Base Load Power Hub (BLPH)

Safety System (ESD, Fire and Gas) Specification

Document Number: 123A90-DDL-IN-SP-40100

Document Class: Class 1

00	23/11/2023	Issue for Review (IFR)	AGS	AMBE/LCA	OYF/MDO
Rev.	Date	Description	Prepared	Reviewed	Approved

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

Revision / Change Log

Rev.	Description
0	Issue for Review (IFR)

HOLDS LIST

No.	Description
HOLD-1	The requirement of dedicated station for Sequence of Events.
HOLD-2	HVAC Design Basis specification document reference

Table of contents

1 INTRODUCTION 7
1.1 PROJECT OVERVIEW 7
1.1.1 Project Location 7
1.1.2 Project Concept 8
2 PURPOSE 10
3 REFERENCES 12
4 DEFINITIONS AND ABBREVIATIONS 14
5 Applicable Codes, Standards, and Regulations 18
5.1 General 18
5.2 Regulations 18
5.3 DEP 18
5.3.1 Fully Applicable DEP 18
5.3.2 DEM-1 Process Safety Only DEP 19
5.4 Industry Standards 19
6 GENERAL REQUIREMENTS 20
6.1 Environmental Conditions 20
6.2 Hazardous Area Certification 20
6.3 EMC Compliance 20
6.4 Equipment Noise 20
6.5 Fire-fighting flooding Systems 20
7 CYBER SECURITY 21
8 SCOPE OF WORK 22
8.1 General 22
8.2 Equipment 22
8.3 Communication with Onshore Facilities 23
8.4 Services 23

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

9 TECHNICAL REQUIREMENTS 25

9.1 General 25
9.1.1 Basic Design 25
9.1.2 Operator Interface or HMI 26
9.1.3 Maintainability 27
9.1.4 High Reliability, Availability and Fault Tolerance 27
9.1.5 SIL Requirements 28
9.1.6 Safety 28
9.1.7 Modular and Flexible 28
9.1.8 Electro-Magnetic Interference (EMI) 28
9.1.9 Voting Logic 28
9.2 System Architecture 28
9.3 System Hardware General Requirements 28
9.3.1 Power Supply Modules 29
9.3.2 Processor Modules 29
9.3.3 I/O Modules 30
9.4 Safety System networks (SIS and FGS) 32
9.4.1 Safety Networks 32
9.4.2 Network Components 32
9.5 Time Synchronisation 33
9.6 Software Requirements 33
9.6.1 Engineering Work Station (EWS) 34
9.7 System Performances 35
9.8 System Testing and Fault Diagnostics 35
9.9 Interface with Third Party Systems 36
9.9.1 Interface with the PAS network 36
9.9.2 Interface with LV switchboard 36
9.9.3 Interface with Packages 36
9.10 System and Marshalling Cabinets 36
9.11 Cables and Wiring 37
9.11.1 Cable Colours Coding 37
9.12 Labelling and Numbering System 38
9.13 Earthing 38

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

9.14 Electrical Supply 38
9.15 Spare Capacity 38
10 DOCUMENTATION 39
10.1 General 39
10.2 Documentation Requirements 39
10.3 Documentation to be provided with the System 39
10.4 Documents Presentation 40
11 INSPECTION AND TESTING 41
11.1 General Requirements 41
11.2 General 41
11.2.1 Test Documentation 42
11.3 Factory Acceptance Tests (FAT) 43
11.4 Integrated Factory Acceptance Test (IFAT) 46
11.5 Site Activities at Worksite 47
12 PACKING AND SHIPMENT 48
13 SPARE PARTS 49
14 SIZING REQUIREMENTS 50
14.1 Hardware Signals 50
14.2 Software signals 50

List of Figures

Figure 1 HOLLANDSE KUST NOORD WIND PARK Location Map 7
Figure 2 - Wind Park Details 8
Figure 3 – BLPH Concept 8

List of tables

Table 1 - Reference Documents 13
Table 2 - Definitions and Abbreviations 14
Table 4 Regulations 18
Table 5- DEP 18
Table 6 Process Safety DEP 19
Table 7 Industry standards 19

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

1 INTRODUCTION

1.1 PROJECT OVERVIEW

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

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

1.1.1 Project Location

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

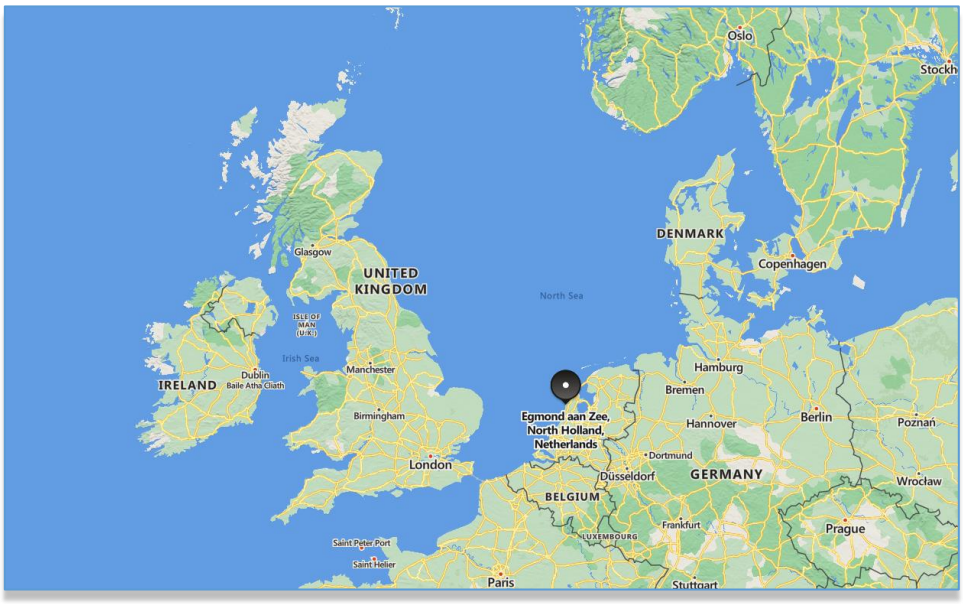


Figure 1 HOLLANDSE KUST NOORD WIND PARK Location Map

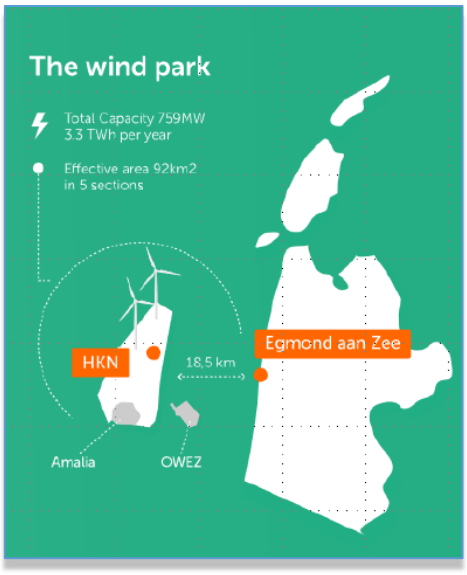


Figure 2 - Wind Park Details

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

1.1.2 Project Concept

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

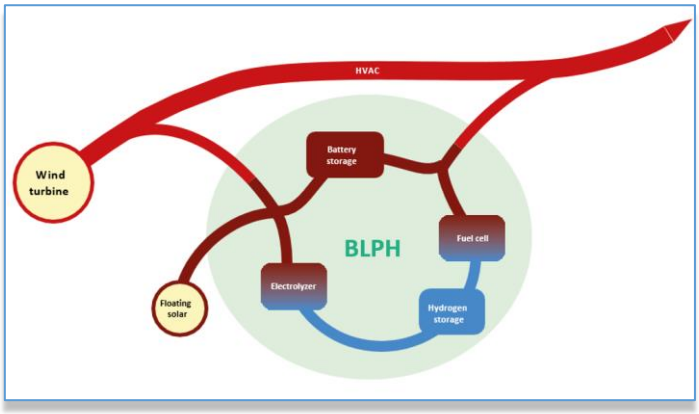


Figure 3 – BLPH Concept

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

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

2 PURPOSE

The purpose of the of the document is to define the functional requirements and the minimum acceptable technical requirements for delivering the Safety system to be used for BLPH project.

The design of the Safety System shall adhere to IEC 61511 and shall comprise of all elements of the SIS and FGS and shall undertake protection or mitigation actions within the process and utility plants.

The Safety System shall perform the following main functions:

- Emergency Shutdown (SIS)
- Fire and Gas Detection and Protection (FGS)
- Critical Action Panel (CAP)
- Sequence of Events (SOE) (HOLD-1)
- Interface with CAP controller at CCR through redundant on-shore Safety Network

Emergency Shut-Down system (SIS) and Fire and Gas System (FGS) shall be interconnected, but independent and there shall be no single point of failure of any element which could lead to an emergency shutdown or result in a loss of production, including an interruption to the hydrogen storage or power generation systems. All elements of the Safety system are to be designed for continuous Protection and Mitigation. All Safety System equipment shall communicate over the Safety Network. All SIS and FGS elements shall communicate as direct point-to-point control using the 4-20mA Smart HART revision 7 protocol including Fire and Gas detectors.

