Base Load Power Hub (BLPH)

Control System (PCS) Specification

Document Number: 123A90-DDL-IN-SP-40098

Document Class: Class 1

02	30/09/2025	Accepted for Construction (AFC)	DC	LCA	CGI
01	24/07/2025	Accepted for Construction (AFC)	DC	LCA	CGI
00	22/01/2024	Issue for Acceptance (IFA)	SEKV	AMBE/LOCA	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
00	Issue for Acceptance (IFA)
01	Accepted for Construction (AFC)
02	Accepted for Construction (AFC)

HOLDS LIST

No.	Description
1	
2	
3	
4	

Table of contents

1 INTRODUCTION7

1.1 PROJECT OVERVIEW7

1.1.1 Project Location7

1.1.2 Project Concept8

2 DOCUMENT SCOPE9

2.1 REFERENCES11

2.1.1 International Standards13

2.1.2 Company Standards14

2.2 DEFINITIONS AND ABBREVIATIONS15

3 CONFIDENTIALITY18

4 RESPONSIBILITIES18

5 GENERAL REQUIREMENTS19

5.1 Environmental Conditions19

5.2 Hazardous Area Certification19

5.3 Radio frequency interference19

5.4 Electromagnetic Interference19

6 CYBER SECURITY19

6.1 Cyber Security Requirements20

6.1.1 Patch Management20

6.1.2 Antivirus21

7 OBSOLESCENCE MANAGEMENT AND LIFE CYCLE23

7.1 Instrument Asset Management System23

8 SCOPE OF WORK24

8.1 General24

8.2 Equipment24

8.3 Services25

9 TECHNICAL REQUIREMENTS27

9.1 General27

9.1.1 Basic Design27
9.1.2 Operator interface27
9.1.3 Operator facilities27
9.1.4 Maintainability28
9.1.5 System reliability and availability28
9.1.6 Redundancy28
9.1.7 Modular and flexible29
9.1.8 Electro-Magnetic Interference (EMI)29
9.2 System Architecture29
9.3 System Hardware General Requirements29
9.3.1 PCS requirements29
9.3.2 Power Supply Module31
9.3.3 Input/Output Requirements31
9.3.4 Time Synchronisation35
9.4 Software Requirements36
9.5 Operator Interface36
9.5.1 Operator WorkStation (OWS)36
9.5.2 PrinterErrore. Il segnalibro non è definito.
9.6 Historian Server39
9.7 Alarm Management System39
9.8 System Performances40
9.9 PAS Networks40
9.9.1 HMI Network41
9.9.2 Service Network41
9.9.3 Safety Control Network41
9.9.4 Control Network41
9.9.5 Technical Network42
9.9.6 Profinet/IEC61850 Network42
9.10 Interface with Third Party Systems42
9.10.1 Interface with LV switchboards42
9.10.2 Interface with Packages42
9.11 System and Marshalling Cabinets43
9.12 Network Cabinet43
9.13 Cables and Wiring44
9.13.1 Cable Colours Coding44

9.14 Labelling and Numbering System45
9.15 Earthing45
9.16 Electrical Supply45
9.17 Spare Capacity45
10 DOCUMENTATION46
10.1 General46
10.2 Software Requirements46
10.3 Documents Presentation46
11 INSPECTION, TESTING AND ACCEPTANCE REQUIREMENTS47
11.1 General Requirements47
11.2 Test Documentation47
11.3 Factory Acceptance Tests (FAT)48
11.4 Integrated Factory Acceptance Test (IFAT)49
11.5 Site Activities at Worksite51
12 PACKING AND SHIPMENT52
13 SPARE PARTS53
14 SIZING REQUIREMENTS54
14.1 Hardware Signals54
14.2 Software Signals54
15 ANNEXES55
55

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

List of Figures

Figure 1 HOLLANDSE KUST NOORD WIND PARK Location Map7

Figure 2 - Wind Park Details8

Figure 3 – BLPH Concept8

List of tables

Table 1 - Reference Documents13

Table 2 - International Standards14

Table 3 - Company DEPs14

Table 4 - Company DEM-115

Table 5 - Definitions and Abbreviations18

List of Attachments

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.

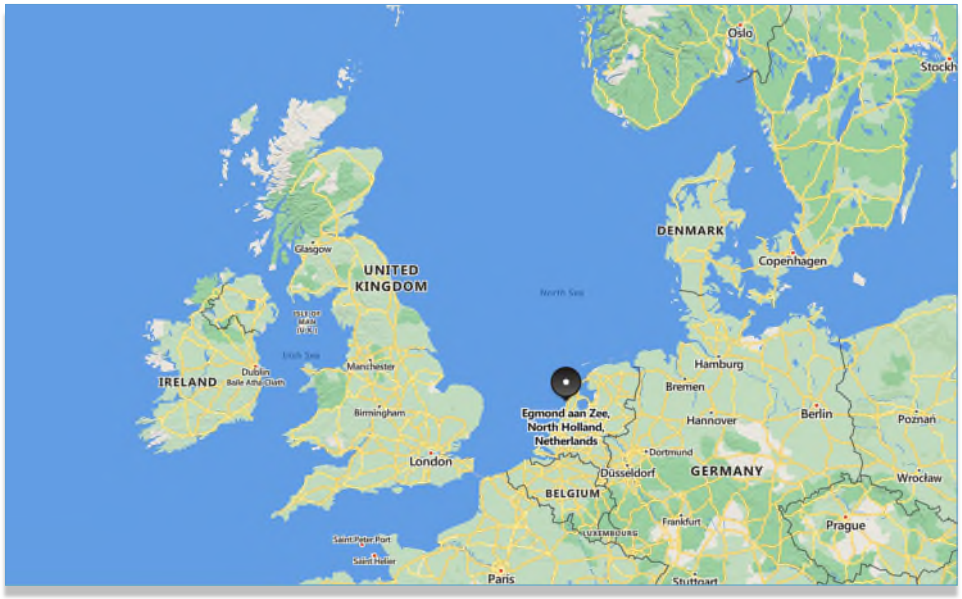


Figure 1 HOLLANDSE KUST NOORD WIND PARK Location Map

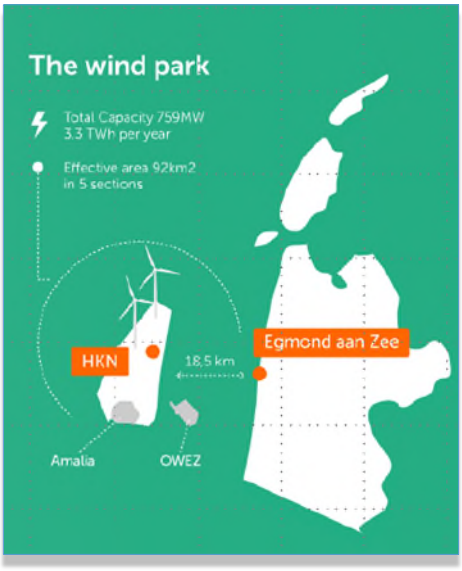


Figure 2 - Wind Park Details

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.

