MICROSOFT WORD / V. 2016 / I-ET-3010.00-5520-862-P4X-001_F.DOCX

INDEX OF REVISIONS

REV.	DESCRIPTION AND/OR REVISED SHEETS
0	ORIGINAL ISSUE
A	GENERAL REVISION
B	REVISED WHERE INDICATED ACCORDING TO CONSISTENCY ANALYSIS
C	REVISED WHERE INDICATED
D	REVISED WHERE INDICATED
E	REVISED WHERE INDICATED
F	REVISED WHERE INDICATED

	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G	REV. H
DATE	SEPT/19/18	JAN/22/20	JUL/20/20	JAN/11/21	AUG/18/21	AUG/12/22	SEP/30/22		
DESIGN	ESUP	ESUP	ESUP	ESUP	ESUP	ESUP	ESUP		
EXECUTION	CAMILA	CAMILA	CAMILA	U5D6	U5D6	U44D	C27N		
CHECK	GNIEDU	PATRÍCIA	EDYLARA	CLWK	U49R	U5D6	U5D6		
APPROVAL	PEDRO	ANDRÉ LUIS	ANDRÉ LUIS	U49R	U4JB	CDC1	CDC1		

SUMMARY

1 INTRODUCTION 3

2 REFERENCE DOCUMENTS, CODES AND STANDARDS 4

3 ENVIRONMENTAL AND OPERATIONAL CONDITIONS 7

4 COMPONENTS DESCRIPTION OVERVIEW 7

5 HARDWARE STRUCTURE 9

6 SOFTWARE STRUCTURE 10

7 HARDWARE REQUIREMENTS 11

8 SOFTWARE REQUIREMENTS 23

9 ACCEPTANCE TESTS 26

10 PACKING REQUIREMENTS 26

1 INTRODUCTION

1.1 Object

1.1.1 This Typical Technical Specification describes the minimum requirements and basic characteristics for the Programmable Logic Controllers (PLCs) that take part of the Control and Safety System (CSS) of the UNIT.

1.1.2 CSS is the system, which uses PLCs as its main components. Other equipment or system documents may also refer to this Technical Specification, entirely or in parts.

1.2 Definitions

1.2.1 Refer to I-ET-3010.00-1200-940-P4X-002 – GENERAL TECHNICAL TERMS for the definition of words emphasized in upper case along this document.

1.3 Abbreviations, Acronyms and Initialisms

1.3.1 The following abbreviations, acronyms and initialisms are used in this document:

A/D	Analog to Digital
AFDS	Addressable Fire Detection System
AI	Analog Input
ANP	Brazilian National Agency of Petroleum, Natural Gas and Biofuels (*Portuguese: Agência Nacional do Petróleo, Gás Natural e Biocombustíveis*)
AO	Analog Output
CO_2	Carbon Dioxide
CPU	Central Processing Unit
CSS	Control and Safety System
DI	Discrete Input
DI4	Discrete Input 4(Four) Wires
DO	Discrete Output
FAT	Factory Acceptance Test
FPSO	Floating, Production, Storage and Offloading
FPU	Floating Production Unit
HART	Highway Addressable Remote Transmitter
HMI	Human Machine Interface
HSDN	High Speed Deterministic Network
I/O	Input / Output
SNTP	Simple Network Time Protocol
OPC UA	Open Platform Communications Unified Architecture
PID	Proportional–Integral–Derivative Controller
PLC	Programmable Logic Controller
RTDS	Real Time Data Server
VCI	Volatile Corrosion Inhibitors
VDC	Voltage Direct Current

2 REFERENCE DOCUMENTS, CODES AND STANDARDS

2.1 External References

2.1.1 International Codes, Recommended Practices and Standards

IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION

IEC	60068	ENVIRONMENTAL TESTING
IEC	60092-504	ELECTRICAL INSTALLATIONS IN SHIPS - PART 504: AUTOMATION, CONTROL AND INSTRUMENTATION
IEC	60533	ELECTRICAL AND ELECTRONIC INSTALLATIONS IN SHIPS - ELECTROMAGNETIC COMPATIBILITY (EMC) – SHIPS WITH METALLIC HULL
IEC	60945	MARITIME NAVIGATION AND RADIO COMMUNICATION EQUIPMENT AND SYSTEMS – GENERAL REQUIREMENTS – METHODS OF TESTING AND REQUIRED TEST RESULTS
IEC	61000	ELECTROMAGNETIC COMPATIBILITY (EMC) SERIES - ALL PARTS
IEC	61086	COATINGS FOR LOADED PRINTED WIRE BOARDS (CONFORMAL COATINGS) – ALL PARTS
IEC	61131	PROGRAMMABLE CONTROLLERS - ALL PARTS
IEC	61892	MOBILE AND FIXED OFFSHORE UNITS – ELECTRICAL INSTALLATIONS - ALL PARTS
IEC	62337	COMMISSIONING OF ELECTRICAL, INSTRUMENTATION AND CONTROL SYSTEMS IN THE PROCESS INDUSTRY – SPECIFIC PHASES AND MILESTONES
IEC	62381	AUTOMATION SYSTEMS IN THE PROCESS INDUSTRY-FACTORY ACCEPTANCE TEST (FAT), SITE ACCEPTANCE TEST (SAT) AND SITE INTEGRATION TEST (SIT)

IEEE - THE INSTITUTE OF ELECTRIC AND ELECTRONIC ENGINEERS, INC.

IEEE	802.3	IEEE STANDARD FOR ETHERNET
ANSI/IEEE	C 37.90.1	SURGE WITHSTAND CAPABILITY (SWC) TESTS FOR RELAYS AND RELAY SYSTEMS ASSOCIATED WITH ELECTRIC POWER APPARATUS

2.1.2 Brazilian Codes and Standards

INMETRO - INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA

PORTARIA Nº 115 (21/MARÇO/2022)	REQUISITOS DE AVALIAÇÃO DA CONFORMIDADE PARA EQUIPAMENTOS ELÉTRICOS PARA ATMOSFERAS EXPLOSIVAS - CONSOLIDADO.