The SS shall provide an independent layer of protection on top of the CCS. The CCS shall not impact the ability of the Safety System to execute the protective and mitigation actions. All Safety System functionality shall be provided to the Remote CCR to ensure effective and safe control of the facility. This will be called upon when the operational personnel cannot mitigate the potential risk. The SIS shall activate safety critical functions and act to isolate the plant via any emergency shutdown valves. The SIS acts, based on a process excursion, to shutdown individual equipment and prevent a hazard from occurring.

The main function of the Fire and Gas System (FGS) is the detection of fire or gas incidents. FGS system will undertake mitigation actions within the process and utility plant on the detection of fire or gas release. It shall include all fire and gas detection and mitigation systems required for the individual fire zones.

All functions of the SIS and FGS shall be automatic in line with the Cause and Effects Diagrams provided by the project, including the vendor packaged equipment. A Critical Action Panel (CAP) shall be software based located at CCR for SIS and FGS functions.

All functional processing equipment of the Safety System shall be located in the ITER.

Provision shall be included for a Demand on Safety System tool that can provide information on genuine SIF activations. This information is required in order to compare actual and predicted demands of each SIF.

The safety system shall be supplied as completely pre-wired and tested systems. VENDOR shall note that all accessories should be supplied as a completely assembled unit to meet the operation requirements. VENDOR is expected to make optimum use of his standard range of equipment to provide as a minimum, the functional requirements as stated in this specification. To the extent possible and practical, the systems

supplied shall be based on VENDOR's standard hardware and software, avoiding any special or customised design for this particular installation. In case where special design cannot be avoided, the description shall positively state so in VENDOR's proposal, otherwise it is taken that VENDOR's standard design is provided. Any deviation with this specification at any stage of the project will require to be approved by COMPANY.

3 REFERENCES

The design of the Safety System shall be based on the requirements described on the following documents. VENDOR shall read, understand, and take into account all requirements indicated in this specification and in all referenced document listed below.

Doc. No.	Description
123A90-DDL-PRE-RE-80040	PROCESS DESIGN PHILOSPHY
123A90-DDL-IN-DD-40096	CONTROL SYSTEMS ARCHITECTURE DRAWING
123A90-DDL-IN-RE-40093	CONTROL SYSTEM PHILOSOPHY
123A90-DDL-IN-SP-40097	SYSTEM SPECIFICATION FOR MAIN AUTOMATION CONTRACTOR
123A90-DDL-SAF-DL-30027	F AND G DETECTORS LAYOUT – LOWER DECK
123A90-DDL-SAF-DL-30028	F AND G DETECTORS LAYOUT – UPPER DECK
123A90-DDL-SAF-RE-30001	FIRE PROTECTION PHILOSOPHY
123A90-DDL-SAF-RE-30046	HSE DESIGN PHILOSOPHY
123A90-DDL-IN-SP-40006	SIS SAFETY REQUIREMENT SPECIFICATION (SRS)
123A90-DDL-IN-DL-40012	LAYOUT DRAWINGS (ONSHORE CCR, OFFSHORE ITER)
123A90-DDL-PR-PID-80009	BLPH PIPING AND INSTRUMENTATION DIAGRAM GENERAL NOTES
123A90-DDL-PR-PID-80010	BLPH PIPING AND INSTRUMENTATION DIAGRAM PIPING SYMBOLOGY
123A90-DDL-PR-PID-80011	BLPH PIPING AND INSTRUMENTATION DIAGRAM ELECTROLYSER PACKAGE
123A90-DDL-PR-PID-80012	BLPH PIPING AND INSTRUMENTATION DIAGRAM FUEL CELL PACKAGE
123A90-DDL-PR-PID-80013	BLPH PIPING AND INSTRUMENTATION DIAGRAM HYDROGEN STORAGE VESSELS HEADER (INLET)
123A90-DDL-PR-PID-80014	BLPH PIPING AND INSTRUMENTATION DIAGRAM HYDROGEN STORAGE VESSELS HEADER (OUTLET)
123A90-DDL-PR-PID-80015	BLPH PIPING AND INSTRUMENTATION DIAGRAM HYDROGEN STORAGE VESSEL A
123A90-DDL-PR-PID-80016	BLPH PIPING AND INSTRUMENTATION DIAGRAM HYDROGEN STORAGE VESSEL B
123A90-DDL-PR-PID-80017	BLPH PIPING AND INSTRUMENTATION DIAGRAM HYDROGEN STORAGE VESSEL C

123A90-DDL-PR-PID-80018	BLPH PIPING AND INSTRUMENTATION DIAGRAM HYDROGEN STORAGE VESSELD
123A90-DDL-PR-PID-80019	BLPH PIPING AND INSTRUMENTATION DIAGRAM HYDROGEN STORAGE VESSEL E
123A90-DDL-PR-PID-80020	BLPH PIPING AND INSTRUMENTATION DIAGRAM HYDROGEN STORAGE VESSEL F
123A90-DDL-PR-PID-80021	BLPH PIPING AND INSTRUMENTATION DIAGRAM SEA-WATER INTAKE SYSTEM SHEET 1
123A90-DDL-PR-PID-80022	BLPH PIPING AND INSTRUMENTATION DIAGRAM SEA-WATER INTAKE SYSTEM SHEET 2
123A90-DDL-PR-PID-80023	BLPH PIPING AND INSTRUMENTATION DIAGRAM WATER TREATMENT PLANT SHEET 1
123A90-DDL-PR-PID-80024	BLPH PIPING AND INSTRUMENTATION DIAGRAM WATER TREATMENT PLANT SHEET 2
123A90-DDL-PR-PID-80025	BLPH PIPING AND INSTRUMENTATION DIAGRAM WATER DISPOSAL SHEET 1
123A90-DDL-PR-PID-80026	BLPH PIPING AND INSTRUMENTATION DIAGRAM WATER DISPOSAL SHEET 2
123A90-DDL-PR-PID-80027	BLPH PIPING AND INSTRUMENTATION DIAGRAM INSTRUMENT AIR PACKAGE
123A90-DDL-PR-PID-80028	BLPH PIPING AND INSTRUMENTATION DIAGRAM HYDROGEN VENT HEADER
123A90-DDL-PR-PID-80029	BLPH PIPING AND INSTRUMENTATION DIAGRAM HYDROGEN VENT DRUM
123A90-DDL-IN-DD-40019	DATA NETWORK ARCHITECTURE DRAWINGS
123A90-DDL-IN-RE-40023	CYBER SECURITY DESIGN PHILOSOPHY
123A90-DDL-IN-MR-40103	MR - AUTOMATION SYSTEMS CCS-SIS
123A90-PML-COM-PRO-03039	PRESERVATION PROCEDURE
123A90-DDL-IN-LIS-40090	INSTRUMENT I/O SERIAL MAPPING LIST
123A90-DDL-IN-LIS-40027	MASTER ALARM DATABASE

Table 1 - Reference Documents

4 DEFINITIONS AND ABBREVIATIONS

2.3.1 DEFINITIONS

COMPANY or Client (CPY):	Crosswind
CONTRACTOR (CTR):	ROSETTI MARINO S.p.A.
PROJECT:	HOLLANDSE KUST NOORD WIND PARK Project
VENDOR:	Means any supplier of goods
Shall:	An absolute requirement.
Should:	This word indicates a recommendation that whilst preferred may not be implemented provided some equivalent is proposed and agreed by COMPANY. The full implications must be understood and carefully weighed before choosing a different course.

Table 2 - Definitions and Abbreviations

2.3.2 ABBREVIATIONS

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
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)
CSU	Commissioning & Start-Up
CW	CrossWind
CWHKN	CrossWind Hollandse Kust Noord
DEM	Design Engineering Manual
DEP	Design Engineering Practice
EMC	Electromagnetic Compatibility
EPC	Engineering, Procurement & Construction

EPCI	Engineering Procurement Construction Installation
EPIRB	Emergency Position Indicating Radio Beacon
ESD	Emergency Shutdown
EU	European Union
EWS	Engineering Workstation
Ex	Explosion Proof
F&G	Fire & Gas
FC	Fuel Cell
FEED	Front End Engineering Design
FERA	Fire and Explosion Risk Analysis
FGS	Fire & Gas System
FO	Fibre Optic
FOC	Fibre Optic Cable
FOPP	Fibre Optic Patch Panel
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positional Satellite
HART	Highway Addressable Remote Transducer
HAZID	Hazard Identification
HAZOP	Hazard and Operability Analysis
HFE	Human Factors Engineering
HKN	Hollandse Kust Noord
HLV	Heavy Lift Vessel
HMI	Human Machine Interface
HP	High Pressure
HRA	Health Risk Assessment
HS(S)E	Health, Safety, (Security) and Environment
HV	High Voltage
HVAC	Heating Ventilation and Air Conditioning
I/O	Input/Output
IACS	Industrial Automation and Control Systems
IAMS	Instrument Asset Management System