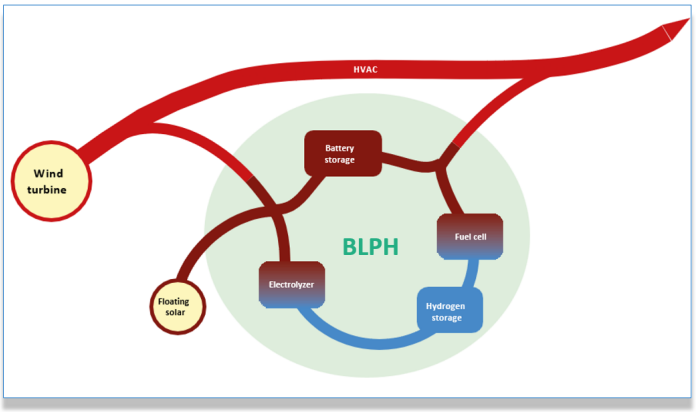


Figure 3 – BLPH Concept

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 DOCUMENT SCOPE

This specification defines the minimum requirements for engineering, manufacturing and delivery, but not limited to the design, material procurement, fabrication, documentation, inspection and testing of the Process Control System used on Crosswind BLHP Project and its interface with the existing onshore facilities.

The Process Control System (PCS) will ensure a safe and efficient control and monitoring of the process platform and utilities. The Process Control System shall monitor and control non safety actions of the facilities and fulfil the requirements of the operating philosophies.

It shall also provide the "backbone" of the PCS communication network and thus allow the Operator to view and manage the entire facility from the HMI located in the control room.

It shall manage all external interfaces with third party packages and other external systems related to control and monitoring functions (e.g. the Safety System, Electrical Management System, Electrolyser, BESS, HVAC,…).

The Process Control System shall be microprocessor-based system, utilizing proven industry standard hardware and software connectivity.

The main functions of the Process Control System are to perform all process control, alarms reporting, data capture and monitoring functions necessary for the proper operation of the BLPH Plant. The Process Control System performs the process control, alarm functions, sequencing and also performs logics, permissive to start or stop components.

The Process Control System is mainly composed of:

- Marshalling and system cabinets located into the Instrument Technical Equipment Room (base case design: Two (2) System cabinets, One (1) Network Cabinet and One (1) Marshalling cabinet)
- Engineering workstation (EWS) cabinet mounted, located into the ITER (The EWS shall allow access to the PCS system for Engineering and Monitoring purposes.
- Engineering workstation located into the Onshore Equipment room(OER),
- The EWS/OWS shall have dedicated connection to Maintenance and Communication networks with a firewall segregating it from PCS and SIS Networks.
- Historian Server (Accessible from OWS),

- Sequence of Events (SOE) (Accessible from OWS),
- Alarm Management System.

The system shall include controller nodes with associated I/O cards and communication cards.

Depending on the size of the system, multiple nodes connected to the PCS network may be required.

There is no SIL requirement for PCS.

The Process Control System shall be based on Programmable Logic Controller.

The Process Control System is part of the PAS (but independent from the Safety Systems). For more details, refer to the Project documents "Safety System (SIS and FGS) Specification" Ref. 123A90-DDL-IN-SP-40100 and "Control System Architecture Detailed Drawings ", Ref. 123A90-DDL-IN-DD-40096.

All materials and equipment furnished shall meet the design and environmental conditions and shall be new, sound and free of defects and of the quality as specified herein.

The Process Control System shall be supplied as completely pre-wired and tested systems. PAS VENDOR shall note that all accessories should be supplied as a completely assembled unit to meet the operation requirements.

The Process Control system and the Safety systems (SIS, F&G) shall be under the responsibility of one and only one responsible Supplier who will be in charge of developing all required software applications and to supply all required hardware for both systems (cabinets, controllers, marshaling, etc.).

This supplier shall be on the Approved Vendor list of the COMPANY, with previous experience working with the COMPANY.

MAC 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 MAC VENDOR's standard hardware and software, avoiding any special or customized design for this particular installation. In case where special design cannot be avoided, the description shall positively state so in MAC VENDOR's proposal, otherwise it is taken that MAC VENDOR's standard design is provided.

The Process Control System shall consist of equipment having been offshore field proven for at least two years with client references.

PAS VENDOR shall have at least three years proven previous experience in supplying Process Control System of similar configuration and functionality.

Any deviation from this specification at any stage of the project will require to be approved by COMPANY.

2.1 REFERENCES

2.1.1 REFERENCE DOCUMENTS

123A90-DDL-IN-SP-40024	ALARM SYSTEM REQUIREMENT SPECIFICATION
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-40094	INTRUMENTATION FOR PACKAGE UNIT SPECIFICATION
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

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

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
123A90-DDL-IN-DL-40013	Earthing Layout drawings (Offshore ITER)
123A90-DDL-IN-SP-40018	Cyber Security
123A90-DDL-EL-SP-20039	#VOID# Functional and Technical Design Specification, IDS and DDS for Electrical Monitoring and Control System (EMCS)
123A90-DDL-IN-DG-40016	BASE LOAD POWER HUB (BLPH) Instrument - Safety system wiring diagram
123A90-DDL-IN-LIS-40089	Project document "Instrument I-O List"

Table 1 - Reference Documents

2.1.2 INTERNATIONAL STANDARDS

EEMUA PUB No 191	Engineering Equipment and Material User's Association Alarm Systems A Guide to Design, Management and Procurement.
IEC 61000	Electromagnetic compatibility (EMC) - 61000 Series.
IEC 61508	Functional safety of electrical/electronic/programmable Electronic safety related systems.
IEC 61511	Functional safety - Safety instrumented systems for the process industry sector
IEC 62443-2-3	Security for industrial automation and control systems. Patch management in the IACS environment.
IEC 62443-2-4	Cyber Securities Capabilities.
IEC 60529	Degrees of protection provided by enclosures (IP Code).
IEC 61131-3	Programmable controllers – Part 3: Programming languages.
IECEx	IEC System for Certification to Standards relating to Equipment for use in Explosive Atmospheres (IECEx System).

Directive 2014/34/EU	Directive 2014/34/EU of European Parliament and Council of 26 February 2014 on the harmonization of the laws of the Member States relating equipment and protective systems intended for use in potentially explosive atmospheres.
ISA 18.2	Management of Alarm Systems for the Process Industries.
RFC 5905 (part 1 of 5)	Network Time Protocol Version 4: Protocol and Algorithms Specification.
ANSI/TIA 232 F	Interface between data terminal equipment and data circuit-terminating equipment employing serial binary data interchange.
API RP 14 C	Recommended practice for analysis, design, installation and testing of basic surface safety systems on offshore production platforms.
API RP 554	Process Control Systems Part 1–Process Control Systems Functions and Functional Specification Development.
API RP 557	Guide to Advanced Control Systems.
DIN V 19250	Control technology; fundamental safety aspects to be considered for measurement and control equipment.
EN50081-2	Electromagnetic Emission for Industrial Electronic Equipment.
EN50082-2	Electromagnetic Immunity for Industrial Electronic Equipment.
RS-485	Electrical characteristics of drivers and receivers for use in balanced digital multipoint systems.