2.1.2.1 All *Secretaria de Inspeção do Trabalho* Regulatory Standards (NRs) shall be followed.

2.1.3 Classification Society

2.1.3.1 Project's Detail Design Phase documents will be submitted to Classification Society's approval and/or certification.

2.1.3.2 The design, installation and operation shall strictly follow the Classification Society's requirements, along with the specific requirements identified in this document, including also all referenced document requirements.

2.2 Internal References

2.2.1 Typical Documents

2.2.1.1 Typical Documents are those that contain functional and technical description of a system or equipment. A Project contains Typical Documents and specific documents, which describe the particularities of the Project.

2.2.1.2 Typical Document List

I-ET-3010.00-5140-700-P4X-003	ELECTRICAL REQUIREMENTS FOR PACKAGES FOR OFFSHORE UNITS
I-ET-3010.00-5520-861-P4X-001	CONTROL AND SAFETY SYSTEM – CSS
I-ET-3010.00-5520-861-P4X-002	SUPERVISION AND OPERATION SYSTEM - SOS
I-ET-3010.00-5520-888-P4X-001	AUTOMATION PANELS
I-ET-3010.00-1200-800-P4X-002	AUTOMATION, CONTROL AND INSTRUMENTATION ON PACKAGE UNITS

I-ET-3010.00-5522-855-P4X-001 ADDRESSABLE FIRE DETECTION SYSTEM

I-ET-3010.00-5520-800-P4X-004 AUTOMATION NETWORK REQUIREMENTS

2.2.2 Specific Project Documents

2.2.2.1 This section mentions documents that are referenced along the text and that are part of a specific project. The documents title and number may vary slightly from one project to another. Project's DOCUMENT LIST shall be consulted in order to verify the correct document number and title.

2.2.2.2 Specific Project Document List

TECHNICAL SPECIFICATIONS (I-ET)

INSTRUMENTATION ADDITIONAL TECHNICAL REQUIREMENTS

DRAWINGS (I-DE)

AUTOMATION AND CONTROL ARCHITECTURE

NETWORK INTERCONNECTION DIAGRAM

DESCRIPTIVE MEMORANDUM (I-MD)

AUTOMATION NETWORK DESCRIPTION

LISTS (I-LI)

DOCUMENT LIST

2.2.3 PETROBRAS Reference Documents

DR-ENGP-M-I-1.3-R.5 SAFETY ENGINEERING GUIDELINE

2.3 In cases where Brazilian regulatory standards (*Secretaria de Inspeção do Trabalho)* and INMETRO regulations are more restrictive, these shall superpose all codes and regulations listed in item 2, since they are enforced by Brazilian law. Additionally, in cases of conflicting requirements, Brazilian regulatory standards shall be adopted.

3 ENVIRONMENTAL AND OPERATIONAL CONDITIONS

3.1 For environmental and operating conditions and/or any requirements regarding this topic, refer to project's technical specification entitled INSTRUMENTATION ADDITIONAL TECHNICAL REQUIREMENTS. Special attention shall be given to the dynamic loads imposed by the vessel motions during tow and on location and to the temperature of the indoor ambient on loss of HVAC.

3.2 All PLC components shall be supplied installed inside panels, according to I-ET-3010.00-5520-861-P4X-001 - CONTROL AND SAFETY SYSTEM – CSS and I-ET-3010.00-5520-888-P4X-001 – AUTOMATION PANELS

3.3 The available power supplied by the UNIT to PLC panels is defined in I-ET-3010.00-5140-700-P4X-003 – ELECTRICAL REQUIREMENTS FOR PACKAGES FOR OFFSHORE UNITS. Internal panel power source distribution shall be according to I-ET-3010.00-5520-888-P4X-001 – AUTOMATION PANELS.

3.4 Power supplied to each PLC internal components (CPUs, I/O cards, network cards etc) shall be 24 VDC. See also item 7.9.

4 COMPONENTS DESCRIPTION OVERVIEW

4.1 General Description

4.1.1 The following items present the PLC main components to be considered. The detailed scope can only be inferred after reading this entire specification and the related documents. Except for the number of programmable logic controllers, I/O points, accessories and others functions of the Application Program, the hardware/software requirements set forth in this Specification apply equally to any PLC in the CSS (see I-ET-3010.00-5520-861-P4X-001 - CONTROL AND SAFETY SYSTEM – CSS).

4.1.2 This technical specification does not necessarily apply to the PLC of PACKAGED UNITS. For more information on how PACKAGED UNITS shall interface with the CSS and its PLCs, see I-ET-3010.00-1200-800-P4X-002 - AUTOMATION, CONTROL AND INSTRUMENTATION ON PACKAGE UNITS and I-ET-3010.00-5520-861-P4X-001 - CONTROL AND SAFETY SYSTEM – CSS.

4.1.3 Brazilian Local Content pertaining to Automation and Instrumentation products and services shall be in accordance with the requirements defined by ANP. Hardware components such as CPU, power sources, communication cards, racks, I/O cards as well as services such as configuration, application development, FAT and commissioning shall meet the local content requirements.

4.2 Hardware

4.2.1 The PLC CPU racks shall be arranged in redundant half-clusters in hot standby configuration. Figure 1 presents a PLC cluster with its two half-clusters, A and B, operating in hot standby.

.

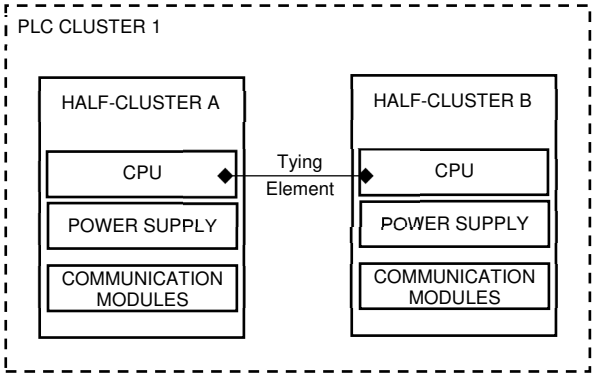

Figure 1 – PLC cluster and its half-clusters in hot standby.