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

IEC	International Electrotechnical Commission
IP	Ingress Protection / Internet Protocol
IS	Intrinsically Safe
ISO	International Organization for Standardization
ITER	Instrument & Telecoms Equipment Room
LAN	Local Area Network
LOPA	Layers of Protection Analysis
LV	Low Voltage
MAC	Main Automation Contractor
MSL	Mean Sea Level
MW	Mega Watt
NAMUR	Interessengemeinschaft Automatisierungstechnik der Prozessindustrie (User Association of Automation Technology in Process Industries)
NIS	Non-Intrinsically Safe
NUI	Normally Unmanned Installation
O&M	Operation & Maintenance
OCC	Onshore Commissioning Complete
OEM	Original Equipment Manufacturer
OHVS	Offshore High Voltage Station
OITC	Onshore Integrated Test Complete
OPCC	Onshore Process Commissioning Complete
OUCC	Onshore Utility Commissioning Complete
OWNER	Crosswind
OWS	Operator Workstation
P&ID	Piping & Instrumentation Diagram
PACO	Process, Automation, Control and Optimisation
PAGA	Public Address and General Alarm
PAU	Pre-Assembled Units
PCS	Power Conversion System
PCU	Package Control Unit

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

PFS	Process Flow Scheme
PLC	Programmable Logic Controller
POB	Personnel on Board
RAM	Reliability, Availability & Maintainability (O&M)
RAM	Risk Assessment Matrix (Safety)
RTD	Resistance Temperature Detector
SCADA	Supervisory Control and Data Acquisition
SCE	Safety Critical Element
SFP	Small Form-Factor Pluggable
SGSI	Shell Global Solutions International
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SLD	Single Line Diagram
SN	Safety Network
TCP/IP	Transmission Control Protocol/Internet Protocol
UCP	Unit Control Panel
UFD	Utility Flow Diagram
UPS	Uninterrupted Power Supply
VHF	Very High Frequency
VIV	Vortex Induced Vibration
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WTG	Wind Turbine Generator
CCS	PCS + EMCS
SS	Safety System (SIS + F&G)

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

5 APPLICABLE CODES, STANDARDS, AND REGULATIONS

5.1 GENERAL

The Safety system shall be designed, manufactured, tested, and delivered in accordance with the philosophy, Project documents, codes, standards, and regulations listed below. It is the VENDOR responsibility to ensure complete compliance in their design, inclusive of all sub-vendors. The normative documents listed below contain requirements that, through reference in this text, constitute the requirements of this Project. Latest editions of all referenced documents shall apply.

The project shall apply relevant Standards and Codes as detailed in this Part. Where there is a conflict of requirements the more conservative standard or code shall be followed. In all other cases the following order of precedence shall be adhered to:.

1. Regulations
2. Selected DEM-1 and DEM-2 requirements.
3. Industry Codes and Standards.

The applicable industry codes and standards are details in sections 6.2, 6.3 and 6.4..

5.2 REGULATIONS

Document Name	Document Title
1999/92/EC	ATEX 153 Workplace Directive
2011/65/EU	Directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment
2014/30/EU	Electromagnetic Compatibility (EMC) Directive
2014/34/EU	ATEX Directive
2014/35/EU	Low Voltage Directive
94/9/EC	Equipment intended for use in Potentially Explosive Atmospheres
99/92/EC	Minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres

Table 3 Regulations

5.3 DEP

5.3.1 Fully Applicable DEP

Document Name	Document Title
DEP 32.01.20.12	Industrial Automation and Control Systems (IACS) Security
DEP 30.00.60.15	Humans Factors Engineering – Control Room Design

Table 4- DEP

DEP 32.01.20.12 shall be applied to the project in full, in conjunction with IEC 62443, for the cybersecurity.

DEP 30.00.60.15 shall be applied to the project for the design of the Control Room.

5.3.2 DEM-1 Process Safety Only DEP

The following DEPs shall have the DEM-1 'Process Safety' requirements applied to the project.

Document Name	Document Title
DEP 32.30.20.11	Fire, Gas and Smoke Detections
DEP 32.80.10.10	Safety Instrumented Systems
DEP 32.80.10.14	Alarm Management (Amendment/Supplements to IEC 62682)
DEP 62.10.08.11	Inspection and Function Testing of Instruments

Table 5 Process Safety DEP

5.4 INDUSTRY STANDARDS

Document Name	Document Title
EN 1127	Explosive Atmospheres, Explosion Prevention and Protection, Basic Concepts and Methodology
EN 61131-3	Programmable Controllers, Part 3: Programming languages.
IEC 60079	Installation & Maintenance of Electrical apparatus for use in Potential explosive atmosphere
IEC 60364	Low-voltage Electrical Installations
IEC 60529	Degrees of Protection Provided by Enclosures (IP Code)
IEC 61158	Industrial communication networks
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511	Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Framework, Definitions, System, Hardware, and Application Programming Requirements
IEC 62305	Protection Against lightning
IEC 62443	Cyber Security for Industrial Automation and Control Systems
IEC 62682	Management of Alarm Systems for the Process Industries
ISO 14001	Environmental Management System
ISO 9001	Certifications of Quality Management System

Table 6 Industry standards

6 GENERAL REQUIREMENTS

6.1 ENVIRONMENTAL CONDITIONS

The Safety System shall be suitable for operation in the following normal (internal) environmental conditions:

- Temperature range: 15 to 25 °C
- Relative humidity: 30 to 70% RH
- Control room(s) Noise Level: < 70dB
- Equipment room(s) Noise level: Noise emission from any source shall be less than 70dB.

The atmosphere within control and equipment rooms shall be filtered.

The Safety System equipment located in onshore CCR and offshore ITER room shall be able to run without degradation or without affecting the overall systems, with HVAC failure. The equipment shall therefore be designed to operate under the following conditions:

- Design Temperature range: 5 to 45 °C
- Design Relative Humidity: 10 to 93% RH

For more details, please refer to the Project document "HVAC Design Basis specification", referenced HOLD-2

6.2 HAZARDOUS AREA CERTIFICATION

The onshore CCR and offshore ITER room is qualified as non-hazardous area.

6.3 EMC COMPLIANCE

The PAS operations shall be protected from electromagnetic exposure/ interference. VENDOR to ensure that the requirements for electromagnetic compatibility are considered during the various stages of design, construction, and installation. All aspects of the Safety system shall be certified to 2014/30/EU.

6.4 EQUIPMENT NOISE

Equipment supplied in onshore CCR and offshore ITER room must not produce a sound pressure level exceeding 65 dB (A) measured at one meter from the equipment cabinets. This includes safety system sub-assemblies, power supplies, printers, etc.

6.5 FIRE-FIGHTING FLOODING SYSTEMS

All control equipment and accessories installed in onshore CCR and offshore ITER room shall be designed as to withstand thermal variation and possible corrosion effects from flooding of fire extinguishing systems.

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

7 CYBER SECURITY

All network architecture and security for SIS shall be designed as per DEP 32.01.20.12 (IACS Security) and IEC 62243.

A cyber security risk assessment of the IACS, including the SIS, shall be carried out by the VENDOR to determine the necessary security controls and countermeasures required to reduce the cyber security risk to a level acceptable by the asset owner.

For more details, please refer to the Project document "Cyber Security Design Philosophy", referenced 123A90-DDL-IN-RE-40023 and "Data Network Design Specification", referenced 123A90-DDL-IN-SP-40018.

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

8 SCOPE OF WORK

8.1 GENERAL

As a minimum, the VENDOR shall be responsible for:

- The engineering, detailed design, procurement, manufacturing, assembly, configuration, wiring, supply, testing, quality assurance procedures and documentation of the safety system (SIS and FGS).
- The implementation of all application software(s) including system and user configuration and testing.
- Ensuring that the safety system supplied meets all the requirements of this specification.
- Supplying all items not specifically mentioned but necessary for the correct operation of the safety system.
- Supplying of Project deliverables as per section 9.4
- Supplying Assistance to Commissioning Activities Phase.
- Supplying assistance to Start-Up Activities Phase.

All correction or modification requested by the COMPANY/CONTRACTOR agreed by the VENDOR will be under VENDOR responsibility. VENDOR shall ensure that request is operable and safe regarding process and safety.

The VENDOR shall issue, as a minimum, all necessary layouts arrangement for COMPANY/CONTRACTOR approval.

Comments made by COMPANY/CONTRACTOR shall be fully taken into account. Any deviation in the implementation from comments previously made, will be under full responsibility of VENDOR and COMPANY will have the right to demand the implementation of all comments that have not been taken into account in any phase of the project.

8.2 EQUIPMENT

VENDOR is responsible for all supplies covered by the present specification and mainly summarized as follows for the safety system (SIS and FGS) part:

- Independent redundant controller set including communication interface modules for SIS and F&G. Panels containing the SIS system and F&G system, I/O and logic controllers shall be located in Offshore ITER.
- Engineering Workstation (EWS) in Onshore shall be Virtual Machine (VM) and Offshore shall be physical machine mounted in cabinet.
- Engineering Workstation /Operator Workstation (EWS/OWS) shall be supplied with all associated components (Common for PCS, EMCS, SIS and F&G).
- History and Backup server with all associated components (Common for PCS, EMCS, SIS and F&G).
- Software based Critical Action Panel (CAP) at CCR.