Table 2 - International Standards

2.1.3 COMPANY STANDARDS

2.1.3.1 Design Engineering Practices

Document Name	Document Title
DEP 33.64.10.32	Electrical network monitoring and control system for global application
DEP 32.01.20.12	Industrial Automation and Control Systems (IACS) Security
DEP 30.00.60.15	Humans Factors Engineering – Control Room Design
32012012_Spec_2021-02_A00	Crosswind Systems Security Requirements

Table 3 - Company DEPs

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

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

2.1.3.2 DEM-1 Process Safety Only DEP

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 4 - Company DEM-1

2.2 DEFINITIONS AND ABBREVIATIONS

DOCUMENT NAME	Document Title
ALARP	As Low as Reasonably Possible
AMS	Alarm Management System
ATEX	Appareils destinés à être utilisés en ATmosphères EXplosibles (Equipment intended for use in explosive atmospheres)
BESS	Battery Energy Storage System
BLPH	Base Load Power Hub
CAP	Critical Action Panel
CAPEX	Capital Expenditure
CAT	Category
CCN	Central Control Network
CCR	Central Control Room
CCS	Central Control System
CCTV	Closed Circuit Television
COMPANY	Crosswind
CONTRACTOR (CTR)	ROSETTI MARINO S.p.A.
CTV	Crew Transfer Vessel
DEM	Design Engineering Manual
DEP	Design and Engineering Practice
DMZ	Demilitarised-Zone
EMC	Electromagnetic Compatibility
EN	Engineering Notice
EPC	Engineering Procurement Construction

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

EPIRB	Emergency Position Indicating Radio Beacon
EWS	Engineering Workstation
Ex	Explosion Proof
FC	Fuel Cell
FEED	Front End Engineering Design
FEED CONTRACTOR	Organisation contracted directly by COMPANY to provide engineering, design, or other services.
FGS	Fire & Gas System
FO	Fibre Optic
FOPP	Fibre Optic Patch Panel
FTP	File Transfer Protocol
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positional Satellite
HART	Highway Addressable Remote Transducer
HAZOP	Hazardous Operability Study
HKN	Hollandse Kust Noord
HMI	Human Machine Interface
HV	High Voltage
HVAC	Heating, Ventilation and Air Conditioning
HV-SCADA	The given name for the COMPANY's control system for the HKN wind farm infrastructure. BLPH's control system shall operate autonomously but will interface with HV-SCADA.
IACS	Industrial Automation and Control Systems
IAMS	Instrument Asset Management System
IDCS	Intrusion Detection Control System
IEC	International Electrotechnical Commission
I/O	Input Output
IP	Ingress Protection
IP	Internet Protocol
IS	Intrinsically Safe
ISO	International Organization for Standardization
ITER	Instrument & Telecoms Equipment Room

LACS	Local Access Control System
LAN	Local Area Network
LED	Light Emission Diode
LOPA	Layers of Protection Analysis
LHVS	Land High Voltage Station
LV	Low Voltage
MAC	Main Automation Contractor,
MCC	Motor Control Centre
NAMUR	Interessengemeinschaft Automatisierungstechnik der Prozessindustrie (User Association of Automation Technology in Process Industries)
NIS	Non-Intrinsically Safe
OHVS	Offshore High Voltage Station
OWS	Operator Workstation
PAGA	Public Address and General Alarm
P&ID	Piping and Instrument Diagram
PACO	Process, Automation, Control and Optimisation (PACO) is the term used to describe all functionality required for the monitoring and controlling of all process, safety and fire and gas systems selected for the project.
PROJECT	HOLLANDSE KUST NOORD WIND PARK Project
PV	Photo Voltaic
PURCHASER	The organisation placing a purchase order for the supply of equipment or services for the Project. The Purchaser could be the COMPANY or the Contractor or some other party appointed by the COMPANY or Contractor.
RVO	Rijksdienst voor ondernemend Nederland – The Netherlands Enterprise Agency
SART	Search and Rescue Transponder
SCADA	Supervisory Control and Data Acquisition
SGSI	Shell Global Solutions International
SHALL	An absolute requirement.
SHOULD	This word indicates a recommendation that whilst preferred may not be implemented provided some equivalent is proposed and

	agreed by COMPANY. The full implications must be understood and carefully weighed before choosing a different course.
SIF	Safety Instrumented Function
SII	Industrial Information System
SIL	Safety Instrumented Level
SIS	Safety Instrumented System
SOLAS	Safety of Life at Sea
TCP/IP	Ethernet Protocol
TETRA	Terrestrial Trunked Radio
TSO	Transmission System Operator
TQ	Technical Query
UCP	Unit Control Panel
UHF	Ultra-High Frequency
UPS	Uninterruptible Power Supply
VENDOR	Manufacturer/Supplier of equipment and services to perform the duties specified by the Purchaser.
VDU	Video Display Unit
VHF	Very High Frequency
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WTG	Wind Turbine Generator

Table 5 - Definitions and Abbreviations

3 CONFIDENTIALITY

This document and its contents shall remain strictly confidential and shall not be distributed to others than the Project Client without ABB AS prior written consent thereto. This document is, unless otherwise agreed in writing, the property of ABB AS, and shall not be reproduced, copied, or used for any other purpose than for which it is supplied or disclosed.

4 RESPONSIBILITIES

It will be the CONTRACTOR responsibility to raise to COMPANY any discrepancy between documents. The CONTRACTOR shall not proceed with any such aspect of the work until he has received any necessary confirmation, in writing from the COMPANY.

5 GENERAL REQUIREMENTS

5.1 Environmental Conditions

The Process Control 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 Process System equipment located in onshore OER/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", (HOLD-1)

5.2 Hazardous Area Certification

The onshore OER/CCR and offshore ITER room is a non-hazardous area.

5.3 Radio frequency interference

Standard industrial VHF and UHF hand-held personal radio equipment of 5W nominal output power will be operated as close as 0.5m from the equipment. This should not influence the system.

All supplied equipment shall comply with IEC 61000 standard.

PAS VENDOR shall state whether its standard system design and construction includes the necessary features to render the installed equipment immune to interference from such radios in operation with all equipment doors opened.

PAS VENDOR shall state the RFI susceptibility (with doors opened and closed) of all supplied equipment.

5.4 Electromagnetic Interference

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.

6 CYBER SECURITY

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

A cyber security risk assessment of the IACS, 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.