4.2.2 Each half-cluster shall have enough communication modules/cards in order to establish, among other networks, the Redundant High Speed Deterministic Network (HSDN), which shall be used to link all CSS PLCs. For more requirements regarding the HSDN see section 7.2.3. For a detailed description of the HSDN, see I-ET-3010.00-5520-861-P4X-001 - CONTROL AND SAFETY SYSTEM – CSS and project's drawing entitled AUTOMATION AND CONTROL ARCHITECTURE.

4.2.3 There shall be a Redundant Remote I/O Deterministic Communication Network, linking the half-cluster of each PLC cluster to the respective Remote I/O racks (i.e., each half-cluster shall read two communication cards from the corresponding Remote I/O panel).

4.2.4 Ethernet TCP/IP Interfaces: at least four (04) for each PLC half-cluster. These interfaces shall be used for communications between Real Time Data Server (RTDS) and all PLCs through CSS DATA ACQUISITION LAN (see project's drawing entitled NETWORK INTERCONNECTION DIAGRAM). At least two Ethernet-TCP/IP Interfaces shall be mounted on each PLC rack, two in the main PLC rack and two on the hot standby PLC rack in order to comply with the redundant topology.

4.2.5 Ethernet-TCP/IP and/or USB Interfaces for programming functions: 4 (four) of the same type for each PLC cluster, 2 (two) per half-cluster.

4.2.6 Modbus interfaces:

- Two Modbus TCP interfaces for each half-cluster for redundant communication with the Electrical System's processor.

- One Modbus TCP interface or Modbus RTU interface for each half-cluster for communication with the corresponding AFDS half cluster (for more information

see I-ET-3010.00-5522-855-P4X-001 - ADDRESSABLE FIRE DETECTION SYSTEM).

4.2.7 The following components shall have diagnostics capability: all I/O cards, communication modules, redundancy modules, CPUs and power supplies. Diagnosis signals shall be made available in a memory region accessible by the Supervision and Operation System.

4.3 Software

4.3.1 Application Program Editor with all necessary drivers for development and maintenance of all hardware that belongs to CSS shall be supplied.

4.3.2 For details on the Supervision and Operation System communications drivers refer to I-ET-3010.00-5520-861-P4X-002 – SUPERVISION AND OPERATION SYSTEM - SOS.

5 HARDWARE STRUCTURE

5.1 Cluster

5.1.1 The PLC hardware structure is constituted by 2 (two) components. The first, referred to as cluster, consists of the PLC CPU racks, and the second consists of I/O racks. The half-clusters that comprise one cluster shall be kept synchronized through a redundant tying element (see Figure 1). Failure of any of these components or of the communication channel(s) among them shall be alarmed in the Supervision and Operation System.

5.2 Half-Cluster

5.2.1 The half-cluster comprises 3 (three) groups of elements: CPU, power supply and communication modules.

5.2.2 The term "CPU" is reserved, in this Specification, for the PLC element responsible for running the Application Program.

5.2.3 The power supply group is the element responsible for supplying power to all the components that take part of the CPU rack.

5.2.4 The communication modules are:

- Standby Update Channel (tying element) or redundancy modules, which establish communication between half-clusters;
- High Speed Deterministic Network (HSDN), which establishes communication between clusters (CPUs with distinct functions);
- Ethernet-TCP/IP Interfaces and/or USB interface (if used) for communication with programming computer;
- I/O Deterministic Communication Network modules, which establish communication between PLC CPU and Remote I/O modules;

- Other communication modules necessary to integrate with third party equipment.

Each of these elements, as well as the CPU and the power supply, are assigned in one half-cluster in the Automation and Control Architecture.

5.2.5 Half-Cluster Operation

5.2.5.1 In the hot standby operation, both half-clusters shall run the same Application Program. Both half-clusters scan the inputs, but only the one configured as "active" effectively drives the outputs. Upon a failure of the active half-cluster, the output control is automatically transferred to the previously configured half-cluster in standby, which then becomes the new active half-cluster. This switching shall be signed by a PLC status register and shall be alarmed at Supervision and Operation System HMIs.

5.2.5.2 The Standby update channel (tying element) shall be redundant and dedicated to the hot standby function of the cluster.

6 SOFTWARE STRUCTURE

6.1 Program Editor and Application Program

6.1.1 The PLC shall provide means to be remotely configured and programmed. Software, referred to as the program editor, running on a PC or notebook, shall allow users to both configure the PLC hardware and develop the application program. The program editor software shall run under the latest Windows® operating system, with the latest Service Pack (SP) installed both for the software and for the operating system. After the development of the application program, the program editor shall allow it to be downloaded onto the PLC memory.

6.1.2 The languages supported by the program editor shall be in accordance with IEC 61131-3.

6.1.3 The program editor software's data shall be transferred to the PLC via Ethernet-TCP/IP interface and/or via USB port (whichever port is available in the PLC for programming functions).

6.2 Firmware

6.2.1 The firmware shall be furnished in the latest version available on the date of supply. If major updates are performed on firmware during warranty period, SUPPLIER shall upgrade the firmware of the supplied PLCs (whether installed or not) and provide assistance in order to guarantee that this upgrade will have no negative effects in CSS.

6.3 Communication Driver

6.3.1 The reading/writing of variables between Supervision and Operation System (Real Time Data Servers) and the PLCs shall be performed by a communication driver.

6.3.2 In order for the supervisory software to be able to recognize the data supplied by the communication driver, the PLC and the driver itself shall be configured in the supervisory software environment.

6.3.3 The data stored in the PLC database can be carried to Supervision and Operation System in 2 (two) ways, called real time data base updating modes: polled and/or unsolicited.

6.3.3.1 In polled mode, the supervisory software solicits the data to the PLC, which is then carried by the communication driver.

6.3.3.2 In unsolicited mode, the communication driver only updates the real time data base when an input point changes its value. Periodically, however, the supervisory software shall solicit all the values, in order to confirm the consistency between the Supervision and Operation System and the PLC databases.

