inc.

1600 Enterprise Parkway

Twinsburg, Ohio 44087

USA

Phone: +1 330 425-3555

E-mail: sales@us.pepperl-fuchs.com

Asia Headquarters

Pepperl+Fuchs Pte. Ltd.

P+F Building

18 Ayer Rajah Crescent

Singapore 139942

Phone: +65 6779-9091

E-mail: sales@sg.pepperl-fuchs.com

https://www.pepperl-fuchs.com

1 Introduction 5
1.1 Content of this Document 5
1.2 Safety Information 6
1.3 Symbols Used 7
2 Product Description 8
2.1 Validity 8
2.2 Function 8
2.3 Interfaces 9
2.4 Marking 9
2.5 Standards and Directives for Functional Safety 9
3 Planning 10
3.1 System Structure 10
3.2 Assumptions 11
3.3 Safety Function and Safe State 12
3.4 Characteristic Safety Values 13
3.5 Useful Lifetime 14
4 Mounting and Installation 15
4.1 Configuration 15
5 Operation 16
5.1 Proof Test Procedure 16
6 Maintenance and Repair 19
7 List of Abbreviations 20

2020-04

2020-04

1 Introduction

1.1 Content of this Document

This document contains information for usage of the device in functional safety-related applications. You need this information to use your product throughout the applicable stages of the product life cycle. These can include the following:

- Product identification
- Delivery, transport, and storage
- Mounting and installation
- Commissioning and operation
- Maintenance and repair
- Troubleshooting
- Dismounting
- Disposal

Note

This document does not substitute the instruction manual.

Note

For full information on the product, refer to the instruction manual and further documentation on the Internet at www.pepperl-fuchs.com.

The documentation consists of the following parts:

- Present document
- Instruction manual
- Manual
- Datasheet

Additionally, the following parts may belong to the documentation, if applicable:

- EU-type examination certificate
- EU declaration of conformity
- Attestation of conformity
- Certificates
- Control drawings
- FMEDA report
- Assessment report
- Additional documents

For more information about Pepperl+Fuchs products with functional safety, see www.pepperl-fuchs.com/sil.

1.2 Safety Information

Target Group, Personnel

Responsibility for planning, assembly, commissioning, operation, maintenance, and dismounting lies with the plant operator.

Only appropriately trained and qualified personnel may carry out mounting, installation, commissioning, operation, maintenance, and dismounting of the product. The personnel must have read and understood the instruction manual and the further documentation.

Intended Use

The device is only approved for appropriate and intended use. Ignoring these instructions will void any warranty and absolve the manufacturer from any liability.

The device is developed, manufactured and tested according to the relevant safety standards.

Use the device only

- for the application described
- with specified environmental conditions
- with devices that are suitable for this safety application

Improper Use

Protection of the personnel and the plant is not ensured if the device is not used according to its intended use.

1.3 Symbols Used

This document contains symbols for the identification of warning messages and of informative messages.

Warning Messages

You will find warning messages, whenever dangers may arise from your actions. It is mandatory that you observe these warning messages for your personal safety and in order to avoid property damage.

Depending on the risk level, the warning messages are displayed in descending order as follows:



Danger!

This symbol indicates an imminent danger.

Non-observance will result in personal injury or death.



Warning!

This symbol indicates a possible fault or danger.

Non-observance may cause personal injury or serious property damage.



Caution!

This symbol indicates a possible fault.

Non-observance could interrupt the device and any connected systems and plants, or result in their complete failure.

Informative Symbols



Note

This symbol brings important information to your attention.



Action

This symbol indicates a paragraph with instructions. You are prompted to perform an action or a sequence of actions.

2 Product Description

2.1 Validity

This manual is only valid for devices with a part number **greater than #310000**.

Contact your Pepperl+Fuchs representative for information about older devices.

2.2 Function

KCD2-STC-1(.SP)

This signal conditioner provides the galvanic isolation between field circuits and control circuits.

The device supplies 2-wire transmitters in the field, and can also be used with current sources.

The device transfers the analog input signal to the control side as an isolated current value.

Bi-directional communication is supported for SMART transmitters that use current modulation to transmit data and voltage modulation to receive data. If the HART communication resistance in the loop is too low, the internal resistance can be used.

Test sockets for the connection of HART communicators are integrated into the terminals of the device.

The output is selected as a current source, current sink, or voltage source via DIP switches.

The device is mounted on a 35 mm DIN mounting rail according to EN 60715.

SP version

The devices are available with screw terminals or spring terminals. The type code of the versions of the devices with spring terminals has the extension ".SP".

KCD2-STC-Ex1(.SP)

This isolated barrier is used for intrinsic safety applications.

The device supplies 2-wire transmitters in the hazardous area, and can also be used with current sources.

The device transfers the analog input signal to the non-hazardous area as an isolated current value.

Bi-directional communication is supported for SMART transmitters that use current modulation to transmit data and voltage modulation to receive data. If the HART communication resistance in the loop is too low, the internal resistance can be used.

Test sockets for the connection of HART communicators are integrated into the terminals of the device.

The output is selected as a current source, current sink, or voltage source via DIP switches.

The device is mounted on a 35 mm DIN mounting rail according to EN 60715.

SP version

The devices are available with screw terminals or spring terminals. The type code of the versions of the devices with spring terminals has the extension ".SP".

HiC2025(A)

This isolated barrier is used for intrinsic safety applications.

The device supplies 2-wire transmitters in the hazardous area, and can also be used with current sources.

The device transfers the analog input signal to the non-hazardous area as an isolated current value.

Bi-directional communication is supported for SMART transmitters that use current modulation to transmit data and voltage modulation to receive data.

The output is selected as a current source, current sink, or voltage source via DIP switches.

This device mounts on a HiC termination board.

A version

Device version A has reduced intrinsically safe parameters.

2.3 Interfaces

The device has the following interfaces.

- Safety relevant interfaces: input I, output I
- Non-safety relevant interfaces: none
  The HART communication is not relevant for functional safety.

Note

For corresponding connections see datasheet.

2.4 Marking

Pepperl+Fuchs Group Lilienthalstraße 200, 68307 Mannheim, Germany
Internet: www.pepperl-fuchs.com

KCD2-STC-1(.SP)	Up to SIL 2
KCD2-STC-Ex1(.SP)	
HiC2025(A)	

2.5 Standards and Directives for Functional Safety

Device specific standards and directives

Functional safety	IEC/EN 61508, part 1 – 7, edition 2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (manufacturer)

System-specific standards and directives

Functional safety	IEC 61511-1:2016+COR1:2016+A1:2017 EN 61511-1:2017+A1:2017 Functional safety – Safety instrumented systems for the process industry sector (user)

3 Planning

3.1 System Structure

3.1.1 Low Demand Mode of Operation

If there are two control loops, one for the standard operation and another one for the functional safety, then usually the demand rate for the safety loop is assumed to be less than once per year.