6.1 Cyber Security Requirements

As a minimum, when the supervisory and/or the engineering workstation (EWS) are based on a computer, PC type using standard computer operating systems (Windows, etc.) and standard network protocol (TCP/IP), the following rules shall apply:

Engineer/Maintenance modes shall not be accessible to operators. Limitation by key, badges, passwords or any combination is mandatory.

Access to the operating system commands shall be restricted to Engineer mode only.

External mass storage devices (CD-ROM, floppy, USB memory, etc) shall not be accessible in normal operation (shall be removed from the set-up).

When remote access for maintenance is necessary, a formal request shall be made to COMPANY Remote maintenance through a stand-alone modem shall not be permitted. Specific procedures shall be set up with COMPANY.

The connection shall be made through the COMPANY local network using secured procedures with strong authentication (e.g. secure ID).

In any case a preliminary evaluation of possible impact on the package's operation resulting of errors or failure of this remote operation shall be made.

All software original licenses, software disks (including operating system) and tools shall be provided with a detailed procedure including all system parameters for a full re-installation from scratch.

PAS VENDOR shall provide a full ghost copy of hard disk to allow for simple restart if new computer is used.

Before start-up PAS VENDOR shall verify and ensure that the UCP including all associated computers and associated configuration and maintenance tools are virus free.

PAS VENDOR shall verify and ensure any electronic documentation supplied is virus free.

The PAS VENDOR shall prepare and submit for approval a package Cyber Security specification outlining the risks associated with the system and the techniques and equipment employed to mitigate such risks.

6.1.1 PATCH MANAGEMENT

Patch is defined as an incremental software change in order to address a security vulnerability, reliability or operability issue, or add a new feature (refer to IEC 62443-2-3 and IEC 62443-2-4).

This paragraph does not differentiate the patch for an Operating System (OS), an antivirus program, the application program or any third party program.

Patch shall not affect the reliability, the operability or the safety of any SII components.

Patch shall be tested and certified by the SII equipment Vendor. A notification of release for each patch shall be provided by the SII equipment Vendor.

Prior to any installation on SII equipment, the patch shall be subjected to internal test(s).

SII equipment Vendor shall provide the necessary test bench to perform these internal tests without affecting the equipment used in a production environment.

SII equipment Vendors shall provide the documentation describing the software patching policy.

SII equipment Vendor shall qualify in terms of applicability and compatibility all relevant patches by analyzing and verifying the patches, including patches that are released by the Vendor of the OS or any third-party software used part of its scope of supply. SII equipment Vendor shall provide part of its inventory, the list of all release notifications.

Documentation that describes how to perform patching manually and how to obtain patching status reports shall be provided.

6.1.2 ANTIVIRUS

All workstations e.g. Engineering, Maintenance, Operator and servers shall have the capability to receive an antivirus program (see IEC 62443-2-4).

The antivirus program with the relevant virus definition file shall be certified and supported by the SII equipment Vendor. The virus definition file contains information that allows an antivirus program to recognize files which contain a virus.

6.1.2.1 Antivirus Study

Antivirus programs and updates may also pose a cybersecurity risk. Their need shall be studied on a system-per-system basis.

This study shall mainly take into account the foreseeable impact and probability of antivirus threats on the relevant SII equipment, the SII equipment Vendor certification, the capability of testing any updates without disturbing the SII equipment.

6.1.2.2 Antivirus Management

Configuration of the antivirus software is the responsibility of the SII equipment Vendor, in order not to impair the behavior of the device (specifically the Operator workstations).

Documented instruction for the proper installation, configuration and update of the antivirus mechanisms shall be provided.

An antivirus server within the SII shall be considered. This antivirus server allows regular & automatic updates of all workstations after downloading from the quarantine workstation (QWS) the antivirus definition file.

This antivirus definition file may be downloaded on the antivirus server either manually or automatically from the DMZ quarantine workstation (for example using an "FTP get" command).

This antivirus server shall be designed and configured to allow a staged definition file update.

This will allow the definition file update to be verified on a single station prior to update all the others.

Stand-alone equipment such as Safety Systems (SIS and FGS) workstations, third party packages workstation may be individually manually updated.

The SII equipment Vendor should specify which directory/files not to scan (with justification), the scanning periodicity and sequence for several workstations, automatic action to be taken after detection, etc.

Logging of events shall be configured in order to report any detection on the antivirus server.

The antivirus policy shall ensure that the antivirus definition file updates are verified prior installation on SII equipment.

Tools and procedure for updating the antivirus definition file shall be provided and tested for all systems within the SII.

Company may specify the preferred antivirus brand to be used for the project; in this case the Vendor shall validate the specified software.

7 OBSOLESCENCE MANAGEMENT AND LIFE CYCLE

The CONTROL AND SAFETY SYSTEMS shall be designed to last the lifetime of the installation (2 years) and shall offer flexibility to allow for future extensions or upgrading in accordance with 123A90-DDL-IN-PRO-40028 "Life Cycle Management Plan (Obsolescence issues and timing requirements)".

Strategy for managing obsolescence needs to be regularly updated as an integral part of the core functions:

- Design and development
- Sourcing and production
- In-service sustainability
- Vendors support

The obsolescence dossier will consider the complete life cycle including:

- Design phase
- Project delivery phase
- Operation & maintenance phase

The obsolescence dossier shall be further complemented by MAC VENDOR and Package Vendors, and shall detail all aspects of equipment life cycle. For more details, please refer to Project Specification "Obsolescence Study dossier", Ref AR-FEN-10-DOEC-373001

7.1 Instrument Asset Management System

An Instrument Asset Management System (IAMS) covering instrumentation shall be provided to maximise the diagnostic and monitoring abilities of the facility. The functionality of this shall be largely provided for by hardwired instrumentation via the 4-20mA HART revision 7 protocol. Packaged Vendor equipment with UCPs shall also provide diagnostic data over the Profinet (alternately Modbus interface).

8 SCOPE OF WORK

8.1 General

As a minimum, the MAC VENDOR shall be responsible for:

- The engineering, detailed design, procurement, manufacturing, assembly, configuration, wiring, supply, testing, quality assurance procedures and documentations of the Process Control System.
- The implementation of all application software(s) including system and user configuration, testing and debugging of the communication protocols between his own equipment and those supplied by others.
- Supplying FAT procedure (Functional Blocks, hardware, software)
- FAT (Functional Blocks, hardware, software) and integration tests with other sub-systems interfacing with the PCS.
- Ensuring that the PCS supplied meets all the requirements of this specification.
- Supplying all items not specifically mentioned but necessary for the correct operation of the PCS.
- Supplying Assistance to Commissioning Activities Phase.
- Supplying assistance to Start-Up Activities Phase.

The COMPANY shall provide for operation training to support electrical and process functions and technology of BLPH. The MAC is to provide operator training to facilitate this.