6.3.3.3 The PLC shall support the use of OPC UA communication drivers.

6.3.3.4 More details about communication drivers are described I-ET-3010.00-5520-861-P4X-002 - SUPERVISION AND OPERATION SYSTEM – SOS.

7 HARDWARE REQUIREMENTS

7.1 CPU

7.1.1 The PLC Central Processing Unit (CPU) is responsible for running the application program. Microcomputers executing the application program (“SoftPLC” technology) or PLC emulators are not accepted.

7.1.2 CPU Operating Modes

7.1.2.1 The PLC shall have the following CPU Operating Modes:

- Running Mode: In this mode, the PLC executes the application program, not allowing any programming intervention. Means to protect the running mode from attempts to program the PLC shall be implemented, by hardware or software.
- Set up Mode: In this mode, the PLC executes the application program, but allows changes of the registers' contents.
- Programming Mode: In this mode, the application program can be altered by the program editor and downloaded to the PLC memory, but it shall not be executed.

7.1.3 Active/Standby Switchover

7.1.3.1 During normal operation, if the current active half-cluster is rejected in some critical test, the control of the common I/O shall automatically be transferred to the standby half-cluster (switchover). This switching shall be signed by a PLC status register and be alarmed at Supervision and Operation System HMIs.

7.1.3.2 Half-cluster switchover shall be “bumpless”, i.e., the application program shall continue its execution on the newly active CPU with no discontinuity in I/O reading/writing.

7.1.4 Memory Sizing

7.1.4.1 PLC SUPPLIER is responsible for the PLC sizing taking into account scan time, I/O addressing capability, I/O quantity and memory sizing.

7.1.4.2 As all data shall remain in the last value during power loss, 100% of the user program memory and tag data of the control modules shall be stored in non-volatile memory.

7.1.4.3 Control modules shall be capable of storing data during power loss. This capacity shall be sufficient to maintain that data for a minimum of 90 (ninety) days.

7.1.5 CPU Card Frontal

7.1.5.1 At least the following signaling shall be available on the CPU card frontal:

- LED for operational status;
- LED for diagnosis;
- LED for the communications channels;
- LED for I/O activity;
- Key for CPU operating modes selection (Running, Setup and Programming).

The implementation of these functions via software is also acceptable. In this case a physical key is not necessary.

7.1.5.2 Any one of the above status can be shown via one LED for each Status or as combination of on/blinking/off LEDs on the front panel.

7.1.6 CPU Tests and Diagnostic

7.1.6.1 The status of all half-cluster cards and of the I/O shall be available on system status registers. These registers shall be updated to the PLC external memory table and accessed by the program editor and application program and by Supervision and Operation System.

7.1.6.2 An independent mean for detecting the overall failure of the CPU shall be provided. In such an occurrence, the sound half-cluster shall acquire control of the common I/O, switching the faulty half-cluster to a standby condition, not relying on a hardware/software component under the influence domain of potentially faulty CPU.

7.1.6.3 Upon active-standby exchange (switchover), the communication driver shall switch automatically, reporting the occurrence and discriminating the new active cluster to the Supervisory Program.

7.1.6.4 The previously active half-cluster shall not spontaneously recover control, unless the current active (previous standby) is realized to be faulty, or commanded by the operator.

7.1.6.5 The diagnosis routine shall consist, for each half-cluster, of the following minimum checks:

- CPU watchdog timer;
- Application program memory parity;
- Operating system memory parity;
- I/O memory parity;
- Memory back-up battery discharged;
- Communications watchdog timer;
- Absence of I/O card in the position addressed by the application program;
- Power supply check-up;
- Enhanced power-up diagnosis.

7.1.6.6 On PLC power loss, the following requirements shall be met:

- System software shall be retained within CPUs;
- PLCs shall restart its normal functioning automatically;
- Any normal start-up diagnostic shall run;
- All sequences shall move to a predefined hold state;
- All mode switching shall progress to the control mode required by the application;
- All auto/manual switching elements and other key functions shall adopt a predefined mode (normally manual) as required for the application;
- All parameters settings shall return to their actual values, i.e., the ones originally configured in the PLC. The I/O values shall be switched to their safe state.

7.1.7 Access Levels

7.1.7.1 The PLC shall have, in the Setup mode, different levels of access, through the program editor, protected by password. The minimum levels shall be “read”, “force” and “change”.

7.2 Networking Communication

7.2.1 Ethernet TCP/IP communication links transfer rate protocol (Gigabit Ethernet, Fast Ethernet etc.) shall be according to project’s descriptive memorandum entitled AUTOMATION NETWORK DESCRIPTION.

7.2.2 Standby Update Channel

7.2.2.1 This is the tying element between the two half-clusters. This is achieved through a connection between the standby update channel with its active dual, and from thereof to the active CPU. Restraining the standby CPU from directly accessing the I/O network prevents a possibly unreliable component to seize the I/O Subsystem. The Standby Update Channel shall be done via a dedicated media

(different from the HSDN and other networks mentioned earlier), in order to keep total independence for this channel and redundancy.

7.2.2.2 The update channel shall be continuously monitored, in order to be ready in case of half-cluster switching.

7.2.2.3 The standby update channel shall be robust and fault tolerant, so that the redundant operation of the two half-clusters will not be impaired by a fault in this link.

7.2.2.4 If the channel is faulty, a critical alarm shall be displayed at Supervision and Operation System HMIs.

7.2.3 High Speed Deterministic Network (HSDN)

7.2.3.1 The High Speed Deterministic Network (HSDN) shall allow the attachment of various CPUs to the same communications media. Therefore, it is possible for a program running on a CPU to access data managed by a program running on any other CPU. The HSDN performs all the functions necessary to communicate across the network, leaving the CPU dedicated to the task of processing the Application Program. The High Speed Deterministic Network (HSDN) shall not be used to transmit interlock signals.

7.2.3.2 Each half-cluster is linked to a fully redundant HSDN, so that the same information is transferred simultaneously over both channels. If one channel fails, the communication shall not be lost. If both channels fail, the switching between the active and the standby half-clusters shall take place.

7.2.3.3 Management of the transmission shall not diminish the CPU scanning rate.

7.2.3.4 The communication card shall embody its own memory and processing capability. The buffer shall be sized to store the state and address of all I/O points.