- All necessary system, marshalling, network and Server cabinets with all required components.
- All communication link cables and network cables and their necessary accessories between safety system equipment and other devices.
- Supply and engineer all hardware and software interface to allow communication between CCS network and safety system as required.
- Supply and engineer of Critical Action Panel (SIS and F&G functions) HMI Screens for operator interface.
- Supply of spare parts for start-up and commissioning including complete set of special tools required for lifting, removal, installation, testing and maintenance purposes and 2 years operation spare parts.
- Required software licenses.
- Any other equipment/software along with license that, despite not being indicated in this specification, is required for the correct and safe operation of the platform and systems.

8.3 COMMUNICATION WITH ONSHORE FACILITIES

The PAS bears overall responsibility for the control of the facility, and it shall operate independently of the Safety System. All SIS and F&G controllers associated with the PAS shall be located on the BLPH Offshore platform in the Instrument and Telecommunications Equipment Room (ITER). For further details refer the Project Document "Layout Drawings (Onshore CCR, Offshore ITER), referenced 123A90-DDL-IN-DL-40012

The interface between CCR and SIS controllers shall be through dedicated redundant safety network.

The interface between the CCR Critical Action Panel and Offshore SIS and F&G controller shall be through the Safety Network.

8.4 SERVICES

Services to be provided by VENDOR shall include the co-ordination and assistance to CONTRACTOR during the studies, FAT, SAT, start-up, and performance tests stages.

VENDOR responsibility shall include, but not be limited to, the following:

- Project management
- System detailed engineering
- System and application configuration and programming (Hardware and Software).
- Data base design (system and communication)
- System documentation (Standard and user)
- Recommended installation procedures
- Commissioning procedure
- Commissioning spare parts list and consumable items for Start-Up.

- Recommended two years operation spare parts and consumables.
- Interface communication protocols (Hardware & Software) with CCS network.
- Develop the data communication list between safety system and CCS network.
- System test procedure for shop and field tests.
- FAT procedures including as a minimum:
    - Hardware FAT procedure.
    - Software FAT procedure,
- Factory Acceptance Test (FAT) including as a minimum:
    - Hardware FAT.
    - Software FAT.
- Packing and shipment to job Site.
- Site services (Technical assistance during Start-Up and commissioning, Inspection, Tests, Training).
- SAT and dedicated procedures, including COMPANY's performance check out at the factory.
- Coordination with CONTRACTOR.
- Software licenses

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

9 TECHNICAL REQUIREMENTS

9.1 GENERAL

Safety system shall be made in accordance with Standards and specifications referenced in Section 6 Applicable Codes, Standards, and Regulations.

9.1.1 Basic Design

Emergency Shut-Down system (SIS) and Fire and Gas System (FGS) shall be interconnected, but independent and there shall be no single point of failure of any element which could lead to an emergency shutdown or result in a loss of production, including an interruption to the hydrogen storage or power generation systems.

Failure of one system shall not impair the functionality of any other subsystem of the SS. This applies to any subsystem within the SS or any part of the PAS in relation to the SS. The SS controllers shall operate independently, regardless of the condition of any other controller on the network or the network itself.

The SIS shall be based on programmable equipment and shall meet the requirements of IEC 61511 and be certified to use in SIL3 applications by an organization accredited by national accreditation authority to certify safety products as per IEC 61508.

No single failure shall cause a spurious trip nor degrade the ability to perform a trip on demand.

SIS shutdown functions shall be fail-safe. Digital loops shall use the "de-energized to trip" general principle (open circuit = trip) and shall be Normally Energized (NE) during normal operating periods (closed circuit = normal).

Digital output loops for total flooding inert gas systems shall use the "energized to trip" general principle (closed circuit = action) and shall be Normally De-Energized (NDE) during normal operating periods (open circuit = normal) with circuit monitoring. The loop integrity shall be continuously checked by line monitoring functions.

Safety system shall incorporate test facilities. Following dedicated functions shall be implemented:

- Periodic test routines.
- Automatic start-up & inhibit functions (according to detailed logic requirements).
- Maintenance inhibits, and reset functions as defined in functional analyses.
- Alarming / re-alarming of inhibit functions.

Safety System SIL Requirements shall be as defined by the Project SIL study. Each loop's required integrity level will be validated at the SIL Assessment Study based on IEC 61508 / IEC 61511 methodology. Refer Project document "SIS Safety Requirement Specification (SRS)", referenced 123A90-DDL-IN-SP-40006.

As a minimum, the safety system components (logic solver, I/O cards, relays, etc.) shall be "SIL 3 certified" (i.e. capable of supporting safety functions up to SIL-3).

The Safety System specified shall be designed, manufactured and configured to perform the main following operation tasks:

- Executive control (manual and automatic).
- Status monitoring and alarm displays via the PAS.
- Interfaces to PAS network.
- Hardwired links with other equipment (packages, other systems, etc.)
- Sequence of events (SOE) recording and analysis via PAS.
- System diagnostics.
- The safety system particular tasks are the following:
- Monitoring of process and plant safe operating conditions.
- Initiation of shutdown and electrical isolation.
- Fire detection.
- Gas detection.
- Interface with extinguishing systems (total flooding system, etc.).

The safety system shall consist of equipment having been field proven for at least two years. No module or component part of the safety system shall be listed on a manufacturer's planned obsolescence list (silver list).

VENDOR shall have at least three years proven previous experience in supplying safety systems of similar configuration and functionality.

Data from the safety system shall be integrated to the control network. For details refer to Project document "Control System Philosophy" referenced 123A90-DDL-IN-RE-40093.

The SIS shall interface directly with the F&G. The SIS interface with the F&G shall be bidirectional in that the SIS shall initiate actions through the F&G and vice versa.

9.1.2 Operator Interface or HMI

An Operator interface for the safety system shall be located in Onshore CCR and provide the operator with information and functionality to control and operate all emergency and essential systems. All shutdown and common system alarms, bypass, status indications from the safety system shall be displayed / annunciate on the CCR OWS.

The following typical information shall be available and visual to the operator:

- Activated inputs.
- Activated outputs.
- Acknowledge and reset facility.
- Audible and visual alarms.
- Indication of inhibits and overrides in the system.

- Common system alarms.
- Electronic dynamic Cause and Effect chart displays indicating the status of the inputs and outputs.
- Sequence of Events.

As a backup to the Operator station there shall be a functionally independent CAP.

In addition, a Safety System Engineering Workstation (EWS) shall be located in the Onshore CCR. The Safety System EWS will allow modification of system function under password and/or key protected access. Alarm handling systems shall be provided to allow operators to be advised of any abnormal operation. Dedicated displays shall be provided for the alarm system and include current alarm summary and alarm history displays.

9.1.3 Maintainability

The safety system shall have comprehensive self-test and diagnostics facilities. All faults shall be identified, alarmed and reported. The diagnostics shall clearly identify the faulty module. The results of diagnostics shall be made available to the Safety System EWS/OWS.

The safety system shall require minimal or no manual intervention. The automatic reconfiguration upon replacement of card shall occur. Hot replacement of module shall be possible without any special tools.

The safety system shall have capability of on-line software download from the EWS without shutdown of the process. Live download shall require security password to avoid unauthorized access.

The system application environment shall permit the user to make on-line changes without restarting the application to view display modifications. Access to all equipment for maintenance shall be provided.

9.1.4 High Reliability, Availability and Fault Tolerance

The basic requirement for the safety system design, manufacturing and utilization shall be to achieve very high degree of reliability and full availability in order to control all safe conditions and associated trip actions during operations on the platform.

The equipment shall be designed to minimize the downtime due to failures of the equipment itself or of the field mounted sensors. The safety system shall be designed so that a single failure shall not cause system malfunction and shutdown.

The VENDOR shall state the Mean Time Between Failure (MTBF) of the safety system where a failure is defined as an event which causes a spurious trip of the platform. The minimum required availability shall be for the safety system: 99.99%. Refer to Project document "SIS Safety Requirement Specification (SRS)", referenced 123A09-DDL-IN-SP-4006.

The maintenance cycle of this two (2) year project is expected to every six (6) months with the facility remaining unmanned otherwise. All equipment shall be designed such that no maintenance shall be required between visits. All software / electronic modifications shall be available to operations remotely, i.e., at CCR or onshore equipment room, via the engineering workstation.

9.1.5 SIL Requirements

The Safety System for Emergency Shut-Down System (SIS) shall be SIL 3 and Fire and Gas System (FGS) shall be SIL 1 certified. For F&G detection system, requirement shall be SIL 2.

9.1.6 Safety

The SIS shall be based on a "fail-safe" design (utilizing de-energize to trip principles).

The FGS shall be based on a "non-fail-safe" design (utilizing energize to trip principles).

Operating, maintenance and control procedures shall be designed to provide maximum safety for operating and maintenance personnel.

9.1.7 Modular and Flexible

The system shall be of modular design for easy maintenance and future expansion and modification.

The safety system shall be designed to minimize and reduce:

- Spare part quantities,
- Training for operators and maintenance technicians.

9.1.8 Electro-Magnetic Interference (EMI)

All equipment shall be capable of withstanding minimum electromagnetic interference and in addition shall only radiate a maximum electromagnetic field in order to prevent interference to other equipment according to 2014/30/EU.