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

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

Comments made by COMPANY and 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

PAS VENDOR is responsible for all supplies covered by the present specification and mainly summarised as follows for the Process Automation System part:

- Independent redundant controller set including communication interface modules for PCS. Panels containing the PCS system, I/O and logic controllers shall be located in Offshore ITER.
- Engineering Workstation (EWS) in OER and Offshore ITER 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 (Internal to the PCS system).
- 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 HMI Graphic displays
- 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 Services

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

PAS 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 and consumable items for Start-Up,
- Recommended two years operation spare parts and consumables,
- Interface communication protocols (Hardware & Software) with equipment supplied by other parties (packages, PLC, Microprocessor systems, ...),
- Coordination with other suppliers for the PCS's interconnections,
- System test procedure for shop and field tests,
- Integrated Factory Acceptance Tests (IFAT) (and dedicated procedures) including test of PCS interfaces with other systems,
- FAT procedures including as a minimum:
    - Functional Blocks FAT procedure,
    - Hardware FAT procedure,
    - Software FAT procedure,
- Factory Acceptance Test (FAT) including as a minimum:

- Functional Blocks FAT,
- Hardware FAT,
- Software FAT,

- Packing and shipment to job Site,
- Site services (Technical assistance during Start-Up and commissioning, Inspection, Tuition, Tests, Training),
- Site Acceptance Test (and dedicated procedures, including COMPANY's performance check out at the factory),
- Co-ordination with CONTRACTOR,
- Software licences,
- HMI screens.

9 TECHNICAL REQUIREMENTS

9.1 General

9.1.1 BASIC DESIGN

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

- Automatic continuous process control (monitoring, control adjustment…).
- Logic sequencing.
- Data management (acquisition, status, treatment, storage).
- Alarm handling generated by PCS, EMCS, Safety System, HVAC and packages (annunciation, logging event recording, alarm suppression, sorting, and printing). An alarm management system shall be developed to assist operators in handling the multiple alarms associated with a shutdown occurrence.
- Communication with other equipment (packages, other systems, PLC, etc.)
- Generation of reports, historical archiving of events, alarms and process data on the Historian server (part of the OWS).
- Automatic diagnostics.
- HART acquisition system (communication cards, software…)

The PCS shall be based at least on a Programmable Logic Controller (processor module(s), redundant power supply unit(s), communication module(s), I/O cards). All components of the Programmable Logic Controller system shall be fully integrated and installed in cabinets.

The PCS and Safety System (SIS and FGS) will be dedicated to their main task and should be completely independent. Each one shall run alone. Data from the safety system shall be exchanged with the PCS through a communication link.

9.1.2 OPERATOR INTERFACE

The operator interfaces shall be via an Operator Workstation (OWS) located in the Central Control Room (onshore).

The platform OWS will provide an operator interface for both routine control and incident management via PCS and via the Safety System.

Human Machine Interface shall be in English language.

9.1.3 OPERATOR FACILITIES

PCS Operator Workstation (OWS) comprising LCD with keyboard and pointing facilities will be provided for the operators and located in the central control room.

The PCS OWS shall also be used for the safety operator interface.

In addition, a Engineering (EWS) rack type will be located in the platform technical room, initial plant commissioning and during local start-up operations.

The 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.

9.1.4 MAINTAINABILITY

The Process Automation 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 PAS OWS.

The Process Control System shall require minimal or no manual intervention. The automatic reconfiguration upon replacement of card shall occur.

The Process Control System shall have capability of on-line software download from the PAS EWS. Live download shall require security password to avoid unauthorised access.

Access to all equipment for maintenance shall be provided.

9.1.5 SYSTEM RELIABILITY AND AVAILABILITY

The minimum required availability shall be for the Process Automation System: 99.95%.

Failure and subsequent on line replacement of any CPU, I/O or communication module shall not affect the working of any other components or cause a system failure.

9.1.6 REDUNDANCY

To obtain the required availability, redundant facilities have to be provided for:

- Process Control network
- Safety Control network
- HMI Network
- Power supply modules
- Controller modules
- Data link communications to the safety system (SIS, FGS). For other systems, redundant communication will be determined case by case.

Redundancy shall be required for critical equipment such as controllers, power supplies, main PAS network and associated communications cards. I/O cards do not require being redundant as long as the overall availability of the system is met.

When the redundancy is contained within one physical module, the slots shall be arranged in adjacent pairs, the left slot containing the module and the right slot empty ready to accept a replacement card. When the redundancy is achieved using two or more physical modules, then they shall be positioned in adjacent slots.

Changeover of any redundant faulty equipment (from duty to back-up and back-up to normal configuration) shall be performed without affecting the relevant application.

9.1.7 MODULAR AND FLEXIBLE

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

The Process Control System shall be designed to minimise 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.

9.2 System Architecture

The Annex 1 Typical Architecture Block Diagram gives the main principles of the control and safety systems 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

9.3.1 PCS REQUIREMENTS

All modules shall be replaceable on-line, without requiring special tools or degrading required performances. Re-initialisation of new components shall be automatic, without specific operator actions.

Failure of any controller card shall generate an alarm to the HMI and shall be alarmed, logged and visualised in “System View” displays.

Controllers shall continuously monitor the status of each component. Auto test and internal diagnostic of major parts (I/O cards, processors, buses, memory, and power supply) shall be considered as being of primary importance, as well as system faults monitoring.

The system shall include controller nodes with associated I/O cards and communication cards.

Depending on the size of the system, multiple nodes connected to the PCS network may be required.

PCS controller nodes used for Safety system-PCS data exchange shall be dedicated to this function.

Loss of the controller shall cause all outputs to be frozen at their last position or driven to predefine fail safe positions, according to all safety requirements. Data processing consequences (non-significant measurement, no longer processed control functions, etc.) shall be indicated to the operator according to HMI requirements. Similar requirement applies in case of card failure.

Controller shall have non-volatile memory and shall be able to perform its own control functions.

Low battery level alarm shall be included as part of diagnostic alarms.

Generally I/O cards will not be redundant except where availability requirements may determine otherwise.

Communications between packages with PCS controllers will be either:

- hardwire link through the marshalling cabinets for status and on/off (if required)
- software link (Profinet or Modbus TCP/IP communication link) for general data.

The following development facilities shall be utilised for the configuration of application programs:

- Logic block diagram.
- Sequential Function Chart (SFC),
- Standard programming languages (C.).

Controller shall be supplied with a minimum set of functionalities to allow the operation of the plant. The following requirements are to be considered as a strict minimum.

- All PCS hardware shall be CE marked.
- All PCS hardware shall be new equipment, second hand equipment is forbidden.

9.3.1.1 Control algorithms

PCS controller shall be able to perform PID control, ratio control, cascade control, supervisory set point control, etc. The algorithms shall be adjustable as far as that the access control allows it.

Computational algorithms for math functions such as addition, subtraction, multiplication, division, square root extraction, logarithms shall be included. Other functions as dead time, high/low selection, high/low alarming (for input and output signals and calculated values), time average, and signal selector switch shall also be included.

During operation, switching from auto to manual output mode or switching from local to remote set point shall be performed without bumping.