7.2.3.5 For the HSDN, each half-cluster shall contain at least two communication cards (or more according to HSDN network topology) operating autonomously. The removal of one card or a fault in one HSDN shall not impair the operation of its dual.

7.2.3.6 The HSDN media shall interconnect the half-clusters of different clusters of the CSS Subsystems. The use of Ethernet in a deterministic configuration is acceptable.

7.2.3.7 Connectors and splicers shall be designed to stand for marine environment. The PLC documentation shall describe the cable/connectors specification and exhibit certificates complying with the environment conditions.

7.2.3.8 The transmission rate of the HSDN shall be at least 2 Mbps.

7.2.4 Minimum hardware capacity of each half-cluster

Memory (in Megabytes)	32.0
Maximum Scan time (in milliseconds)	**NOTE 1**
Real Time Clock	1
Standby Update (or redundancy modules)	2 (redundant)
HSDN interface	2 (redundant)
Ethernet-TCP/IP Interface for communication with the Supervision and Operation System	2 (redundant)
Ethernet-TCP/IP and / or USB Interface for programming functions	1
I/O Deterministic Communication Network (local and remote) Interfaces	2 (redundant)
Ethernet Modbus TCP Interface (electrical system network interface)	2 (redundant)
Ethernet Modbus TCP or Modbus RTU Interface (AFDS interface)	1 (redundant per installation, see item 7.2.8.1)
Minimum Remote I/O Subsystems	25
Minimum Discrete inputs	2,000
Minimum Discrete outputs	2,000
Minimum Analog inputs	1,000
Minimum Analog outputs	400

NOTE 1: Scan time shall be such as to meet the following processor cycle times:

- Fast control loops (typically pressure and flow): 0.5 second
- Slow control loops (typically temperature and level): 1 second
- Motor start/stop: 0.5 second
- Monitoring and alarming: 1 second
- Sequences: 1 second
- Critical trip functions: 0.5 second
- Trip functions: 1 second

7.2.5 Ethernet-TCP/IP Interface

7.2.5.1 This element allows each half-cluster to communicate with the Real Time Data Servers.

7.2.5.2 The Ethernet-TCP/IP Interface comprises its own processor for the whole protocol implementation, namely the lower layers of the IEEE 802.3. The Ethernet-TCP/IP Interface is also redundant; each half-cluster has its own interface, so the standby offers an alternative path for communicating with the Supervision and Operation System. If the active network fails, the standby half-cluster shall automatically assume the control.

7.2.5.3 The physical media for the Ethernet-TCP/IP Interface is shall be according to I-ET-3010.00-5520-800-P4X-004 - AUTOMATION NETWORK REQUIREMENTS.

7.2.5.4 Analogously to the HSDN, the Ethernet-TCP/IP protocol monitors abnormalities in the transmission media even when idling. Criterion shall be accorded for classifying the abnormality severity that shall trigger the active-standby switching.

7.2.5.5 An Ethernet-TCP/IP Interface may also be included on CPU card or on other cards for programming purpose.

7.2.6 I/O Deterministic Communication Network

7.2.6.1 In order to be shared by both half-clusters, the local I/O (when applicable) interconnects similarly to the cluster as the remote I/O, therefore, even allowing for manufacturing differences, it is assumed only one type of I/O Deterministic Communication Network, for both local and remote I/O Systems.

7.2.6.2 The I/O Deterministic Communication Network shall be fully redundant, so the data can be transferred over both active channels, with fault tolerance characteristics. If one component of the I/O channel fails, the occurrence shall generate an alarm at the Supervision and Operation System HMIs, but the I/O communication shall not be lost. No discontinuity shall be observed in I/O values during communication channel switchover. If both channels fail, the occurrence shall generate an alarm at the Supervision and Operation System HMIs and the related I/O System shall have all its output points set to a safe state (fail-safe status retraction) and all input values overridden in order to avoid multiple alarms and unnecessary control actions from a common cause failure. Once the communication is reestablished with at least one of the channels, all signals shall return to normal operating condition (overrides shall be removed).

7.2.6.3 Communication between PLC CPUs and PLC Remote I/O shall be done by optical fibers (outdoors) or by twisted pair (indoors), according to Project documents. In case of using optical fibers, independent electro-optical converter shall be used for each channel.

7.2.6.4 The distances involved in the interconnection between the CPUs and the Remote I/O panels may vary from 2 to 300 meters.

7.2.6.5 The transmission rate of the I/O Deterministic Communication Network shall be at least 2 Mbps.

7.2.6.6 Redundant cables shall be furnished and installed with proper connectors at both ends and routed through distinct paths.

7.2.6.7 The I/O Deterministic Communication Network status/diagnostic shall be available in system status registers, discriminating the evaluated channel.

7.2.6.8 Each half-cluster shall access both redundant I/O Deterministic Communication Networks independently of the status of the other redundant CPU.

7.2.6.9 The I/O Deterministic Communication Network scan time shall not be higher than the CPU scan time. If so, the bus shall be broken down into as many

busses as necessary in order to have a bus scan below the CPU scan time. It shall be stated in the proposal the I/O Deterministic Communication Network scan time for each bus (worst case and normal operation).

7.2.7 Communication Network with Electrical System

7.2.7.1 Each half-cluster shall have redundant communication port Ethernet Modbus TCP for communication with third party equipment (typically, Electrical System controllers). For more information, see I-ET-3010.00-5520-861-P4X-001 - CONTROL AND SAFETY SYSTEM – CSS.

7.2.7.2 This communication shall be done through other ports than those dedicated to PLC programming access.

7.2.8 Communication with the AFDS

7.2.8.1 Each half-cluster shall have one communication port (Ethernet Modbus TCP or RS-485 Modbus RTU) for communication with AFDS. The connection shall be as follows:

- FGS half cluster A communicates with Topsides AFDS half cluster A;
- FGS half cluster B communicates with Topsides AFDS half cluster B;
- HFGS half cluster A communicates with Hull AFDS half cluster A;
- HFGS half cluster B communicates with Hull AFDS half cluster B;

For more information see I-ET-3010.00-5522-855-P4X-001- ADDRESSABLE FIRE DETECTION SYSTEM and I-ET-3010.00-5520-861-P4X-001 - CONTROL AND SAFETY SYSTEM – CSS.