9.1.9 Voting Logic

When a voting logic is to be implemented each signal shall be wired to a different I/O card. For example, in a 2oo3 voting logic, the three (3) sensors shall be connected to three (3) different I/O cards. Detector voting and resulting actions shall be as per the Project document "FIRE PROTECTION PHILOSOPHY" referenced as 123A90-DDL-SAF-RE-30001

9.2 SYSTEM ARCHITECTURE

For detailed system architecture refer Project document "Control System Architecture Detailed Drawings" referenced 123A90-DDL-IN-DD-40096

9.3 SYSTEM HARDWARE GENERAL REQUIREMENTS

Safety system (SIS and FGS) will be based on a fully redundant programmable system to achieve SIL 3 rating.

Safety Shutdown Systems (SIS) shall be based on fail safe design built using high reliability, high availability and at minimum full dual fault tolerant system.

FGS shall generally be of a non-fail-safe design utilizing "energize to trip" principles. It shall be built using high reliability, high availability and at minimum full dual fault tolerant system.

System components shall be modular in design with chassis' mounting and plug-in type assemblies. Modules shall be hot replaceable without requiring special tools.

Systems shall have self-diagnostic programs, running independently from the application programs, on a continuous basis with fault detection capability down to the I/O module individual channel.

All modules shall be on-line replaceable without degrading the system performance. Re-initialization of newly installed module will be automatic.

Each system module shall be equipped with light indicators for fault and status display. Systems shall provide full status information on PAS OWS.

All hardware shall be within Project Approved Vendor List. Special care shall be taken for communication switches and firewalls (if any).

9.3.1 Power Supply Modules

Safety system shall operate with dual redundant power supply modules. Each one shall be sized for the total power requirement of safety modules.

Diagnostic facilities as LEDs shall be provided to check running and fault of power supply. As for all modules, power supply shall be replaceable during operation with no impact on other modules.

The power supply modules shall be capable to receive 230V AC, 50Hz, TN-S - 1ph+N+PE.

9.3.2 Processor Modules

The SIS and F&G system shall be based on redundant controllers. All I/O shall be redundant in the Node.

Identical operating software and application programs, including fault history, residing in each processor memory shall be running independently.

Processors shall contain extensive diagnostic routines and execute diagnostic software which shall be capable of locating and reporting the following faults as a minimum:

- Watchdog timer
- Scan failure of main or I/O processors
- Memory faults in PROM or RAM
- Memory backup battery faults
- Microprocessor faults
- I/O interface or addressing faults
- I/O module faults
- Voted signal discrepancies on inputs / outputs
- Load power / fuse faults on field circuits
- Power supply faults.

Safety system Processor shall be Redundant.

Processors shall be provided with security to prevent unauthorized software modification.

VENDOR shall specify the minimum processor cycle time (maximum 250 ms).

Internal bus between modules (CPU, I/O and communication) shall be at minimum duplicated.

9.3.3 I/O Modules

The SIS and F&G system shall be based on redundant controllers. All I/O shall be redundant in the Node. I/O's shall be powered by 24V DC from the I/O cards or from the System Terminal Boards or for specific loops from the power supply terminal blocks located in the marshalling cabinets.

All I/O modules shall include line-monitoring facilities. Suitable End-of-Line (EOL) devices shall be provided for all line monitored I/O circuits.

All I/O shall be electrically isolated for protection against power supply, field surges and short circuits.

Each I/O module shall have LED's on the front face, reporting diagnostic fault, I/O circuit status, etc. Alarms and faults shall be displayed on the operator interface (PAS OWS).

I/O shall generally be certified to Eex "d" protection concept. Where intrinsically safe circuits are unavoidable, IS barriers used shall be of the galvanic isolator type certified Eex "i".

During operation, input and output modules shall be capable of being removed from or inserted into a fully powered and operational chassis without risk of damage.

Failure and subsequent replacement of an input or output module shall not affect other components or initiate a system failure.

I/O modules shall be capable of being replaced without removing the wiring between the module and the termination module.

VENDOR shall include slots for future I/O cards, terminal to accommodate future I/O expansion / modifications.

9.3.3.1 Analogue Inputs

Analogue input shall operate on 4-20mA signals or 0-20mA as needed.

Analogue input modules shall support active and passive loops.

Analogue input circuits shall be powered from safety supply 24V DC (safety system shall be fed from Uninterruptible Power Supplies).

Analogue input modules shall include a fault detection circuitry (out-of-range, open loop measure, short circuit, etc.).

Input cards shall have filters for EMI / RFI protection.

The FGS shall be able to receive the inputs from F&G detectors (as well as smoke, flame, heat detectors, etc.), packages and field as required where the package does not have autonomous FGS systems.

All SIS push buttons shall include line-monitoring facilities. Suitable end-of-line (EOL) devices shall be provided (by F&G device vendor) for all line monitored I/O circuits.

Instrumentation on BLPH shall be 4-20mA Smart HART Revision 7.

HART Revision 7 device diagnostic information shall be presented and be available on EWS.

All transmitters shall be NAMUR NE43 compliant for defining and differentiating when the process variable is within normal range, out of range but fault-free or when fault detection has occurred.

9.3.3.2 Digital Inputs

These inputs shall monitor field input contacts from switches, pushbuttons, etc. Input sensors shall generally provide free of voltage contacts and shall be powered by the system 24V DC.

Digital input modules shall be configurable and shall support ON / OFF sensor (solid state or contact) and voltage monitoring. Digital modules shall be configurable and shall include circuitry to ensure that any "chatter" or "bounce" encountered during contact closures does not initiate an erroneous alarm.

Switches shall be normally closed (open on trip condition) for shutdown systems, but if executive digital inputs are normally open (de-energised), they shall have line-monitoring feature. For FGS, switches shall be normally open (close on trip condition).

9.3.3.3 Digital Inputs Supervised (DIS)

For instruments associated to digital signals with End of Line monitoring, the digital signal shall be connected to Analog cards.

This standard function shall be applied to safety digital input loops based on "energize to trip" principle (e.g. local Manual Call Points, F&G matrix and SIS matrix push buttons, local SIS push buttons).

Any discrete contacts shall be line monitored to avoid single point of failure.

9.3.3.4 Digital Outputs

Each output shall be configurable (software configuration) one per one to allow the following actions:

- Maintained, latching, pulse contact.
- Normal Open / Normal Closed (fail-safe configurable position for each channel is required)
- Pulsed output (the pulse duration shall be adjustable).

The digital outputs shall be based on solid-state or relay switching. Each channel shall be individually isolated and individually protected by fuse. Output modules shall be able to drive loads powered by an external supply or by modules internal source.

Three different types of digital output shall be required:

- 24V DC powered outputs powered by the safety system,
- Volt-free output rate 24V DC powered by other systems,
- Supervised 24V DC powered outputs powered by the safety system.

The 24VDC powered output modules shall provide power to the field devices. These outputs shall generally be used for normally energized, de-energized to trip, executive action devices, typically solenoid valves, interposing relays, etc. with coil voltage of 24V DC.

The supervised 24V DC powered outputs shall be generally used for normally de-energized, energize to trip, executive action devices, typically fire extinguishing systems. The output channels shall monitor the loops or circuits up to field devices. All powered outputs shall be individually fused. Other outputs shall generally provide volt free contact outputs to other systems (e.g.: PLC package types, trip motors, electrical isolation, etc.).

9.3.3.5 Communication Cards

The safety system shall interface with the PAS networks.

Redundant communication shall be supplied between the Safety System and CCS.

The communication cards shall have integrated LED's showing card and communication port status.

Open communication by a various kind of standard protocols based on Profinet (alternately MODBUS TCP).

Safety system will be dedicated to their main task and will continue to operate in the event of an inter-systems communications failure.

9.4 SAFETY SYSTEM NETWORKS (SIS AND FGS)

The Safety System Networks shall be industrial type Ethernet IEEE network (10/100Mbps).

Loss of the Safety System Network communications to node shall ensure that the node shall continue to operate normally whilst a diagnostic alarm shall be generated in the PAS OWS.

Failure of any of system connected to the Safety System Network via hub, gateway shall automatically isolate the connection to the faulty system so as not to impair communication of other healthy systems.

The Safety System Networks together with any required accessories (switches, etc.) shall be supplied by MAC VENDOR.

The Safety System Networks shall provide error-free transmissions. VENDOR shall supply details of any error checking or correction methods used. All communication faults shall be reported to PAS. Resetting of communications link shall be automatic and achievable without disruption of normal system operation.

Time synchronization between all PAS equipment shall be configured to allow events and incidents analysis. It shall be possible for any subscriber device to be added to, or removed from, the PAS communication networks without having to shut down the network and without impairing the safety and security of the system.

9.4.1 Safety Networks

This network shall provide connections between all safety nodes belonging to the safety systems for information exchange, and if necessary executive actions.

This network shall be physically independent and not directly connected to any other network. It shall be fully redundant.

Dedicated communication cards shall be used for the safety network which shall not be shared with any other communication networks.

Executive actions may be transmitted by this safety network between safety controllers belonging to the same safety subsystem.