9.3.1.2 Digital algorithms

The controller must handle a large number of binary inputs and outputs to operate valves and pumps. This requires the use of binary "blocks" allowing inputs and several outputs to be processed to implement: auto/manual processing, on/off control, discrepancy alarming, interlocking and duty/stand-by changeover.

The controller shall support logic functions such as AND, OR, NAND, NOR, XOR, NOT, as well as timers, delays, and counters.

9.3.1.3 Sequence control

PAS VENDOR shall state and provide the programming language and tools necessary to implement sequences.

The interaction between analogue algorithms and sequences is a mandatory requirement. Sequences shall be synchronised with controller scan cycle.

The running of sequences in parallel in a controller is required. The PAS VENDOR shall ensure that the system is design to avoid locking-up the processors on a sequence.

9.3.1.4 Time management

PAS VENDOR shall detail internal time management and synchronisation between all PCS nodes (controllers, operator stations, external PLC…) and clearly state how accurate events can be discriminated (i.e. events in the same controller, controllers on same network, controller in different networks, safety systems, etc.).

The PAS VENDOR shall indicate the maximum discrepancies between the clocks of the different controllers and how these clocks are automatically synchronised.

9.3.2 POWER SUPPLY MODULE

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

The design shall be such that failure of one power supply does not affect the performance or integrity of the overall system.

The power supply modules shall be fitted with status and diagnostic LED's (as a minimum module status, fault).

The power supply modules shall be replaceable without affecting the working of any other PAS modules.

9.3.3 INPUT/OUTPUT REQUIREMENTS

I/Os shall be powered by 24V DC from the I/O cards or from the Field Termination Assemblies or for specific loops from the power supply terminal blocks located in the marshalling cabinets.

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 (PCS OWS).

All instruments and Accessories protection level shall be EEx"d".

EEx "i" will only be acceptable when EEx"d" are not available.

When intrinsically safe circuits are used, then an IS barrier shall be applied and shall follow the Project requirement stated in Project document "Safety System (ESD, Fire and Gas) Specification", Ref. 123A90-DDL-IN-SP-40100,

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.

PAS VENDOR shall include slots to accommodate I/O spare capacity of 10%.

I/O modules shall be associated to each control unit; they shall be designed such that a short circuit or a high voltage on one input (or output) will not induce a fault on any other I/O of the same module.

I/O modules shall be modular and rack-mounted with adequate identification of module types and tag numbers, replaceable on line without removing the signal wiring and without the need for special tools. They shall have LED's for card fault indication, mounted on the front of the card.

Insulation test voltage shall be as a minimum 500V.

The system shall have self-diagnostic programs that run independently from the application programs on a continuous basis with fault detection capability down to the I/O module individual channel.

It shall be possible to replace cards without switching off the power. The modules shall be replaceable without requiring special tools. All modules shall be replaceable on-line without degrading the system performance. Re-initialisation of newly installed module shall be automatic.

Each PCS board power supply shall be overload protected.

Input and output cards shall have a galvanic isolation between field equipment and the system.

Each Input/output channel shall be fully isolated and shall be able to operate in parallel. Input/Output channel shall be individually protected by fuse.

When instruments (such as flowmeters, analysers and gas detectors) have their own power supply or use an external power supply, analogue I/O boards shall be protected by fuse on the input signal.

When an analogue input board powers the instrument on a separate (3rd) wire that wire shall be fuse protected. Otherwise each input and/or output shall be individually short circuit protected and shall have electrical insulation between thePAS and the plant.

All I/O PCS boards shall be provided with dedicated connectors for connections with their Field Termination Assemblies (FTA) located in the marshalling cabinets.

Careful consideration shall be given to allocation of I/O to cards in order to ensure that failure of a single card or component does not impinge on overall system and plant functionality and performance.

9.3.3.1 Analogue Input

These converters shall be dedicated to each input point, otherwise a redundant design shall be provided.

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

Each input channel of card shall be isolated from the others and protected by fuse.

Input cards shall have filters for EMI/RFI protection.

4-20mA analogue input modules shall be able to power 2-wire field transmitters.

The transmitters shall be powered by 24V DC from the PCS through galvanic isolation.

Few self-powered transmitters shall also be connected to analogue input module.

Accidental application of main supply voltage or test voltages shall not damage the modules.

Smart Transmitters

All smart devices shall interface with the PCS via bi-directional HART Revision 7 digital communication with the smart transmitters.

Electronic transmitters shall be smart type based on HART protocol. Transmitters shall be capable of supporting full digital communications with the selected system.

Smart devices shall be used for diagnostics and calibration purpose from the PCS.

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 Analogue Outputs

These converters shall be dedicated to each output point, otherwise a redundant design shall be provided.

Each analogue output shall be a standard 4-20mA DC signal. The output channels shall be isolated, independent and individually protected by fuse.

Analogue output shall be powered by PCS internal 24V DC supply.

The negative and positive sides of the circuit output shall be wired to independent terminals (common supply or return bus-bar is not allowed).

The system shall detect and alarm operator when a discrepancy occurs between the software values generated by controllers and the real electrical value of the output.

9.3.3.3 Digital Inputs

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. 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.).

If required, NAMUR amplifiers for proximity limit switches shall be provided by SUPPLIER.

9.3.3.4 Digital Inputs Supervised (DIS)

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

VENDOR shall follow the "Safety System (ESD, Fire and Gas) Specification", Ref. 123A90-DDL-IN-SP-40100.

9.3.3.5 Digital Outputs

Each output shall be configurable 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 isolated and independent.

Output modules shall be able to drive loads powered by an external supply or by modules internal source.

Two different types of digital output shall be required:

- 24V DC powered outputs powered by the PCS,
- Volt-free / ground-free output rate 24V DC powered by other systems.

Output contacts shall be suitably protected against surge current when switching-off inductive DC circuits.

Auxiliary relays, when used, shall be plug-in type with socket, sealed with heavy silver or gold contact according to the voltage.

9.3.3.6 Communication card(s)

Communication card(s) shall be provided for the data links between the PCS and the following equipment:

- Control network,
- Packages when required:
  - Electrolyser
  - Fuel cell
  - BESS,
  - HVAC,
  - Instument Air
  - Nitrogen
  - Water Treatment
- Etc.

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

Open communication by a various kind of standard protocols based on Profinet by default (and MODBUS TCP/IP as an alternative). Physical interfaces may include, but not be limited to, Ethernet (IEEE 802.3).

The PCS will be dedicated to their main task and will continue to operate in the event of an inter-systems communication failure.

As part of the bid, PAS VENDOR shall provide a list of all communication protocols that the offered system can support to interface with third party systems.

9.3.4 TIME SYNCHRONISATION

All Control and safety systems elements shall be time synchronised. All PCS elements shall be time synchronized.

The PAS system shall use a suitable GPS clock or equivalent to synchronise its network clock. The GPS clock shall also provide clock synchronisation signals to PCS.