The relevant safety parameters to be verified are:

- the PFD_{avg} value (average **P**robability of dangerous **F**ailure on **D**emand) and the T_1 value (proof test interval that has a direct impact on the PFD_{avg} value)
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance)

3.1.2 High Demand or Continuous Mode of Operation

If there is only one safety loop, which combines the standard operation and safety-related operation, then usually the demand rate for this safety loop is assumed to be higher than once per year.

The relevant safety parameters to be verified are:

- the PFH value (**P**robability of dangerous **F**ailure per **H**our)
- Fault reaction time of the safety system
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance)

3.1.3 Safe Failure Fraction

The safe failure fraction describes the ratio of all safe failures and dangerous detected failures to the total failure rate.

$SFF = (\lambda_s + \lambda_{dd}) / (\lambda_s + \lambda_{dd} + \lambda_{du})$

A safe failure fraction as defined in IEC/EN 61508 is only relevant for elements or (sub)systems in a complete safety loop. The device under consideration is always part of a safety loop but is not regarded as a complete element or subsystem.

For calculating the SIL of a safety loop it is necessary to evaluate the safe failure fraction of elements, subsystems and the complete system, but not of a single device.

Nevertheless the SFF of the device is given in this document for reference.

2020-04

3.2 Assumptions

The following assumptions have been made during the FMEDA:

- Failure rate based on the Siemens standard SN 29500.
- Failure rates are constant, wear is not considered.
- External power supply failure rates are not included.
- The safety-related device is considered to be of type **A** device with a hardware fault tolerance of **0**.
- The device will be used under average industrial ambient conditions comparable to the classification "stationary mounted" according to MIL-HDBK-217F.

  Alternatively, operating stress conditions typical of an industrial field environment similar to IEC/EN 60654-1 Class C with an average temperature over a long period of time of 40 °C may be assumed. For a higher average temperature of 60 °C, the failure rates must be multiplied by a factor of 2.5 based on experience. A similar factor must be used if frequent temperature fluctuations are expected.
- The application program in the programmable logic controller (PLC) is configured to detect underrange and overrange failures.
- The device do not has a fault bus.

SIL 2 Application

- To build a SIL safety loop for the defined SIL, it is assumed as an example that this device uses 10 % of the available budget for PFD_{avg}/PFH.
- For a SIL 2 application operating in low demand mode the total PFD_{avg} value of the SIF (**S**afety **I**nstrumented **F**unction) should be smaller than 10^{-2}, hence the maximum allowable PFD_{avg} value would then be 10^{-3}.
- For a SIL 2 application operating in high demand mode the total PFH value of the SIF should be smaller than 10^{-6} per hour, hence the maximum allowable PFH value would then be 10^{-7} per hour.
- Since the safety loop has a hardware fault tolerance of **0** and it is a type **A** device, the SFF must be > 60 % according to table 2 of IEC/EN 61508-2 for a SIL 2 (sub) system.

3.3 Safety Function and Safe State

Safety Function

The device transfers analog signals from the input to the output with a tolerance of 2 % related to the full signal range.

Use the following DIP switch settings for safety-relevant applications:

DIP Switch Settings KCD2-STC-(Ex)1(.SP)

Function	S1	S2	S3	S4
Current source 4 mA to 20 mA	II	II	I	II
Voltage source 1 V to 5 V	II	II	I	I
Current sink 4 mA to 20 mA	II	I	II	II

Table 3.1

DIP Switch Settings HiC2025(A)

Function	S1	S2	S3	S4
Current source 4 mA to 20 mA	OFF	OFF	ON	OFF
Voltage source 1 V to 5 V	OFF	OFF	ON	ON
Current sink 4 mA to 20 mA	OFF	ON	OFF	OFF

Table 3.2

Safe State

In the safe state, the following values must be reached at the output:

- < 3.6 mA or > 21.5 mA,
- < 0.9 V or > 5.375 V,

Reaction Times

The safety reaction time is the maximum time required from the occurrence of the fault to the reaction of the outputs in normal operation without faults.

The combined fault detection and fault reaction time is the time in which the device outputs react to an occurred fault. See chapter 3.4.

Note

See corresponding datasheets for further information.

3.4 Characteristic Safety Values

Parameters	Characteristic values
Assessment type	Full assessment
Device type	A
Mode of operation	Low demand mode or high demand mode
HFT	0
SIL	2
SC	3
Safety function	Transfer of the analog signals
λ_s [1]	0 FIT
λ_{dd}	163 FIT
λ_{du}	40.9 FIT
$\lambda_{total\ (safety\ function)}$ [1]	204 FIT
$\lambda_{not\ part}$	18.6 FIT
SFF [1]	79 %
MTBF [2]	276 years
PFH	4.09×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	1.79×10^{-4}
PFD_{avg} for T_{proof} = 2 years	3.58×10^{-4}
PFD_{avg} for T_{proof} = 5 years	8.96×10^{-4}
PTC	100 %
Safety reaction time Fault reaction time [3]	< 20 ms < 100 ms

Table 3.3

1 "No effect failures" are not influencing the safety function and are therefore not included in SFF and in the failure rates of the safety function.

2 acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 24 h.

3 Time between fault occurence and fault reaction

The characteristic safety values like PFD, SFF, HFT and T_1 are taken from the SIL report/FMEDA report. Observe that PFD and T_1 are related to each other.

The function of the devices has to be checked within the proof test interval (T_1).

3.5 Useful Lifetime

Although a constant failure rate is assumed by the probabilistic estimation this only applies provided that the useful lifetime of components is not exceeded. Beyond this useful lifetime, the result of the probabilistic estimation is meaningless as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular. For example, electrolytic capacitors can be very sensitive to the operating temperature.

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that failure calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation and therefore the assumption of a constant failure rate during the useful lifetime is valid.

However, according to IEC/EN 61508-2, a useful lifetime, based on general experience, should be assumed. Experience has shown that the useful lifetime often lies within a range period of about 8 to 12 years.

As noted in DIN EN 61508-2:2011 note N3, appropriate measures taken by the manufacturer and plant operator can extend the useful lifetime.

Our experience has shown that the useful lifetime of a Pepperl+Fuchs product can be higher if the ambient conditions support a long life time, for example if the ambient temperature is significantly below 60 °C.

Please note that the useful lifetime refers to the (constant) failure rate of the device. The effective life time can be higher.

The estimated useful lifetime is greater than the warranty period prescribed by law or the manufacturer's guarantee period. However, this does not result in an extension of the warranty or guarantee services. Failure to reach the estimated useful lifetime is not a material defect.

4 Mounting and Installation

Mounting and Installing the Device

1. Observe the safety instructions in the instruction manual.
2. Observe the information in the manual.
3. Observe the requirements for the safety loop.
4. Connect the device only to devices that are suitable for this safety application.
5. Check the safety function to ensure the expected output behavior.