9.4.2 Network Components

All network components (hubs, switches, routers, etc.) shall be of industrial type: either rack or DIN mounted with redundant power supplies.

They shall not downgrade the whole reliability.

They shall be validated and fully supported by VENDOR.

9.5 TIME SYNCHRONISATION

Time synchronization shall be configured to allow events and incident analysis.

The safety system shall be capable of receiving the synchronization signal from the PAS without disrupting the execution of the application program. The PAS shall be the clock master for time synchronization.

9.6 SOFTWARE REQUIREMENTS

VENDOR shall provide a complete documentation of the application software used and a hard support (CD ROM type, DVDs, external hard disk drives, etc.) of the program used in the safety systems (Last Version "After FAT").

VENDOR shall provide to COMPANY/CONTRACTOR all the software licenses including full "ghost" version of the operating and application software, upon completion of FAT and after SAT. Final version of all software shall be handed over to COMPANY after system commissioning by the VENDOR.

The software development tools to be provided shall include the following as a minimum:

- Hardware configuration editor
- Communication configuration editor
- Logic configuration and compiler
- Automatic conversion of cause and effect matrix to functional logic diagrams
- Diagnostic of system faults
- Event logger
- Off-line simulation
- On-line documentation.

Setting of trip alarm levels for analogue inputs, setting of timers shall be done by software configuration via the Safety System EWS.

The configuration and application development environment shall be as per IEC 61131 standards. Mnemonic and high level language type programming shall not be used.

All application program source code shall be supplied with the system.

The software package shall be version control and version compactor capable of comparing two application software versions and to indicate where the variations have taken place and the means of navigation to them directly by point and click.

9.6.1 Engineering Work Station (EWS)

The safety system shall be supplied with Engineering Workstation (EWS) common for SS and CCS, Engineering Workstation (EWS) in Onshore shall be Virtual Machine (VM) and Offshore shall be physical machine mounted in cabinet. The EWS shall be provided to allow uploading and downloading memory, system maintenance operations, program development, etc. They shall be able to support both on-line and off-line programming. The EWS software shall have on-line help facility.

EWS shall be based on WINDOWS operating system, latest available version.

EWS shall enable the following functions to be performed:

- Configure and commission the shutdown systems and FGS logic
- Download a modified configuration into the shutdown systems and FGS
- Perform diagnostic testing of the shutdown systems and FGS
- Download / upload diagnostic data from the shutdown systems and FGS
- On-line documentation (self-documentation) of the shutdown systems and FGS
- Off-line simulation of logic
- EWS operating levels (loading, programming, modification, monitoring, etc.) shall be controlled by security password.

The Maintenance part of this Workstation shall provide functions to carry out normal instrument maintenance activities such as loop verifications, inhibits, system diagnostic status.

The maintenance inhibition will be done via the EWS. This EWS shall perform maintenance activities other than system engineering/maintenance such as SS loop inhibits, loop verifications, system diagnostic.

EWS shall include but not limited to the following:

- Visual Display Unit (VDU),
- Keyboard,
- Touch pad.

The VDU monitors shall be high-resolution color graphic screen capable of displaying mixed alphanumeric/ graphic information.

The minimum requirements for the VDU shall be:

- Diagonal size 22" as a minimum, Flat screen
- Full HD 1920 x 1080 pixels, Pixel Pitch less than 0.2
- Colour gamut 86 %, from VENDOR's standard palette,
- Height adjustable stand, tilt, swivel, pivot and built-in cable management,
- Response time 8 ms as a minimum.

For commissioning purposes, it shall be possible to force I/O signals into a particular logic status via the EWS. EWS shall be permanently connected to the safety system.

9.7 SYSTEM PERFORMANCES

The response time of the safety system from input change (trip request via discrete signal change, or analogue signal exceeding software configured trip set point) to output response (trip action) shall be very fast in any operational mode. The SIS shall respond to alarm inputs and give automatic actions and alarm outputs within typical response times laid down in the SRS.

The system performance requirements shall be in accordance with the project document "SIS Safety Requirement Specification (SRS)", referenced 123A90-DDL-IN-SP-40006.

9.8 SYSTEM TESTING AND FAULT DIAGNOSTICS

The safety system shall incorporate extensive self-diagnostics, fault monitoring and fault diagnostics via continuous and periodic testing procedures automatically and upon operator initiation. The self-diagnostics shall be such that all transient and permanent faults are identified, alarmed and reported. In the event of failure, the system shall automatically alert operator at the PAS OWS, and at the location of the malfunctioning service. Self-testing shall be performed to ensure that the modules are capable of performing correctly prior to being put into operation and to monitor the performance during operation. Tests shall be performed on all modules whether primary or backup. The system shall be capable of monitoring all main processors, power supply modules, I/O modules and the communication highways. The following tests shall be regarded as the minimum requirement:

- I/O Module fault monitoring.
- I/O circuit operation verification, line monitoring.
- Logic system self-tests.
- Power supply distribution monitoring.
- Data storage availability and integrity tests.
- Communication interface checks.

All detected faults shall be shown on the diagnostic interface (Safety System EWS).

The system configuration and design shall be modular in construction utilizing plug-in modules. The removal of one such module shall not affect the overall system operation or associated circuits i.e. redundancy shall not be on the same card. Module replacement will be possible with the associated chassis powered up and system operational. System diagnostics shall alarm a failure in the minimum of time and switch to the redundant unit automatically.

Communication diagnostics should include tabulations showing communications statistics and type of failures, updated in real time i.e. (framing errors, parity, timeout etc.). System diagnostics shall have an error reporting and indicating structure that make use of Safety System EWS diagnostic displays and LED status indicators to indicate status of hardware. System diagnostics shall prevent communication errors from upsetting the process. Testing and fault monitoring shall not in any way affect the normal operations of the systems. A malfunction in the testing and monitoring facilities shall not degrade the operation of the system.

9.9 INTERFACE WITH THIRD PARTY SYSTEMS

9.9.1 Interface with the PAS network

The inter-system communications between Safety System and PAS shall be the responsibility of the VENDOR. Safety system shall be supplied as an integrated system.

9.9.2 Interface with LV switchboard

Remote shutdown commands from the safety system to LV switchboard shall be hardwired via the safety system marshalling cabinets.

9.9.3 Interface with Packages

Refer to the Project document "Instrumentation for Package Unit Specification" referenced 123A90-DDL-IN-SP-40094.

Hardwired signals to trip package equipment shall be from the safety system.

Hardwired Digital Output from Safety System to UCP shall be through relays SIL 2 minimum certified, installed inside UCP, powered 24 Vdc by Safety system.

Hardwired Digital input from UCP to Safety System shall be through relays SIL 2 minimum certified, installed inside UCP, powered 24 Vdc by UCP (free voltage contact to safety system).

Where the Package does not have their own autonomous Fire and Gas system, all fire and gas detectors on the package equipment shall be hardwired back to the safety system (FGS). The safety system shall monitor all the fire and gas actions of the packages with autonomous control and safety cabinets and manage all fire and gas actions of all other packages.

9.10 SYSTEM AND MARSHALLING CABINETS

The system and marshalling cabinets shall be in accordance with the Project document "Automation Detailed Design and Construction Package" referenced 123A90-DDL-IN-DD-40029. VENDOR shall estimate the required size and number of Safety System cabinets based on the I/O Summary (which will include 10% spare).

System cabinets shall likely be limited to Power supply units, controllers, I/O cards and communication links. Marshalling cabinets shall be provided to house the Field Termination Assembly (FTA) mirror of the I/O cards, the IS barriers (if necessary), the Field Terminal Blocks (FTB) mirror of the field cables (mirror of the junction boxes) and power supply distribution terminal strips and Relays (if necessary).

Allocated cabinet configuration:

- ESD System and Marshaling cabinet #1at ITER
- F&G System & Marshaling cabinet #1 at ITER
- F&G Marshalling cabinet #2 at ITER
- Critical Action Panel (CAP) at CCR shall be software based.

All equipment and accessories inside cabinets (such as terminal strips, power supplies, etc) shall be from an approved vendor.

Fusible terminal strips shall be used for AI, AO, DO, signals. 24VDC distribution terminal strips shall be used. It will be forbidden to take the power supply directly from distribution bars. In all cases, the power supply to distribution terminal strips or equipment shall be able to be isolated. Dedicated 24VDC terminal strips shall be available for Field Instruments. In case, where different model are proposed, VENDOR shall submit technical proposal for COMPANY's approval.

All negative points of the signals shall be of the type "Disconnect feed-through" terminal blocks type. In all cases, fusible terminal strips shall be used for power supply terminal blocks.

9.11 CABLES AND WIRING

All interconnection cables shall be supplied by MAC VENDOR, including pre-wired and pre-tested system cables with multi-way connectors between the System Cabinets and the Marshalling Cabinets, all communication links, the associated connectors and installation kits.

The exact length of the cables shall be decided based on the location of System Cabinets and Marshalling Cabinets. Wiring details shall be in accordance with the Project document "Instrument - Safety System Wiring Diagrams" referenced 123A90-DDL-IN-DG-40016.