7.2.8.2 This communication shall be done through other ports than those dedicated to PLC programming access.

7.2.9 USB Interface

7.2.9.1 The USB port is optional. If the USB interface exists, it shall be located on the CPU card or on a specific card. It is through this port that the programming terminal is connected to the half-cluster, as an alternative to the Ethernet-TCP/IP Interface, for downloading the Application Program or for allowing the operator to intervene directly in the PLC operation. Analogously to the Ethernet-TCP/IP Interface, there shall be a driver for protocol management.

7.2.10 Synchronization

7.2.10.1 Each half-cluster CPU shall be able to receive SNTP communication protocol to perform synchronism.

7.3 Common Requirements for the I/O System

7.3.1 I/O modules of the system shall meet the following requirements:

- Accuracy: ± 0.1% of full scale;

- Resolution: 12 bits minimum;
- Linearity: ± 0.05% of full scale;
- Repeatability: 0.025%;
- Temperature effect: ± 0.5% per 25 °C change in the range 0 – 50 °C;
- Supply voltage effect: ± 0.2% for a ± 5% change in supply voltage;
- Common mode rejection: 120 dB minimum;
- Surge: I/O components shall meet ANSI/IEEE C 37.90.1 with respect to withstanding electrical surge such that no permanent damage occurs;

7.3.2 The fail-safe states for I/O cards shall be configurable on an individual basis as follows:

- Analog Inputs: 0%, 100% or last value;
- Analog outputs: 0%, 100% or last value;
- Discrete Inputs: 1, 0 or last value;
- Discrete outputs: 1, 0 or last value.

7.3.3 The I/O cards shall perform signal preconditioning from/to field devices. At least, PLC shall be able to address the following I/O signal types:

- Analog input 4 – 20 mA, system powered, 2-wires field transmitter (including temperature transmitter) with Hart protocol (AI Hart);
- Analog input 0 – 20 mA, field powered, 3-wires (24 VDC, common and signal) – signal range 0 – 4 mA used for diagnostics with Hart protocol (AI3 Hart);
- Analog input 0 – 20 mA, field powered, 4-wires (24 VDC, power supply input separate from the current loop) with Hart protocol (AI4 Hart);
- Analog input capable of reading resistor temperature detector (RTD) signals;
- Analog input capable of reading thermocouple signals;
- Analog output 4 – 20 mA, system powered with Hart protocol (AO Hart);
- Discrete input, DI 24 VDC;
- Discrete input with line monitoring (DIM);
- Discrete input capable of counting pulsed signals;
- Discrete output 24 VDC, system powered, load consumption 5 W maximum (**NOTE 1**) (DO);
- Discrete output 24 VDC with line monitoring (DOM);
- I/O cards for special signals (**NOTE 3**).

NOTE 1: All of these output terminals shall be equipped with fuses, located at their associated terminal strip. There shall be one fuse per channel.

NOTE 2: Field equipment shall be suitable for operation in hazardous area and have explosion proof certification. Use of I.S. equipment shall be restricted, submitted to PETROBRAS approval and conditioned to the use of galvanic isolation barrier. Signals out of 4-20 mA range are defined as fault signals and this shall be detected and indicated as bad quality/failure measurement.

NOTE 3: Signals that require an I/O card different from the ones listed shall be discussed with PETROBRAS. Discrete outputs with relays that receive

external voltage (DOR) shall not be used and will not be accepted by PETROBRAS.

7.3.4 Each channel of discrete I/O cards shall have individual short-circuit protection (fuses).

7.3.5 Cards shall be of plug-in type and shall have welded male connectors at the edges of the printed circuit, for connection with the rear bus and with the input/output terminals.

7.3.6 The contacting surface of the card connectors shall be gold coated. PLC MANUFACTURER shall certify the construction and coating technique of the plug-in connections.

7.3.7 The I/O racks/slots shall be standardized, for maximum interchangeability of cards and for storing the spare parts (i.e., the same rack shall be adequate for fitting various I/O card types).

7.3.8 The I/O cards shall have hot-swap capability, i.e., removal/insertion without requiring them to be previously de-energized and without carrying out any damage to the cards or to the PLC functioning. This intervention shall not impair the program running on the PLC, nor damage the cards.

7.3.9 Each I/O field connection terminal block shall fit, at the external side, up to two wires with minimum cross-sectional area of 1.5 mm^2.

7.3.10 Each I/O field connection terminal block shall be provided with a suitable space for affixing the field device identification and the I/O sequential number. Hanging badges and/or adhesive tape or similar means for identification are not acceptable.

7.3.11 The PLC shall be able to automatically identify when a new I/O card is inserted into an empty slot.

7.3.12 The I/O cards shall have reverse polarity protection.

7.4 Discrete Inputs

7.4.1 The following types of signals shall be handled: 24 VDC with inputs insulated from each other, sinking 2 mA; discrete input with line monitoring (DIM).

7.4.2 Cards shall have frontal LEDs, one for each input point, for field state indication.

7.4.3 Each input shall have individual insulation by optical coupling between the field interface and the internal circuit.

7.4.4 All Input channels shall be protected against voltage surges, 60 Hz interference and radio frequency interference.

7.4.5 The protection technique against over-voltage, under-voltage, inverted voltage and interference for the input circuits shall be clearly stated in the card's documentation.

7.4.6 The maximum level and duties for the above interference supported by the PLC shall be clearly stated. The PLC shall support them without false switching or damage of components.

7.4.7 Each discrete input card shall have, at maximum, 16 (sixteen) input channels. Other quantities shall be evaluated in Detail Engineering Design Phase based on the total power consumption, space inside panels and wiring design, and be subject to PETROBRAS approval.

7.4.8 For Monitored Discrete Inputs (DIM), the cards shall be compatible with monitored circuits. Circuits that require energy to be activated shall use such cards so that the loss of continuity is detected.