4.1 Configuration

Configuring the Devices with DIP Switches on the Device Side

The device is configured via DIP switches. The DIP switches for setting the safety functions are on the side of the device.

1. De-energize the device before configuring the device.
2. Remove the device.
3. Configure the device for the required safety function via the DIP switches, see chapter 3.3.
4. Secure the DIP switches to prevent unintentional adjustments.
5. Mount the device.
6. Connect the device again.

Configuring the Devices with DIP Switches on the Front Side

The device is configured via DIP switches. The DIP switches for setting the safety functions are on the front of the device.

1. De-energize the device before configuring the device.
2. Open the cover.
3. Configure the device for the required safety function via the DIP switches, see chapter 3.3.
4. Close the cover.
5. Secure the DIP switches to prevent unintentional adjustments.
6. Connect the device again.

Note

See corresponding datasheets for further information.

5 Operation

Danger!

Danger to life from missing safety function

If the safety loop is put out of service, the safety function is no longer guaranteed.

- Do not deactivate the device.
- Do not bypass the safety function.
- Do not repair, modify, or manipulate the device.

Operating the device

1. Observe the safety instruction in the instruction manual.
2. Observe the information in the manual.
3. Use the device only with devices that are suitable for this safety application.
4. Correct any occurring safe failures within 24 hours. Take measures to maintain the safety function while the device is being repaired.

5.1 Proof Test Procedure

This section describes a possible proof test procedure. The user is not obliged to use this proposal. The user may consider different concepts with an individual determination of the respective effectiveness, e. g. concepts according to NA106:2018.

According to IEC/EN 61508-2 a recurring proof test shall be undertaken to reveal potential dangerous failures that are not detected otherwise.

Check the function of the subsystem at periodic intervals depending on the applied PFD_{avg} in accordance with the characteristic safety values. See chapter 3.4.

It is under the responsibility of the plant operator to define the type of proof test and the interval time period.

Equipment required:

- Digital multimeter with an accuracy better than 0.1 %

  Use for the proof test of the intrinsic safety side of the device a special digital multimeter for intrinsically safe circuits.

  If intrinsically safe circuits are operated with non-intrinsically safe circuits, they must no longer be used as intrinsically safe circuits.
- Power supply set to nominal voltage of 24 V DC
- Process calibrator with current source and current sink function with an accuracy better than 20 µA

Proof Test Procedure

1. Put out of service the entire safety loop. Protect the application by means of other measures.
2. Prepare a test set-up, see figures below.
3. Test the devices. Verify the current values as given in table below.
4. Set back the device to the original settings for the application after the test.

Step No.	Input	Output		
	Input value (mA)	Output value (mA)	Output value for 2-wire Tx (V)	Output value for 4-wire Tx (V)
1	20.00	20.00 ± 0.4	15.3 ± 0.6	4.1 ± 1.5
2	12.00	12.00 ± 0.4	17.3 ± 0.6	4.1 ± 1.5
3	4.00	4.00 ± 0.4	19.3 ± 0.6	4.1 ± 1.5
4 [1]	23.00	23.00 ± 0.4	14.4 ± 0.6	4.1 ± 1.5
5 [1]	0	< 0.2	22.0 ± 2.0	n. a.
6	12.00			

Table 5.1 Steps to be performed for the proof test

[1] The output shall detect a fail high or fail low condition.

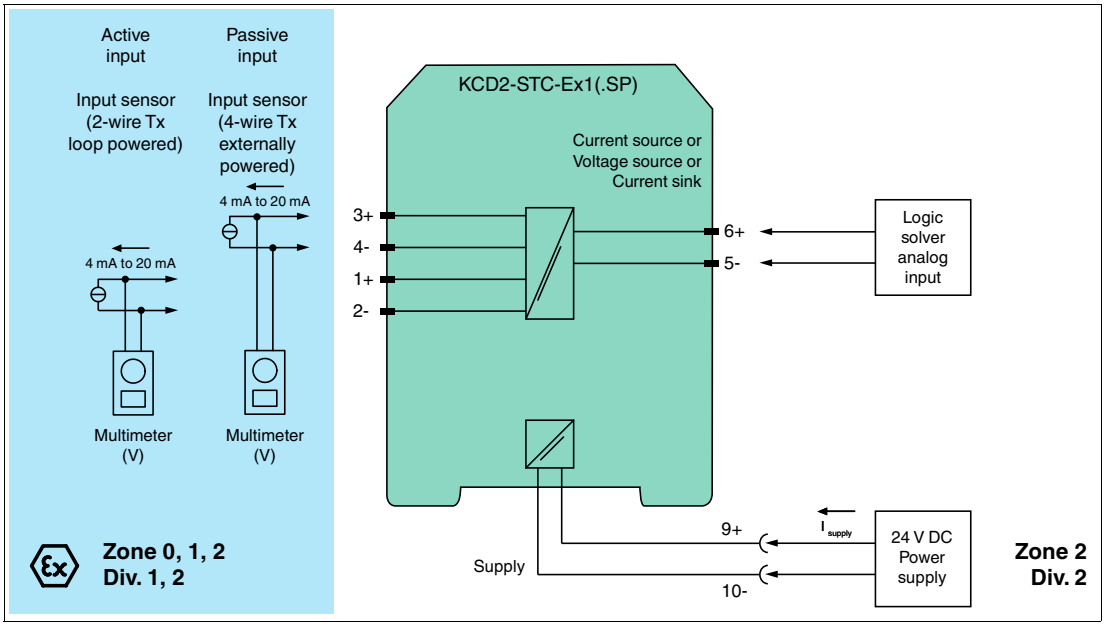


Figure 5.1 Proof test set-up for KCD2-STC-(Ex)1(.SP)

Usage in Zone 0, 1, 2/Div. 1, 2 only for KCD2-STC-Ex1(.SP)