9.11.1 Cable Colours Coding

Instrument cable shall be constructed in accordance with EN 50288-7:

- Pairs:
  - (+) Black (BLK)
  - (-) White (WHT)
- Triads:
  - (+) Black (BLK)
  - (Signal) Red (RD)
  - (0V) White (WHT)
- Power supply
  - 24V DC
    - (+) Red (RD)
    - (-) Blue (BL)
- Earthing system cables shall be colored as follows:
- Protective Earth (PE) = Green (RAL 6018) and Yellow (RAL 1021)
- Instrument Earth (IE) = Green (RAL 6018)
- Intrinsically Safe Earth (ISE) = White (RAL 9010)

All Cross wiring points inside cabinets shall be clearly identified. Identification shall be such that in each terminal point it shall be printed the opposite side to which is connected the cable.

9.12 LABELLING AND NUMBERING SYSTEM

Identification of all equipment provided by the VENDOR (chassis, cables, terminal blocks, I/O modules, cabinets, etc.) shall be marked with its own label. Each wire must be marked at both ends by tagging sleeves or tapes.

9.13 EARTHING

Instrument signals shall have segregated earthing for protective, reference and intrinsically safe.

Earthing in hazardous areas shall adhere to IEC 60079-14.

VENDOR to provide separate Protective Earth (PE), Instrument Earth (IE) and Intrinsically Safe Earth (ISE).

9.14 ELECTRICAL SUPPLY

The following electrical supplies will be provided:

- 230V AC/50Hz from UPS (2Ph - IT System) for the marshalling and system cabinets.
- 230V AC/50Hz from UPS (2Ph - IT system) for OWS and EWS.

Each cabinet shall include redundant power supply modules converting 230V AC UPS to 24VDC for its associated field devices and internal components. The power supply modules shall be capable to receive 230VAC.

9.15 SPARE CAPACITY

The Safety system design shall include spare capacity (in term of hardware and system) to allow for maintenance, repair and extensions of all electronic systems to be performed with minimal disturbance to the process and utilities, fixed cabling infrastructure and general facilities infrastructure.

The Safety System shall be designed so that this spare capacity is available at plant start-up. In particular, after commissioning activities, at least 10% spare I/Os shall be available for future extension.

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

10 DOCUMENTATION

10.1 GENERAL

The VENDOR shall deliver sets of documentation with the system in accordance with Product document "MR- Automation systems CCS-SIS" referenced 123A90-DDL-IN-MR-40103..

All project documents shall be in the English language.

The scope of documentation, the layout of drawings and list should be agreed by CONTRACTOR.

Drawings and printing will be clear and legible. Documentation shall be hard backed and shall be of A4 size, together with all drawings permanently fixed in the drawing size not exceeding A3 size.

All documents and drawings shall be well documented and shall be provided with legend sheet showing symbols used.

All documentation shall be approved before the beginning of the construction/implementation of the application.

If VENDOR starts without proper approval, it will be under its own responsibility and any modification required by COMPANY/CONTRACTOR will have to be implemented.

Final documentation / Operating & Maintenance Manuals shall be in English language.

10.2 DOCUMENTATION REQUIREMENTS

All references to any instruments on any documents shall be by the tag number.

10.3 DOCUMENTATION TO BE PROVIDED WITH THE SYSTEM

The following documentation shall be provided as minimum:

- Equipment Nameplate List
- Packing List
- Safety Function Design Specifications
- Safety System Test specification/FAT Procedure
- Datasheets
- Packing, marking and Shipping Procedure
- Transportation, Storage, Preservation Procedure
- Monthly Report
- Planning
- Safety system typical functional tests report
- FAT Report
- Integrated FAT Report
- Safety System Architecture Block Diagram

- Cabinet Equipment Specification
- Power and heat load calculation
- Bill of Material
- Critical Action Panel Layout
- Two (2) years Operation Spare Parts List
- Reliability and Availability Calculation Notes
- System Cabinets arrangement drawings
- System Cabinets fixing details drawings
- System Cabinets wiring diagram drawings
- Marshalling Cabinet arrangement drawings
- Marshalling Cabinet fixing and Lifting details drawings
- Marshalling Cabinet wiring diagram drawings
- I/O Channel Assignment and Database
- Cable List
- Power Supply and Earthing wiring diagram
- Safety system typical functional test
- Safety system detailed test procedure c/w tests planning and test set up
- Safety system installation procedure
- Safety system software list
- Safety system graphics (Process mimic screens and Safety shutdown matrix mimic screens)
- Operation and Maintenance Manual
- Equipment and System Certificates. (including SIL Certificates and SIL Loop calculation where applicable)
- Software license list.
- Any other documents that may be requested by COMPANY.

10.4 DOCUMENTS PRESENTATION

The form of the documents used by VENDOR shall be the same that those used by CONTRACTOR and agreed for the Project by COMPANY.

11 INSPECTION AND TESTING

11.1 GENERAL REQUIREMENTS

VENDOR shall be responsible for the integration, inspection and testing of the Safety System. VENDOR shall assume final responsibility for the inspection and testing of the safety system to ensure that the systems are conform to the requirements of the codes and standards specified in this document and in accordance with Project document "MR – Automation systems CCS-SIS" referenced 123A90-DDL-IN-MR-40103..

The COMPANY shall reserve the right to perform inspection of the equipment / material at any stage during manufacture and at any time. COMPANY shall be notified ten (10) working days prior to any testing. Material certifications and record dispatching shall be made available to the COMPANY during or at completion of fabrication. It is expected that assistance will be available for inspection of parts, during or after completion of fabrication, during a shop inspection.

VENDOR shall submit full testing procedure for factory testing, site testing and acceptance procedure for COMPANY's approval. For hardware, the procedures shall include purpose of test, test definition of input, procedure, result expected and acceptance criteria. For software, it shall include details of the method, list of tests, sequence of execution, result expected and acceptance criteria.

11.2 GENERAL

The VENDOR system shall be fully tested to ensure satisfactory system performance meeting all the requirements as outline in this specification and in accordance with MR - Automation systems CCS-SIS 123A90-DDL-IN-MR-40103.

The tests shall comprise of the following:

- Design Validation Tests
- Logic typical tests
- Hardware typical tests
- Serial link typical tests
- System typical tests
- Functional Blocks Test; (prior to application software development)
- Factory Acceptance Tests
- Mechanical inspection
- Hardware tests
- Loop functional tests
- Logic tests
- System tests
- Integrated tests
- Integrated Factory Acceptance Test (IFAT)

- Site Acceptance Test (SAT)

11.2.1 Test Documentation

Before commencement of tests witnessed by Company, VENDOR shall make available the records of his internal tests demonstrating that they have been fully carried out successfully and all documents shall have the "Approved for Construction" state APPROVED prior to the beginning to the FAT. An approved test procedure shall be provided for each test.

The FAT procedures and IFAT procedure shall include a mark-up of the overall VENDOR architecture showing the battery limits of the test. VENDOR shall present to COMPANY a test report prior to the FAT. This report shall contain the same test to be made during the FAT with COMPANY presence, demonstrating the VENDOR has test all the equipment/software prior to the final FAT.

A detailed test schedule shall be issued for FAT and IFAT, broken down into sufficient detail, e.g. by cabinet for hardware tests, by functional analysis for software tests, by standard function for configuration etc

For FAT, the plan will show the internal test planning, the number of test teams, vendor participation windows, etc. Other external impacting events, such as functional analysis AFC (Approved for Construction) issue dates may also be included.

A test progress measurement and reporting method shall be developed.

Test documentation shall be and in accordance with Project document "MR - Automation systems CCS-SIS" referenced 123A90-DDL-IN-MR-40103.

Testing shall be performed using project documents in latest AFC status approved by Company. These documents shall be printed and the master present on the test platform, including:

- FDS (Functional Design Specification)
- Standard functions specifications
- P&IDs
- Fire and Gas Cause & Effect
- Fire and Gas layout drawings
- I/O database printout
- Full set of VENDOR project documentation.

11.3 FACTORY ACCEPTANCE TESTS (FAT)

The FAT shall be a thorough and complete functional test of the hardware and software of the safety system. During the FAT, CCS and safety system shall be tested as standalone systems.

CONTRACTOR shall make arrangements to test all systems linked or communicating in any way to the PAS with their actual hardware and application at VENDOR's FAT staging facility. These arrangements shall include hardware shipping and technical assistance from the package VENDORS. The communication link mappings shall be 100% tested.

VENDOR shall demonstrate the functional integrity of the system hardware and software. No material or equipment shall be transported until all required tests are successfully completed and certified 'Ready for Shipment' by the CONTRACTOR / COMPANY.

VENDOR reserves the right to be involved at each and every stage of inspection. COMPANY shall be free to request any specific test on any equipment considered necessary although not listed in this specification.

VENDOR shall note that acceptance of any equipment or the exemption of inspection or testing shall in no way absolve VENDOR of the responsibility for delivering the equipment which meets all the requirements specified in the specification.

All equipment (including the shutdown functions) shall be tested separately and then together as a system complete with all operating controls.

All tests shall be conducted utilizing only equipment that will eventually be shipped to the CONTRACTOR / COMPANY. Use of "replacement" units during any part of the FAT is not allowed.