7.5 Analog Inputs

7.5.1 The analog input cards shall receive a 4 – 20 mA signal from the field transmitters.

7.5.2 Analog input cards shall always have HART capability. Exceptions may be made for the RTD and thermocouple AI cards.

7.5.3 Some field transmitters are energized from a power supply series connected with the PLC analog points (two-wire transmitters). Analog input cards shall permit use with 2, 3, and 4-wire input sensor field devices in the same card. Different analog input cards proper for each wire configuration (2-wire, 3-wire or 4-wire) are not allowed.

7.5.4 Each input point shall feature independent zero/span adjustment.

7.5.5 Each card shall have, at maximum, 8 (eight) inputs. Other quantities shall be evaluated in Detail Engineering Design Phase based on the total power consumption, space inside panels and wiring design, and be subject to PETROBRAS approval.

7.5.6 For all analog input cards, it shall be possible to configure the A/D conversion range in order to prevent overflow and/or internal failure due to current signals greater than 20 mA.

7.6 Discrete Outputs

7.6.1 The following types of loads shall be handled: discrete output 24 VDC, system powered, power consumption 5 W maximum (DO); discrete output 24 VDC with line monitoring (DOM). Both cards shall supply 24 VDC when active and 0 VDC otherwise.

7.6.2 Each card shall have, at maximum, 16 (sixteen) outputs. The card shall have capacity to drive, simultaneously, all the outputs at their maximum current. Other quantities shall be evaluated in Detail Engineering Design Phase based on the

total power consumption, space inside panels and wiring design, and be subject to PETROBRAS approval.

7.6.3 Each output channel shall have individual protection for short-circuit.

7.6.4 Cards shall have frontal LEDs to indicate the state of each output point.

7.6.5 The logic signals and the driving signals shall be separated by optical or magnetic isolation for each output point.

7.6.6 Discrete output modules shall have the feature of fuse protection and blow fuse diagnostics.

7.6.7 For the actuation of the solenoids of the CO_2 suppression systems, each discrete output shall be compatible with the corresponding solenoid consumption. External relays shall not be used for interlocking.

7.6.8 For Monitored Discrete Outputs (DOM), the cards shall be compatible with monitored circuits. Circuits that supply energy to be activated shall use such cards, so that the loss of continuity is detected.

7.7 Analog Outputs

7.7.1 The analog output point shall drive line impedances from 15 Ω to 600 Ω @24 VDC.

7.7.2 Analog output cards shall always have HART capability.

7.7.3 The control circuit and the drive circuit shall be separated by magnetic/optic insulation.

7.7.4 Each output point shall feature independent zero/span adjustment.

7.7.5 Each card shall have, at maximum, 8 (eight) outputs. Other quantities shall be evaluated in Detail Engineering Design Phase based on the total power consumption, space inside panels and wiring design, and be subject to PETROBRAS approval.

7.8 Racks for Circuit Cards

7.8.1 Every I/O rack shall be provided with 2 (two) power supplies (hot standby). Under normal conditions, each of their power supplies shall be operating at a maximum of 85% of its nominal capacity. Special attention shall be given so that the redundant power sources will not be connected improperly in parallel.

7.8.2 Each slot shall have borders or guides for conducting the insertion of the card and be docked.

7.8.3 Each slot shall allow easy identification of the inserted card.

7.8.4 Besides the fans installed on the panel walls, the racks that hold high thermal dissipation cards shall be outfitted with their own fans.

7.9 Power Supply Requirements

7.9.1 The PLC power supply shall withstand the following input voltage range:

- 24 VDC +10 % or -15 % on a continuous basis;
- 24 VDC ± 20 % for 10 seconds;
- 24 VDC ± 100 % for 10 milliseconds.

7.9.2 In case of power failure, all programs loaded onto the PLC memory shall be preserved.

7.9.3 The actuation of the protection devices on the power supply of an active PLC half-cluster shall trigger the active/standby switching.

7.9.4 A "hold last state" feature is required, to be accessed by means of program, holding the last state attained by the power supply before the failure.

7.9.5 The Operating System (firmware) shall be insensitive to power failures.

7.9.6 The power supply shall feature over-voltage, under-voltage and over-current protection.

7.9.7 The wiring between the power supplies, CPUs, local cards and remote cards shall be of plug-in type, without splicing.

7.10.8 PLC SUPPLIER shall report the total power consumption per PLC subcomponent.

7.10 Environmental Protection of Circuit Cards

7.10.1 The circuit cards and accessories shall withstand the operation environment mentioned in 3.1, without impairing their performance.

7.10.2 For the achievement of such ruggedness, the cards shall be protected with a special varnish film, suitable for offshore industrial environment.

7.10.3 Besides the coating of the cards, the varnish is also to be furnished separately, in adequate quantity, for maintenance purposes.

7.11 Electromagnetic Interference and Radio-Frequency Immunity Requirements

7.11.1 PLC SUPPLIER shall report the basic requirements for proper installation of the communications cables, in order to minimize EMI/RFI.

7.11.2 For EMI, PLC shall comply with the standards series IEC 61000-4.

7.11.3 The above compliance shall be assured for the overall system, including the CPUs, embracing the Standby Update Channels, power supplies, all network cards, Local/Remote I/O Systems, loop/line monitors, I/O test circuits, etc.

7.12 If any of the supplied hardware becomes obsolete during warranty period, it shall be replaced and installed and tested without any additional cost to PETROBRAS. After warranty period SUPPLIER shall keep PETROBRAS informed if any of the supplied hardware becomes obsolete.

8 SOFTWARE REQUIREMENTS

8.1 Program Editor

8.1.1 The program editor shall be delivered properly licensed to PETROBRAS, complete with manuals, in dedicated media and installed in the hard drive/SSD of the maintenance computer or notebook.

8.1.2 The program editor shall accept Brazilian Portuguese language characters, along with extended ASCII Set. These Portuguese characters are intended to be used in the comments added to the application program source code.