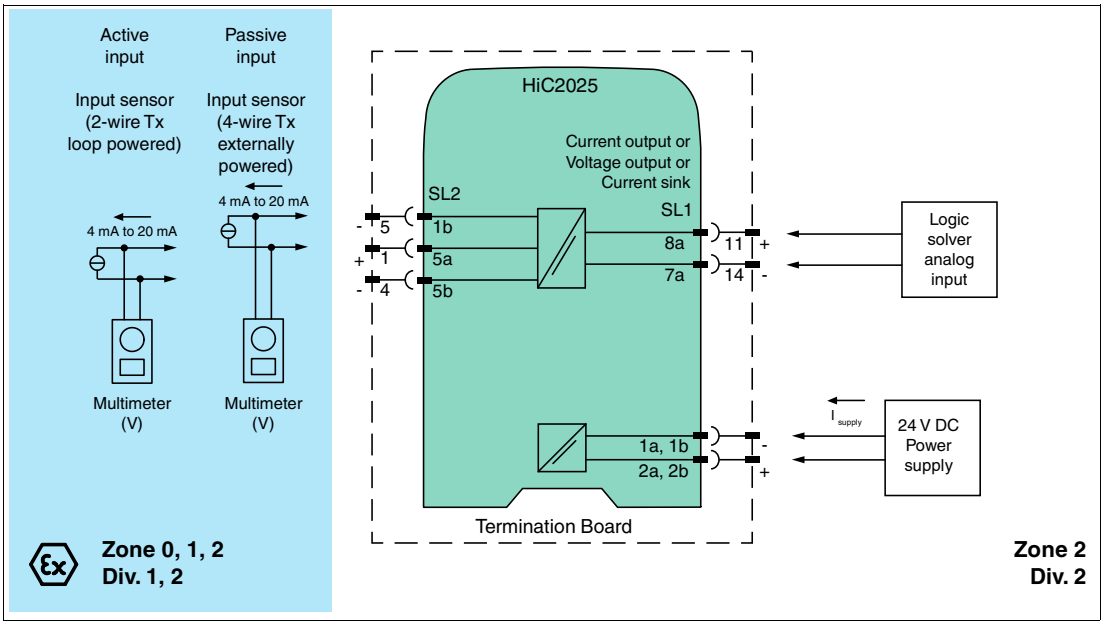


Figure 5.2 Proof test set-up for HiC2025(A)

Tip

The easiest way to test HiC devices is by using a stand-alone HiCTB**-SCT-***-**-** termination board. In this test, it is not necessary to disconnect the wiring of the existing application. Faults in a subsequent wiring can be avoided.

6 Maintenance and Repair



Danger!

Danger to life from missing safety function

Changes to the device or a defect of the device can lead to device malfunction.
The function of the device and the safety function is no longer guaranteed.

Do not repair, modify, or manipulate the device.



Maintaining, Repairing or Replacing the Device

In case of maintenance, repair or replacement of the device, proceed as follows:

1. Implement appropriate maintenance procedures for regular maintenance of the safety loop.
2. While the device is maintained, repaired or replaced, the safety function does not work.
   Take appropriate measures to protect personnel and equipment while the safety function is not available.
   Secure the application against accidental restart.
3. Do not repair a defective device. A defective device must only be repaired by the manufacturer.
4. If there is a defect, always replace the device with an original device.

7 List of Abbreviations

ESD	**E**mergency **S**hut**d**own
FIT	**F**ailure **I**n **T**ime in 10^{-9} 1/h
FMEDA	**F**ailure **M**ode, **E**ffects, and **D**iagnostics **A**nalysis
λ_s	Probability of safe failure
λ_{dd}	Probability of dangerous detected failure
λ_{du}	Probability of dangerous undetected failure
$\lambda_{no\ effect}$	Probability of failures of components in the safety loop that have no effect on the safety function.
$\lambda_{not\ part}$	Probability of failure of components that are not in the safety loop
$\lambda_{total\ (safety\ function)}$	Probability of failure of components that are in the safety loop
HFT	**H**ardware **F**ault **T**olerance
MTBF	**M**ean **T**ime **B**etween **F**ailures
MTTR	**M**ean **T**ime **T**o **R**estoration
PCS	**P**rocess **C**ontrol **S**ystem
PFD_{avg}	Average **P**robability of dangerous **F**ailure on **D**emand
PFH	Average frequency of dangerous failure per hour
PLC	**P**rogrammable **L**ogic **C**ontroller
PTC	**P**roof **T**est **C**overage
SC	**S**ystematic **C**apability
SFF	**S**afe **F**ailure **F**raction
SIF	**S**afety **I**nstrumented **F**unction
SIL	**S**afety **I**ntegrity **L**evel
SIS	**S**afety **I**nstrumented **S**ystem
T_1	Proof Test Interval

2020-04

Your automation, our passion.

Explosion Protection

- Intrinsic Safety Barriers
- Signal Conditioners
- FieldConnex® Fieldbus
- Remote I/O Systems
- Electrical Ex Equipment
- Purge and Pressurization
- Industrial HMI
- Mobile Computing and Communications
- HART Interface Solutions
- Surge Protection
- Wireless Solutions
- Level Measurement

Industrial Sensors

- Proximity Sensors
- Photoelectric Sensors
- Industrial Vision
- Ultrasonic Sensors
- Rotary Encoders
- Positioning Systems
- Inclination and Acceleration Sensors
- Fieldbus Modules
- AS-Interface
- Identification Systems
- Displays and Signal Processing
- Connectivity

Pepperl+Fuchs Quality
Download our latest policy here:

www.pepperl-fuchs.com/quality

PEPPERL+FUCHS

www.pepperl-fuchs.com

© Pepperl+Fuchs · Subject to modifications

Printed in Germany / DOCT-6393A

Pepperl+Fuchs - Relay Module				
Device Type No. KFD0-RSH-1.4S.PS2				
Doc. ref.	Document name	Date	Revision	Institute
225538	Safety Manual SIL	04-01-2011	-	P+F
P+F 100397R1C P0006 C04.2	Certificate	03-05-2011	-	Exida

Yokogawa's independent group of Safety Experts has assessed the reliability data in the attached report and proposes to use these data as follows (values in E-06/hr):

Manufacturer	Model	Type	λ_S (*)	λ_{DD} (*)	λ_{DU} (*)
Pepperl+Fuchs	KFD0-RSH-1.4S.PS2 **DTS**	A	3.50E-02	0	1.83E-03
Pepperl+Fuchs	KFD0-RSH-1.4S.PS2 **ETS**	A	5.71E-02	0	7.10E-03

(*) The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60541-1 class C (sheltered location) with an average temperature of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied by 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

Yokogawa's approach is to use the reliability data in a conservative way, thus minimizing the chance of a too optimistic calculation. On request the calculation can always be repeated with less conservative data.

Manufacturer claims compliance to Systematic Capability: SC3(*)
(*) P+F 090535 P0006 C011.2, Exida (or more recent)

Considerations

The attached report clearly refers to IEC61508:2000 (see 1.4)

Currently the reference should be to IEC61508: 2010 and consequently some failures that have been included in the λ_{total} should be left out of the calculation (this results in the value of λ_S above).

The failures that have been left out of the calculation were established in a discussion with P&F in November 2010; however they did not find their way into above report of April 2011.