NTP Time Server, shall be installed into PCS Network. NTP data packets shall be broadcasted over the SII network as well by the Firewall in between PCS / SII networks

Offshore PCS shall be synchronised and shall be the clock master for time synchronisation of the platform safety system and other systems (e.g.: packages).

Time synchronisation between all control and safety systems equipment shall be configured to allow events and incident analysis.

PAS VENDOR shall detail all time management facilities and synchronisation types between all PAS sub-systems.

Time synchronization between all PAS sub-systems from all entities shall be better than +/- 25ms.

PAS VENDOR shall clearly state the technique of how the system discriminates between events and alarms. The time stamping shall be based on the CPU cycle time.

9.4 Software Requirements

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

- Hardware configuration editor,
- Communication configuration editor,
- Logic configuration and compiler,
- Diagnostic of system faults,
- Event logger,
- Cross Reference list between database and display,
- Off-line simulation,
- Application graphic builder,
- Alarm management,
- Report generation builder,
- System access security management,
- Smart Field devices management,
- Network management,
- Database management,
- System and network diagnostic,
- File management utilities,
- Print services,
- Message board,
- Asset management functionalities,
- On-line documentation.

Setting of alarm levels for analogue inputs, setting of timers shall be done by software configuration via the OWS.

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.

Complete and comprehensive documentation shall be provided with the delivered system that covers each of the software modules. The documentation shall be available in USB Memory Stick or equivalent and fully set up on the EWS.

All system software, configured and tested during FAT, shall be delivered to COMPANY together with software operating license as per IEC61131.

9.5 Operator Interface

9.5.1 OPERATOR WORKSTATION (OWS)

The main operator interface is the Operator Workstation (OWS) located in the onshore control room.

Operator Workstation shall be based on WINDOWS operating system, latest available version at PAS contract award.

The main control of operations shall remain onshore at the CCR via the PAS Operator Workstation.

Each OWS shall allow the operators to perform all routine process adjustments such as changing controller set points and alarm settings, opening and closing valves starting, stopping and duty selection of pumps, initiating starting sequences, etc...

As part of the documentation to be developed during the Project, PAS VENDOR shall provide all required information for the future modifications and integration of BLPH project to the Onshore System. That onshore works will be performed within a third-party Scope of Work. As a minimum, the following input shall be defined:

- Details on the data transfer: communication protocols, data exchange,
- Quantity of HMI screens to be provided.

Multiple levels of security access shall be provided as per IEC 62443-2-4 (engineer, method, maintenance, Operator and visitor) protected by hardware or software key.

One Local OWS shall be installed in BLPH technical room. This OWS shall also function as an EWS and incorporate the historians' functions. Access shall have password protection and user shall decide to access either as operator or as maintenance/engineering workstation. The default configuration is that OWS shall be log-in as operator.

PAS VENDOR shall size the system accordingly to support the required various functions.

PAS VENDOR shall supply, install and configure any software that the OWS need to perform its intended functions.

9.5.1.1 Operator workstation

The Operator Workstation (OWS) shall be composed of a double screen VDU, one functional keyboard and one trackball or equivalent device.

9.5.1.2 HMI Video Display Unit (VDU)

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

The minimum requirements for the VDU shall be:

- Diagonal size 23,8" as a minimum,
- Flat screen,
- Full HD 1920 x 1080 pixels,
- Colour gamut 86 %, from SUPPLIER's standard palette,
- Height adjustable stand, tilt, swivel, pivot and built-in cable management,
- Response time 8 ms as a minimum,

- Pixel Pitch less than 0.2.

9.5.1.3 Operational keyboard and trackball

The keyboard shall be a QWERTY keyboard. An easy-to-use trackball/touch pad shall also be provided.

These devices, when pointed to a target on the screen, shall not directly initiate any control function, with only one action. Confirmation is always required by the activation of either the "enter" key of the keyboard or a specific trackball push button.

Errors such as entry of "out of range values" or clicking "wrong screen zones" shall be signaled by means of audible tone and/or visible warning.

The keyboard/trackball shall allow the user to perform operating, tuning and configuring functions, from configurable dedicated function keys.

The cursor shall be able to change from one screen to the other without special action.

9.5.1.4 HMI system electronics

The system electronics shall consist of a microprocessor-based system, which supports connections to keyboard, mass storage unit, VDU, trackball and printing driver.

Dedicated system electronics shall be provided for the Operator Workstation.

All electronics shall be powerful enough to allow complete control of the BLPH Platform (including historian server) to be performed on one unique station. All electronics shall support communication interface module to ensure an efficient connection to the CONTROL AND SAFETY SYSTEMS communication network.

The HMI system electronics will be by remote installation of OWS electronics with OWS system electronics housed in dedicated locked cabinet and via a KVM on control desk in the Onshore technical room/ITER.

9.5.1.5 PCS EWS functions

Maintenance access to the Safety System shall be done via the EWS.

The onshore EWS will be connected to the offshore using the HMI-A/B Network.

VENDOR shall supply install and configure any software that the PAS workstation need to perform its intended functions.

Modifications of the system functionalities shall be allowed only under password and/or key protected access.

EWS shall facilitate maintenance functionality for the PAS.

In this case, the workstation shall enable the following functions to be performed:

- System configuration,
- System maintenance,
- PCS and network system performance monitoring,

- HART devices configuration and maintenance management,
- Display graphic builder,
- Application and logic builder,
- File management,
- Download a modified configuration into the PCS,
- On-line and off-line system test, diagnostic and systems performance reports,
- On-line system documentation,
- Off-line simulation.

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

9.6 Historian Server

Historical configuration is fully integrated into the control and safety systems configuration (a native function of the PAS) and is a complete different system from the PDS.

The PAS operator workstation includes an access to the historian data. The storage of these data collected in a buffer is done cyclically and event triggered. All data logged will be time stamped.

Historical data collected from controller is available for viewing and analysis as embedded displays to provide the operator with more information.

Historical data collected should be exported in csv format or equivalent.

Different data can be stored in the same journal e.g. batch journal containing events, history trends and reports related to a specific batch.

In order to limit control and safety systems network traffic, historian data collection shall have capabilities such as data compression.

Minimum retention time should be at list at 1sec.

The history data is available for use across workstation for trend displays, reports, custom displays, applications, spreadsheets.

All the historian data will be collected in the server and/or "data collectors". Historian server shall have enough capacity to store one month events and trending of the whole control and safety systems. It shall use redundant hard disks based on Raid 5 technology.

The system will be studied and optimized in order to reach the 100% data availability.

9.7 Alarm Management System

An Alarm Management System shall be provided to ensure that the operator is alerted to plant upsets in a clear manner without being overloaded during normal operation, downgraded operation and even plant upset.

All OWS shall be provided with alarm management interface facilities.

Minimum functional requirements and rules to be applied are defined by Alarm System Requirements Specification, Ref 123A90-DDL-IN-SP-40024.