Any defects found during the FAT shall be rectified in the presence of the CONTRACTOR / COMPANY. In the event this is not possible, a checklist shall be prepared stating all outstanding items for approval by CONTRACTOR / COMPANY.

It shall be VENDOR responsibility to modify and/or replace any hardware and modify the software if the specified functions are not satisfactorily achieved during testing and factory acceptance.

The equipment shall not be shipped until all discovered defects have been rectified and satisfactorily re-tested.

The following test shall be included into the FAT as a minimum:

- Power Supply tests.
- Processor tests.
- I/O tests.
- Full functional and logic tests.
- All communication interfaces.
- Communication link tests between CCS and safety system.
- Data link mappings.
- Archiving and Historical functions.

- Historian servers' tests.
- Printing test.

The inspection and factory inspection shall be carried out as follows:

- VENDOR shall perform in-house testing prior to CONTRACTOR / COMPANY witnessed FAT to assure smooth testing during the FAT.
- VENDOR shall then systematically, fully and functionally test all the hardware and software in the presence of CONTRACTOR / COMPANY. All systems shall be interconnected to simulate, as close as possible, the total integrated system. VENDOR shall use a simulator suitable for all types of I/O. Individual system I/O shall be able to be tested with the simulator concurrently, with related checks being made on interactions between other parts of the system.

Apart from visual and mechanical testing, functional testing shall include the simulation of each input and output to verify proper system response for both analogue and discrete signals. All hardwired inputs and outputs shall be wired to simulator panel prior to FAT. The testing, as a minimum shall include:

- Check of all input/output points.
- Check of scan time values.
- Check of all control configurations as to input, output, modes, failure, action, etc.
- Check of loop configuration as to ranges, limits, alarm points, units etc.
- Check of all computations.
- Check of all logic and sequence control.
- Check of correct changeover of the back-up units.
- Check of keyboard/touch screen functions, key-lock functions.
- Check of log reports and historical functions.
- Check of all displays.
- Check of LCD screen refresh rates, data base update and display call-up time.
- Check of module diagnostics.
- Check of remote diagnostics.
- Power failure and redundancy checks.
- Communication failure and redundancy checks.
- Communication between CCS and safety system (including redundancy checks).
- All hardware must be inspected for physically damaged components and general workmanship standards.

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

- Particular note should be made of:
    - Wiring loops and terminations.
    - Quality of earth and power connections.
    - Ease of access for maintenance work.
    - Door seals and paint finish with reference to the final site environmental conditions.
    - Printed circuit board connections to backplanes in card cages.
    - Plug and socket connections.
    - Robustness of supports frames and circuit boards.

The system shall be subjected to tests sufficient to determine its compliance with all functional requirements specified in the Specification. The following tests shall be performed, where applicable:

Operator Interfaces:

- All specified operator commands, including data entry, cold and warm starts, changeovers, display and printout requests shall be exercised. The response to all commands shall be verified to be correct and within the specified response times.
- Particular attention should be paid to commands under restricted access by means of key locks or passwords. The specified security access level shall be verified for all commands.
- Where applicable, alarm annunciation facilities shall be exercised and operator silence and acknowledge commands shall be tested. The response time to alarm conditions shall be verified against that specified in the Specification.
- All operator and system displays shall be demanded and examined for compliance with the Specification. Where displays are accessible by various routes, all such routes shall be tested and display cross references and indices shall be checked.
- Verification that terminal and wiring coding is in accordance with the panel drawings.

Subsystem Failures:

Tests shall be carried out in order to verify that redundant systems operate as specified, i.e. changeover to back-up occurs correctly and is annunciated to the operator. Operator displays and diagnostics identifying the particular failed sub-system shall be checked as sufficient. The following redundant sub-systems are typical.

- Redundant Processors
- Redundant Power Supplies
- Degraded Operations
- System Diagnostics

After acceptance, a comprehensive test report shall be written and issued by the VENDOR. After completion of the FAT and previous to the starting of commissioning, documents shall be issued in a state "ISSUED AFTER FAT" including all mark-ups done during FAT.

11.4 INTEGRATED FACTORY ACCEPTANCE TEST (IFAT)

During IFAT, VENDOR shall perform the system performance tests with the whole Integrated Control & Safety System.

The objective of the IFATs is to test that the overall PAS architecture works as a whole including its interfaces. It shall be performed after the completion of the subsystems FAT in the sequence depending on the project requirements:

- For each individual facility (offshore or onshore) of the project, all PAS subsystems shall be interconnected together. If different PAS sections or domains have been defined, all of them shall be interconnected together.
- And then, the whole field / plant including any different locations/facilities (e.g. CPI, remote onshore central control room), all PAS shall be interconnected together through telecommunications means. The PAS arrangement during IFAT will reflect the final PAS site configuration/architecture, including all inter-site and intra-site PAS communication networks and interfaces with other networks.
- During IFAT, VENDOR shall ensure that overall PAS performance has not been adversely impacted by the extension or modifications at onshore site. Regression testing, or equivalent, shall ensure that the new modifications have not unduly compromised the existing logic.

To do these tests, the equipment configuration shall reflect the actual site equipment configuration by using the actual site PAS and Telecom equipment.

The IFAT shall be performed with all equipment and shall include as a minimum:

- Performance tests and response time with all subsystems/equipment interconnected with the full load. A detailed set of benchmark results shall be recorded including response times, memory usage, cycle time, free-time, communication time, etc. for all PAS subsystems.
- All integration aspects (e.g. communication networks, nodes hook-ups, database…)
- Safety bus loss of communications executive actions as per project requirements (unless already fully tested during the FAT with all nodes).
- All common/shared subsystems, including as a minimum: HMI including reports and print-out, IAMS, Alarm Management system, Historians and Clock synchronization.
- Test of site integration and merging procedures of networks and master software, as applicable.
- To validate all software interfaces and integration aspects of the PAS,
- To carry out full load, performance tests with response time.
- To carry out full redundancy tests and degraded operations tests.
- The Maintenance inhibit enable / disable key switches overall function.
- Verification and test of all Cybersecurity requirements not performed previously.
- Test of all back-up/restoration procedures.

During the IFAT, all documentation and licenses shall be reviewed. The documentation shall be based on the project requirements and shall be and in accordance with project document "MR - Automation systems CCS-SIS" referenced 123A90-DDL-IN-MR-40103.

At the end of the IFAT, COMPANY shall conduct a number of days of operation tests. For this purpose, the VENDOR shall make free to COMPANY all interconnected systems and provide necessary assistance.

11.5 SITE ACTIVITIES AT WORKSITE

VENDOR shall provide assistance for the Site Acceptance Test (SAT), pre-commissioning and commissioning operations, and start-up activities.

The SAT procedures shall be prepared by VENDOR and submitted to CONTRACTOR and COMPANY agreements.

The VENDOR will be expected to assist with unpacking, installing and hook up the system ready for site commissioning.

The Site Acceptance test (SAT) will consist of a series of test to demonstrate that:

- System integrity has not been affected in transport,
- Actual system interfaces are fully functional,
- Field interfaces are fully functional.
- All equipment/software has been delivered including consumables and spare parts.
- All documentation relevant to the has been delivered.
- All software is correctly installed and revision noted.
- Equipment has been correctly installed and assembled. All devices, cards, cables and connectors are securely fastened.
- Powering and earthing are fully operational.
- Communication interfaces and networks are fully functional.
- Redundancy functionality is fully operational.
- All Subsystems fault alarms are cleared or accounted for.
- Back-up systems are fully operational.

The SAT will therefore demonstrate that the System has been correctly installed, earthed, powered up and is fully operational to allow loop commissioning tests to start.

A full set of benchmarks shall be measured and recorded and compared with the IFAT results (response times, memory usage, cycle time, free-time, communication time, etc. for all subsystems). This shall be performed at yard/worksite and at site.

12 PACKING AND SHIPMENT

Shipment authorization will be given by inspection release certificate after all pending points raised during acceptance tests have been resolved.

All equipment supplied by VENDOR must be packed so as to avoid any damages as defined in packing and shipments requirements.

In particular the following considerations and action shall be taken.

- All main moving part shall be locked.
- All glasses shall be protected against shock.

In addition, all necessary precautions shall be taken for adequate protection of the safety system, including accessories, during shipment and long term outdoor storage at their destination.

Each item shall be identified by the complete purchase order number.

Packing and shipment shall be according to project document "Preservation Procedure" referenced 123A90-PML-COM-PRO-03039.

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

13 SPARE PARTS

VENDOR shall define and supply the consumables and spare parts required during the installation, testing and commissioning phases.

VENDOR shall provide in particular:

- The special tools required for correct operation and for maintenance.
- The spare parts for commissioning and start up for all equipment supplied. Spare parts for a 2 year period.

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

14 SIZING REQUIREMENTS

14.1 HARDWARE SIGNALS

The hardware signal sizing shall be taken from the Project document "Instrument I-O List" referenced 123A90-DDL-IN-LIS-40089.

14.2 SOFTWARE SIGNALS

The software signal sizing shall be taken from the Project document "Instrument I/O Serial Mapping List " referenced 123A90-DDL-IN-LIS-40090.

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