Amersfoort, 15 – 10 – 2019
Rob van der Harst
Functional Safety Consultant
FS Eng (TÜV Rheinland, #13190/16, SIS)

Amersfoort, 15 – 10 – 2019
Arjan Kroon
Functional Safety Consultant
FS Eng (TÜV Rheinland, #4458/19, SIS)



SAFETY MANUAL SIL

RELAY MODULE

KFD0-RSH-1.4S.PS2

SIL
IEC 61508/61511

ISO9001

CE

SIL3

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

With regard to the supply of products, the current issue of the following document is applicable: The General Terms of Delivery for Products and Services of the Electrical Industry, published by the Central Association of the Electrical Industry (Zentralverband Elektrotechnik und Elektroindustrie (ZVEI) e.V.) in its most recent version as well as the supplementary clause: "Expanded reservation of proprietorship"

1 Introduction 4
1.1 General Information 4
1.2 Intended Use 4
1.3 Manufacturer Information 5
1.4 Relevant Standards and Directives 5
2 Planning 6
2.1 System Structure 6
2.1.1 Low Demand Mode 6
2.1.2 High Demand Mode 6
2.2 Assumptions 7
2.3 Safety Function and Safe State 8
2.4 Characteristic Safety Values 9
3 Safety Recommendation 10
3.1 Interfaces 10
3.2 Configuration 10
3.3 Useful Life Time 10
3.4 Installation and Commissioning 11
4 Proof Test 12
4.1 Proof Test Procedure 12
5 Abbreviations 16

225538 2011-04

1 Introduction

1.1 General Information

This manual contains information for application of the device in functional safety related loops.

The corresponding data sheets, the operating instructions, the system description, the Declaration of Conformity, the EC-Type-Examination Certificate, the Functional Safety Assessment and applicable Certificates (see data sheet) are integral parts of this document.

The documents mentioned are available from **www.pepperl-fuchs.com** or by contacting your local Pepperl+Fuchs representative.

Mounting, commissioning, operation, maintenance and dismounting of any devices may only be carried out by trained, qualified personnel. The instruction manual must be read and understood.

When it is not possible to correct faults, the devices must be taken out of service and action taken to protect against accidental use. Devices should only be repaired directly by the manufacturer. De-activating or bypassing safety functions or failure to follow the advice given in this manual (causing disturbances or impairment of safety functions) may cause damage to property, environment or persons for which Pepperl+Fuchs GmbH will not be liable.

The devices are developed, manufactured and tested according to the relevant safety standards. They must only be used for the applications described in the instructions and with specified environmental conditions, and only in connection with approved external devices.

1.2 Intended Use

This signal conditioner is a loop powered safety relay module with a logic input and two different relay outputs:

It can be used as an interface in output loops for fire and gas systems classified as SIL3. The safe state in this application is **e**nergized **t**o **s**afe (ETS). Output I with two relays in parallel must be used, no fuse available.

It can also be used as an interface in output loops for ESD (**E**mergency **S**hut **D**own) systems classified as SIL3. The safe state in this application is **d**e-energized **t**o **s**afe (DTS). Output II with two relays in series must be used. An additional fuse in series to the relay contacts is available (see chapter 3).

With both outputs in combination a non safety application for dual pole switching (DPS) is possible.

Additionally a test input for proof tests is available. The proof test checks if each single relay is working correctly.

The device is usually mounted on a DIN rail in cabinets with access for qualified personnel only.

225538 2011-04

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200
68307 Mannheim/Germany

KFD0-RSH-1.4S.PS2

Up to SIL3 (for DTS), up to SIL3 (for ETS)

1.4 Relevant Standards and Directives

Device specific standards and directives

- Functional safety IEC 61508 part 1 – 7, edition 2000:
  Standard of functional safety of electrical/electronic/programmable electronic safety-related systems (product manufacturer)
- Electromagnetic compatibility:
  - EN 61326-1:2006
  - NE 21:2006

System specific standards and directives

- Functional safety IEC 61511 part 1 – 3, edition 2003:
  Standard of functional safety: safety instrumented systems for the process industry sector (user)

2 Planning

2.1 System Structure

2.1.1 Low Demand Mode

If there are two loops, one for the standard operation and another one for the functional safety, then usually the demand rate for the safety loop is assumed to be less than once per year.

The relevant safety parameters to be verified are:

- the PFD_{avg} value (average **P**robability of **F**ailure on **D**emand) and T_{proof} (proof test interval that has a direct impact on the PFD_{avg})
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance architecture)

2.1.2 High Demand Mode

If there is only one loop, which combines the standard operation and safety related operation, then usually the demand rate for this loop is assumed to be higher than once per year.

The relevant safety parameters to be verified are:

- PFH (**P**robability of dangerous **F**ailure per **H**our)
- Fault reaction time of the safety system
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance architecture)

225538 2011-04

2.2 Assumptions

The following assumptions have been made during the FMEDA analysis:

- Failure rates are constant, wear out mechanisms are not included.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed Classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
  - IEC 60654-1 Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40 °C. Humidity levels are assumed within manufacturer's rating. For a higher average temperature of 60 °C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.
- Failure rate based on the Siemens SN29500 data base.
- It was assumed that the appearance of a safe error (e. g. output in safe state) would be repaired within 8 hours.
- During the absence of the device for repairing, measures have to be taken to ensure the safety function (for example: substitution by an equivalent device).
- For high currents and high ambient temperature the de-rating given in the data sheet needs to be considered.
- The input of the device must be connected to a safety PLC which has minimum the SIL needed in the loop.
- The device shall claim less than 10 % of the total failure budget for a SIL3 safety loop.
- For a SIL3 application operating in Low Demand Mode the total PFD_{avg} value of the SIF (**S**afety **I**nstrumented **F**unction) should be smaller than 10^{-3}, hence the maximum allowable PFD_{avg} value would then be 10^{-4}.
- For a SIL3 application operating in High Demand Mode of operation the total PFH value of the SIF should be smaller than 10^{-7} per hour, hence the maximum allowable PFH value would then be 10^{-8} per hour.
- Since the circuit has a Hardware Fault Tolerance of **0** and it is a type **A** component, the SFF must be > 90 % according to table 2 of IEC 61508-2 for SIL3 (sub)system.

2.3 Safety Function and Safe State

DTS

Safety Function

The safety function of the device is defined: Whenever the input of the device is de-energized, the DTS output is not conducting.

Safe State

For the DTS safety function the safe state is defined as the DTS output being open (not conducting).

Reaction Time

The reaction time is < 20 ms.

ETS

Safety Function

The safety function of the device is defined: Whenever the input of the device is energized, the ETS output is conducting.

Safe State

For the ETS safety function the safe state is defined as the ETS output being closed (conducting).

Reaction Time

The reaction time is < 20 ms.

DPS

The dual pole switching application is no safety application.

General

For all applications the maximum switching frequency is limited to 10 Hz.

225538 2011-04

2.4 Characteristic Safety Values

Parameters acc. to IEC 61508	Variables	
Assessment type and documentation	Full assessment	
Pepperl+Fuchs FMEDA report [1]	FS-0042EA-20A	
Device type	A	
Demand mode	Low Demand Mode or High Demand Mode	
Safety function [2]	ETS [4]	DTS
HFT	0	0
SIL	3	3
$\lambda_{sd} + \lambda_{su}$	139.7 FIT	144.77 FIT
λ_{dd}	0 FIT	0 FIT
λ_{du}	7.1 FIT	1.83 FIT
$\lambda_{total\ (safety\ function)}$	146.6 FIT	146.6 FIT
SFF	95.2 %	98.7 %
MTBF [3]	639 years	560 years
PFH	7.1×10^{-9} 1/h	1.83×10^{-9} 1/h
PFD_{avg} for T_1 = 1 year	3.1×10^{-5}	8.01×10^{-6}
T_{proof} max.	3 years	12 years
Reaction time	< 20 ms	

[1] Pepperl+Fuchs documentation number

[2] The device can be used in two safety functions, ETS (energized to safe) and DTS (de-energized to safe).