9.8 System Performances

The Control and Safety Systems shall be responsive to real-time process data change, events or operator manual inputs to ensure the plant operates efficiently, safely and accurately. PAS VENDOR shall be responsible to check and size the system to meet the intent.

PAS VENDOR shall note that the definitive peak load figures may change during detail design and thus, PAS VENDOR shall reconfirm system performance accordingly.

PAS VENDOR shall include in the bid, the initial overall system performance calculations based on the I/O.

PAS VENDOR has to submit the different calculated response times for the complete system in the bid.

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

The performances shall be checked during the project development stage and during acceptance test.

The proposed equipment, including the operator control stations shall tolerate unexpected power supply failure at any geographical location.

The Control and safety systems shall restart automatically upon power supply restoration without extensive time-consuming system rebooting procedures and without the needs for highly qualified engineers.

The Control and safety systems restart procedure shall not be more than 5 minutes upon power supply restoration (per equipment, e.g. controllers, OWS, etc.).

9.9 PAS Networks

PAS Networks refers collectively to the PAS control node data and PAS OWS network, separate maintenance network is foreseen for the EWS.

The PAS Network shall be industrial type Ethernet IEEE network (10/100Mbps). 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.

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

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

The PAS Network together with any required accessories (switches, etc.) shall be supplied by PAS VENDOR. The Network/Package Cabinet which shall house the PAS switches shall be connected via a redundant Ethernet communication link. Maintenance network switches shall also be integrated in the Network/Package Cabinet.

The Offshore EWS pc shall be installed inside the offshore network cabinet.

The Onshore EWS pc shall be installed inside the Server cabinet.

The PAS Network shall provide error-free transmissions. PAS 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.

9.9.1 HMI NETWORK

This network shall interconnect the various nodes of the PAS system including controllers, workstations and servers. The network shall be fully redundant including communication cards.

9.9.2 SERVICE NETWORK

Maintenance network will be interconnected between onshore and offshore throughout the Telecom SIE links. This network allows for OWS and historian servers, anti-virus update, printers and other service functions for the PAS.

9.9.3 SAFETY CONTROL NETWORK

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.

The PAS OWS located in the CCR is the operation window for the safety system (ESD and FGS).

9.9.4 CONTROL NETWORK

This network shall provide connections between all nodes belonging to the PCS and EMSC 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 Control network which shall not be shared with any other communication networks.

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

9.9.5 TECHNICAL NETWORK

This Network shall provide access to the DMZ and Access to maintenance services such as backup servers, Antivirus servers and VM- Hosts.

9.9.6 PROFINET/IEC61850 NETWORK

This network shall provide access between third party packages and the PCS/EMSC controllers.

9.10 Interface with Third Party Systems

9.10.1INTERFACE WITH LV SWITCHBOARDS

Interface with LV Switchboard shall be done in accordance with "Technical Specification for Electrical Monitoring and Control System (EMCS), 123A90-DDL-EL-SP-20039"

9.10.2INTERFACE WITH PACKAGES

External interfaces with Package units will be implemented to provide control and monitoring from the PAS.

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

Interface between packages and PAS may be via communication links or hard wired (less than 20 data points). The selection will be determined by the quantity of data to be transmitted.

Communication protocols such as Profinet by default (MODBUS TCP/IP as an alternative) shall be preferable. PAS shall act as master.

All signals generated from the UCP shall be available for transmission to the PAS as per the requirements of DEP 33.64.10.32, the CCS shall be designed to perform event time stamping at 1 ms. However, given the nature of the plant, load shedding and upset conditions are not expected to be as prominent as in traditional hydrocarbon plants with turbine compressors and generators. As such, data recording at 1 ms may prove to be excessive, i.e., recording of uneventful events. Therefore, the response of the system shall be rationalised for the upset conditions that are identified by EPCI contractor through HAZOP and SAFOP studies. Any bidders shall provide options for minimising any data recording whilst ensuring any upset events are captured.

The communication interface shall be certified "Interference Free" according to DIN V 19250.

Hardwire to PCS for time synchronisation and system fault alarms shall also be provided.

CONTRACTOR shall arrange for a complete testing of all Packages type / PAS communication links mapping at the ICSS VENDOR works during the FAT. Communication testing shall include the actual hardware, applications and simulation means. Integration tests shall be performed by PAS VENDOR with all package systems witnessed by CONTRACTOR and COMPANY engineers.

BLPH System will interface with the following package systems but not limited to:

- BESS
- Electrolyser
- Fuel Cell
- Solar farm

- HVAC Panel B-100 Container
- HVAC Panel B-200 Container
- HVAC Panel B-300 Container
- HVAC Panel B-400 Container
- Water treatment
- Instrument Air
- Nitrogen
- Wind farm (HV-SCADA)

9.11 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 controllers, I/O cards, power supply units and communication links.

Marshalling cabinets shall be provided for housing the Field Termination Assembly (FTA) mirror of the I/O cards, the IS barriers (if necessary) and the Field Terminal Blocks (FTB) mirror of the field cables (mirror of the junction boxes).

Allocated cabinet configuration:

- B400-PCS-001(Controller + Marshalling) in ITER
- B400-PCS-002(Marshalling) in ITER

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.

9.12 Network Cabinet

The network cabinet shall be in accordance with the Project document "Automation Detailed Design and Construction Package" referenced 123A90-DDL-IN-DD-40029.

The network cabinet shall follow the same requirements as stated in section 9.11. For system cabinet. Cabinet and all associated equipment (e.g.: switches) with redundant power supplies shall be provided by the PAS VENDOR.

The network cabinet shall include two major functions:

- Interfacing the System with
  - Packages
  - On-shore link between the Onshore Control Room and BLPH.
- Containing all the Switches for the PAS networks (refer to section 9.9)

Allocated cabinet configuration:

- B400-NET-001 (Network)
- OER-SRV-001 (Server)
- OER-NET-001 (Network)

9.13 Cables and Wiring

All cabinet internal 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.

9.13.1 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.

9.14 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.

9.15 Earthing

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

Earthing in hazardous areas shall adhere to IEC 60079-14, ref. doc. "Earthing Layout drawings (Offshore ITER)",123A90-DDL-IN-DL-40013.

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

9.16 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.

9.17 Spare Capacity

The CCS 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 CCS 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 reserved 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.

VENDOR shall deliver documentation in accordance with Project document "MR – Automation systems CCS-SIS" referenced 123A90-DDL-IN-MR-40103.

10.2 Software Requirements

PAS 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").

PAS VENDOR shall provide to COMPANY/CONTRACTOR all the software licences 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 PAS VENDOR.

10.3 Documents Presentation

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

11 INSPECTION, TESTING AND ACCEPTANCE REQUIREMENTS

11.1 General Requirements

VENDOR shall be responsible for the integration, inspection and testing of the Control 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 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 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.

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.

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

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.

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.

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.

15 ANNEXES

Annex 1 – Typical Architecture Block Diagram