[3] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h.

[4] For ETS in SIL2 applications no proof test has to be carried out, the calculated proof time is higher than the useful time (T_{proof} max. for ETS SIL2 is 32 years).

The characteristic safety values like PFD/PFH, SFF, HFT and T_{proof} are taken from the SIL report/FMEDA report. Please note, PFD and T_{proof} are related to each other.

The function of the devices has to be checked within the proof test interval (T_{proof}).

225538 2011-04

3 Safety Recommendation

3.1 Interfaces

The device has the following interfaces. For corresponding terminals see data sheet.

- Safety relevant interfaces: input, output I (ETS), output II (DTS)
- To avoid contact welding in DTS application we recommend to use a serial fuse in the load circuit. This can be the internal fuse F1 or any external fuse of max. 5 A nominal value.
- Test input interface may not be used during normal operation (only for proof test)

3.2 Configuration

A configuration of the device is not necessary and not possible.

ETS, DTS and DPS can be selected by using the referring terminals. See data sheet. The fuse in delivery status (2.5 A) can be changed to max 5 A. Please note the temperature derating according to the data sheet.

3.3 Useful Life Time

Although a constant failure rate is assumed by the probabilistic estimation this only applies provided that the useful life time of components is not exceeded. Beyond this useful life time, the result of the probabilistic calculation is meaningless as the probability of failure significantly increases with time. The useful life time is highly dependent on the component itself and its operating conditions – temperature in particular (for example, the electrolytic capacitors can be very sensitive to the working temperature).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that failure calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful life time of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful life time is valid.

However, according to IEC 61508-2, a useful life time, based on experience, should be assumed. Experience has shown that the useful life time often lies within a range period of about 8 ... 12 years.

225538 2011-04

Our experience has shown that the useful life time of a Pepperl+Fuchs product can be higher

- if there are no components with reduced life time in the safety path (like electrolytic capacitors, relays, flash memory, opto coupler) which can produce dangerous undetected failures and
- if the ambient temperature is significantly below 60 °C.

Please note that the useful life time refers to the (constant) failure rate of the device. The effective life time can be higher.

Maximum Switching Power of Output Contacts

The useful life time is limited by the maximum switching cycles under load conditions. You can see the relationship between the maximum switching power and the load conditions in the diagram below.

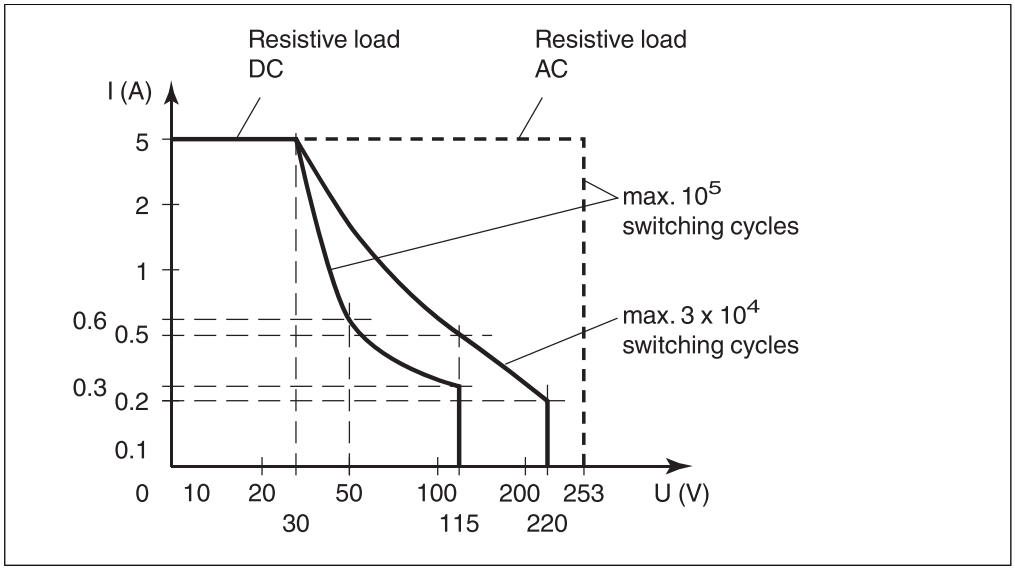


Figure 3.1

3.4 Installation and Commissioning

Installation has to consider all aspects regarding the SIL level of the loop. During installation or replacement of the device the loop has to shut down. Devices have to be replaced by the same type of devices.

4 Proof Test

4.1 Proof Test Procedure

According to IEC 61508-2 a recurring proof test shall be undertaken to reveal potential dangerous fails that are otherwise not detected by diagnostic test.

The functionality of the subsystem must be verified at periodic intervals depending on the applied PFD_{avg} in accordance with the data provided in see chapter 2.4.

It is under the responsibility of the operator to define the type of proof test and the interval time period.

The ancillary equipment required:

- A digital multimeter (without special accuracy) will be used as ohmmeter (mid range recommended) to check the relay outputs. Closed contacts are shown with 0 Ω (low impedance), open contacts are shown with OL (overload/high impedance).
- Power supply set at nominal voltage of 24 V DC

Procedure:

For the proof test five tests have to be done as shown in the following table and pictures:

Test No.	Input or Test Input	Output (mA)
1	$V_{test\ input}$ = 24 V DC between terminals 10+, 11-	■ DTS output (terminals 5, 6): OL (overload) ■ ETS output (terminals 2, 3): shows 0 Ω ■ Red LED TST1 is flashing.
2	$V_{test\ input}$ = 24 V DC between terminals 11-, 12+	■ DTS output (terminals 5, 6): OL (overload) ■ ETS output (terminals 2, 3): shows 0 Ω ■ Red LED TST2 is flashing.
3	$V_{test\ input}$ = 24 V DC between terminals 10+, 11- and between terminals 11-, 12+	■ DTS output (terminals 5, 6): shows 0 Ω ■ ETS output (terminals 2, 3): shows 0 Ω ■ Both red LEDs are flashing.
4	$V_{test\ input}$ = 0 V DC between terminals 10+, 11- and between terminals 11-, 12+	■ DTS output (terminals 5, 6): OL (overload) ■ ETS output (terminals 2, 3): OL (overload) ■ Both red LEDs are off.
5	V_{input} = 24 V DC between terminals 7+ and 8- and with changed input polarity between terminals 7-, 8+	■ DTS output (terminals 5, 6): shows 0 Ω ■ ETS output (terminals 2, 3): shows 0 Ω ■ Yellow LED is on.

Table 4.1 Expected test results for a successful proof test

225538 2011-04

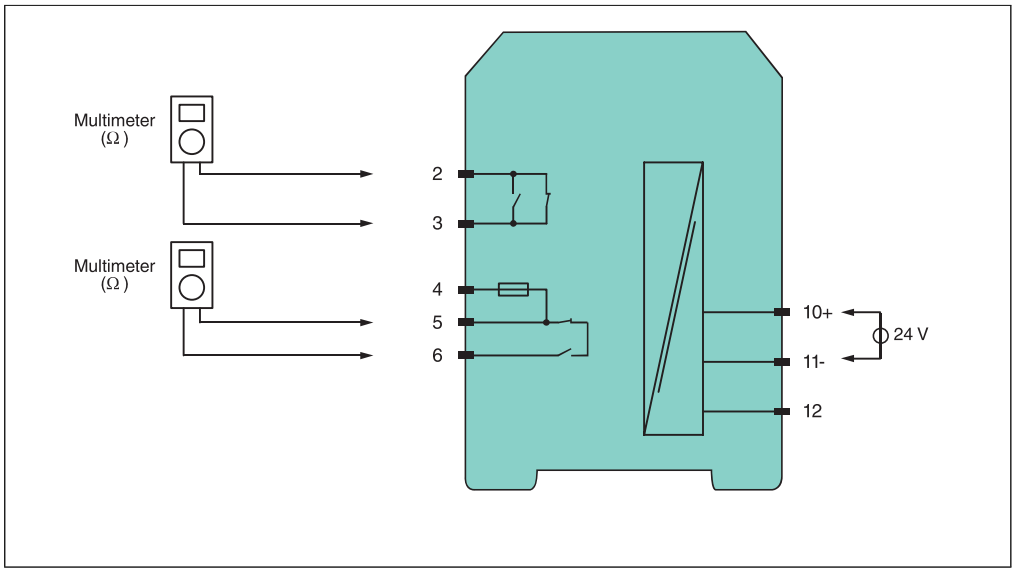


Figure 4.1 Proof test set-up for KFD0-RSH-1.4S.PS2, test 1

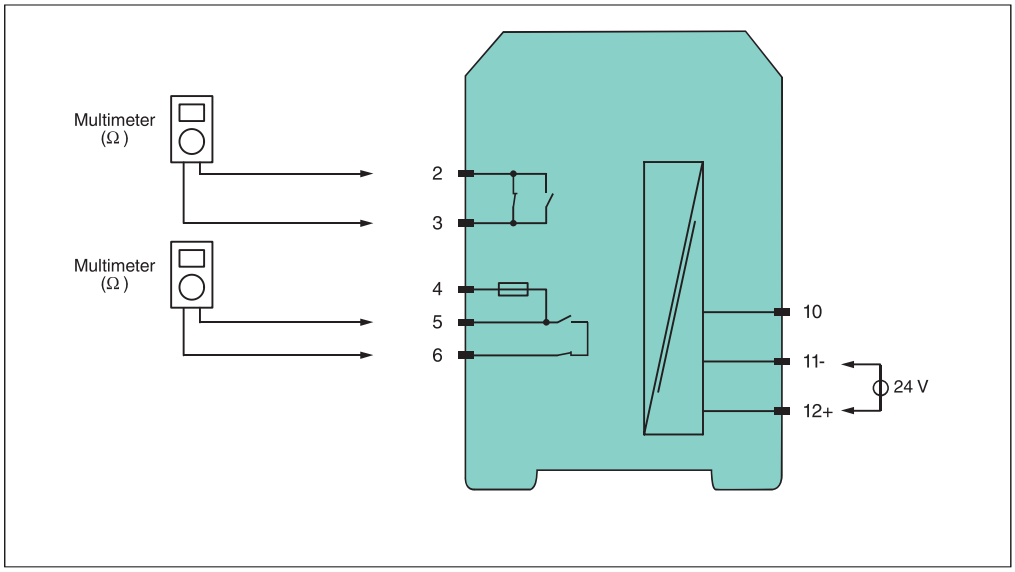


Figure 4.2 Proof test set-up for KFD0-RSH-1.4S.PS2, test 2

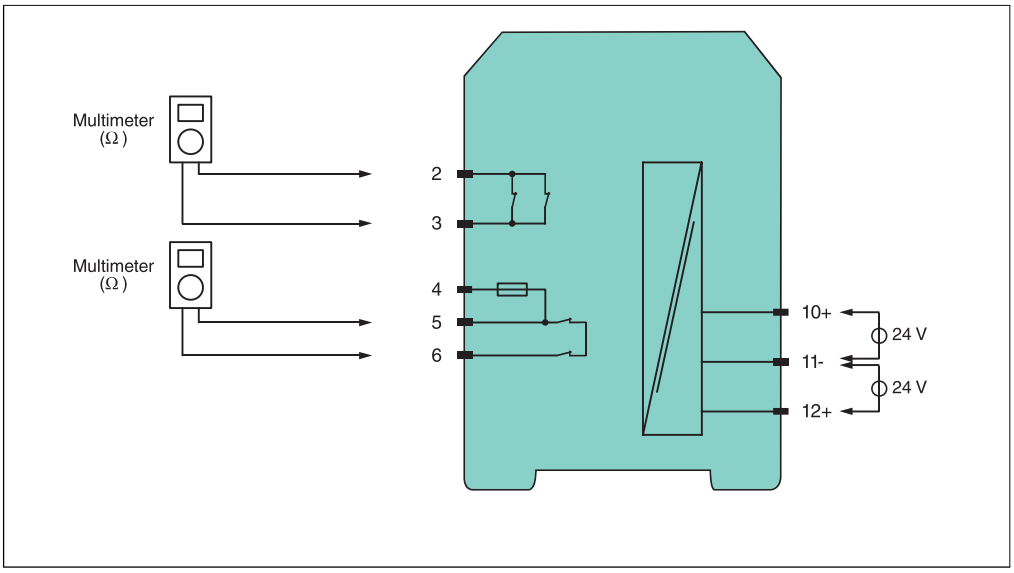


Figure 4.3 Proof test set-up for KFD0-RSH-1.4S.PS2, test 3

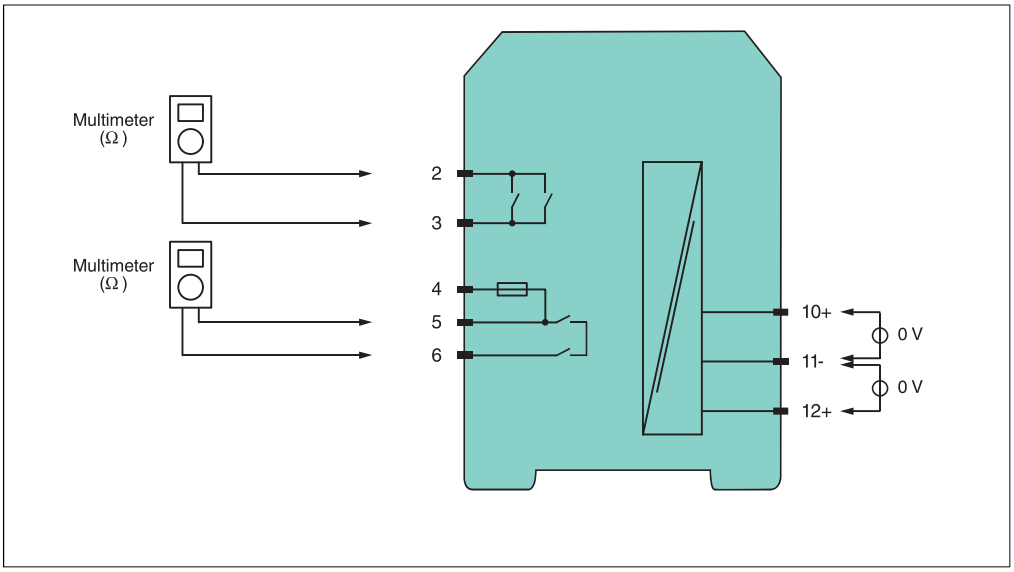


Figure 4.4 Proof test set-up for KFD0-RSH-1.4S.PS2, test 4

225538 2011-04

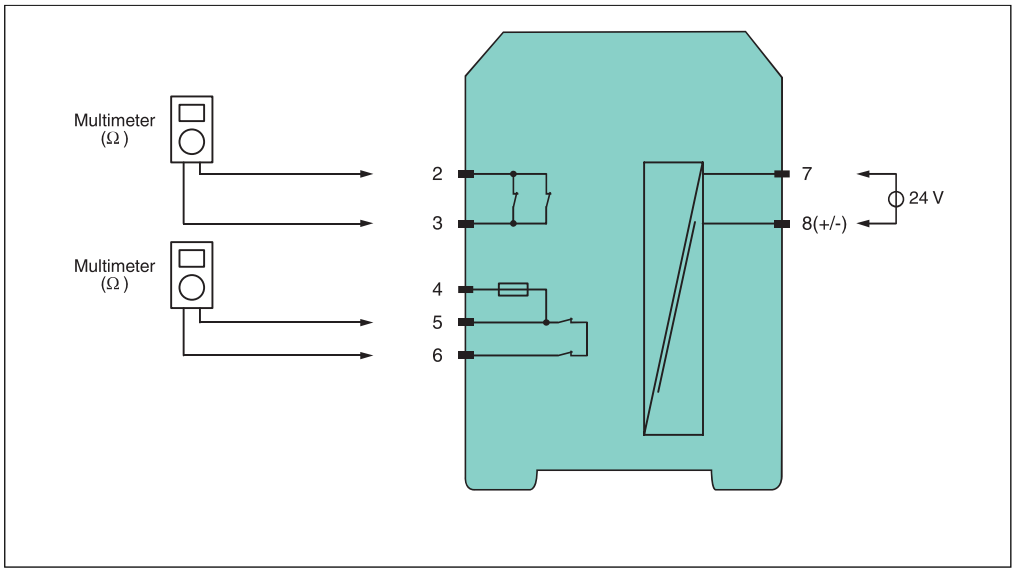


Figure 4.5 Proof test set-up for KFD0-RSH-1.4S.PS2, test 5

Only if all tests are successfully done, the proof test is successfull.

5 Abbreviations

FMEDA	**F**ailure **M**ode, **E**ffects and **D**iagnostics **A**nalysis
HFT	**H**ardware **F**ault **T**olerance
PFD_{avg}	Average **P**robability of **F**ailure on **D**emand
PFH	**P**robability of dangerous **F**ailure per **H**our
PTC	**P**roof **T**est **C**overage
SFF	**S**afe **F**ailure **F**raction
SIF	**S**afety **I**nstrumented **F**unction
SIL	**S**afety **I**ntegrity **L**evel
SIS	**S**afety **I**nstrumented **S**ystem
T_{proof}	Proof Test Interval
DPS	**D**ual **P**ole **S**witching
DTS	**D**e-energized **T**o **S**afe State
ESD	**E**mergency **S**hut **D**own
ETS	**E**nergized **T**o **S**afe State

225538 2011-04

225538 2011-04

PROCESS AUTOMATION – PROTECTING YOUR PROCESS





Worldwide Headquarters
Pepperl+Fuchs GmbH
68307 Mannheim · Germany
Tel. +49 621 776-0
E-mail: info@de.pepperl-fuchs.com

For the Pepperl+Fuchs representative
closest to you check www.pepperl-fuchs.com/pfcontact

www.pepperl-fuchs.com

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

225538 TDOCT-2052CENG
04/2011

Subject to modifications
Copyright PEPPERL+FUCHS • Printed in Germany

exida® CERTIFICATION

CERTIFICATE

P+F 100397R1C P0006 C04.2

exida Certification S.A. hereby confirms that the

Relay Module KFD0-RSH-1.4S.PS2

Product Version: 05-6166

Pepperl+Fuchs GmbH

Mannheim, Germany

Has been assessed per the relevant requirements of

IEC 61508:2000

Parts 1 - 2, and meets requirements providing a level of integrity to

Systematic Integrity : SIL 3 Capable

Random Integrity : SIL 3 Capable

Safety function

The Relay Module KFD0-RSH-1.4S.PS2 shall provide the following two Type A safety functions for applications in low or high demand mode of operation:

1. DTS - De-energize To trip (Safe) the relay output when the input is de-energized..
2. ETS - Energize To activate (Safe) the relay output when the input is energized.

Application Restrictions

The unit must be properly designed and validated in a Safety Instrumented Function per the requirements in the Safety Manual.

Assessors

Certifying Assessor

Date: 3 May 2011

exida Certification SA, Nyon, Switzerland

CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証

exida® CERTIFICATION

CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証

Systematic Integrity: SIL 3 Capable

SIL 3 Capability

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than the statement.

Random Integrity: SIL 3 Capable

Summary for KFD0-RSH-1.4S.PS2
Type A device,
IEC 61508 failure rates:

Failure category	DTS	ETS
Fail Safe (λ_{SAFE})	144.77	139.5
Fail Dangerous Detected (λ_{DD})	0	0
Fail Dangerous Undetected (λ_{DU})	1.83	7.1
Total failure rate (safety function)	146.6	146.6
SFF	98.7 %	95.2 %

All failure rates are given in FIT=10^{-9}/h

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} / PFH considering the architecture, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are mandatory part of this certificate:

P+F 1003-97R1-C R017 V1R2 Assessment Report
Safety Manual Relay Module KFD0-RSH-1.4S.PS2 Ver: 225538 DOCT-2052C 04 2011

The holder of this certificate may use this mark.