8.1.3 The program editor software shall allow its installation of at least four licenses in different computers.

8.2 Editing Tools

8.2.1 The following minimum facilities for editing the application program are required:

- Source and compiled files management, as read, write, merge, etc.;
- Application program source files printing in graphic form, providing a readable list of the program;
- The printing output shall reproduce the screen presentation;
- Use of Windows® environment, in order to speed up the program development;
- At least Ladder-type and Function block diagram representations for input and output variables, respectively contact and coil symbols. In case of analog points, an alternative representation shall be provided;
- Capability of generating routines/sub-routines for repetitive tasks;
- Pre-configured control blocks, at least PID, including action mode (direct / reverse), and output fail mode (open / close);
- Functional type representation for advanced instructions such as arithmetic operations, string handling, register/table movements, masking, and AND/OR logics over register bits. The instructions shall be represented in a detachable form, namely encapsulated in rectangles, wherein the required arguments shall be indicated;
- Each functional type instruction shall have at least two external binding posts, one for triggering the instruction and the other for confirmation of instruction activation. The latter allows propagation of instruction activation, by chaining the binding posts of the functions;
- Conventional text editor facilities for cursor positioning anywhere in the loaded file, such as one character forward/backward skipping, one line up/down, page up/down, beginning/end of file, etc.;
- Character deleting;

- Facilities for identifying and accessing sequences of instructions, including the particular case of a single instruction;
- Facilities for copying, moving and deleting a specified sequence of instructions;
- Consistency analysis of syntax statements;
- Facilities for debugging the application program;
- Instantaneous PLC memory availability, by automatic estimation of the already edited program needs, in compiled code;
- Command for comparing two application programs, one in programmer station another in CPU PLC or both program stations;
- Command for replacing an address by another address in a specific subroutine or in optional way in whole program in the automatic option;
- Facilities for appending comments, in Brazilian Portuguese Language statements, near I/O points (tag identification) and related to instructions or sequence of instructions;
- Assignment of the PLC model, rack allocation, I/O Systems, network nodes and all the information necessary to perform a thorough configuration of the PLC hardware;
- Compile/Link facilities, yielding machine code ready to drive the PLC;
- Download facility for transferring the machine readable code to the target PLC;
- Starting, stopping, monitoring and step execution of the downloaded program;
- Program changes and downloading while PLC is running;
- Register content modification while PLC is running;
- PLC emulator module for testing/development of the application program;
- Change management and version control tools;
- Databases shall be imported/exported at least in the following file extensions: CSV or XSL/XSLX;
- Logic shall be imported/ exported in ate least in the following file extensions: TXT or XML.

8.3 Functions and Data Types

8.3.1 At least the following programming facilities are also required:

- Flexible forms of addressing, in addition to the absolute address formulation, namely indirect, indexed and/or base addressing;
- Alternative means for designating a physical address, such as string association;
- Acceptance of various number formats (binary, octal, hexadecimal, decimal integer, floating point, negative and 2's complement);
- Arithmetic functions: ADD, MUL, SUB, DIV, etc.;
- Bitwise Boolean functions: AND, OR, XOR, NOT;
- Counting functions: UP/DOWN COUNTER;
- Transition sensing contacts;
- Latched coils: set/reset pairs;
- Retentive coils: corresponding Boolean variables are retained upon power supply failure;
- External variable accessing: special network instructions to allow a program running on a PLC to access data managed by a program running on another PLC, both interconnected through the same HSDN;

- Ethernet-TCP/IP accessing instructions for Supervision and Operation System communications;
- Count timer;
- Capability of sending diagnosis status to an external memory map, accessible by the Supervision and Operation System.

8.4 Communication Driver

8.4.1 Changes in the PLC database shall update the Supervision and Operation System.

8.4.2 Changes in the Supervision and Operation System, as a result of operator intervention or triggered by user programs, shall update the related field actuator devices.

8.4.3 The address of each point in the PLCs database shall be identified and related to an indirect addressing scheme (variable name) provided by the tools for editing and linking the PLC Real Time Data Base.

8.4.4 Each PLC half-cluster shall have its respective OPC UA communication driver, and this shall be supplied in conjunction with the PLC. The OPC UA driver shall be installed in the Supervision and Operation System server or embedded in the corresponding CPU firmware.

8.4.5 The PLC MANUFACTURER shall report to the communication driver developer all information needed for the development of the communication driver.

8.4.6 The communication driver shall support the following modes: polled and/or unsolicited.

8.4.7 The communication driver shall carry out appropriate actions in the event of a communication failure. This feature shall be provided at both sides of the link, in order to avoid PLC waiting indefinitely for Supervision and Operation System and vice versa.

8.4.8 The communication driver shall allow the configuration of the Ethernet Protocol parameters (half-cluster node, physical/logical port name, speed, etc.).

8.4.9 The configuration process shall be carried out at Supervision and Operation System side. It may be necessary, however, to configure some of these parameters at PLC side as well.

8.5 If any of the supplied software becomes obsolete during warranty period, it shall be replaced by SUPPLIER without any additional cost to PETROBRAS. After warranty period SUPPLIER shall keep PETROBRAS informed if any of the supplied software becomes obsolete.

9 ACCEPTANCE TESTS

9.1 Since PLC is part of the UNIT's CSS and is supplied installed in an automation panel, acceptance tests (FAT, SAT and SIT) shall be according to I-ET-3010.00-5520-888-P4X-001 - AUTOMATION PANELS and I-ET-3010.00-5520-861-P4X-001 - CONTROL AND SAFETY SYSTEM - CSS.

9.2 All deviations and anomalies found during Factory Acceptance Test (FAT), Site Acceptance Test (SAT) and Site Integration Test (SIT) shall be adequately registered according to the punch list defined in contract.

9.3 The acceptance tests shall be according to IEC-62381 – AUTOMATION SYSTEMS IN THE PROCESS INDUSTRY – FACTORY ACCEPTANCE TEST (FAT), SITE ACCEPTANCE TEST (SAT) AND SITE INTEGRATION TEST (SIT).

9.4 Detailed FAT, SAT and SIT proceedings shall be submitted to PETROBRAS for approval according to the informed schedule.

10 PACKING REQUIREMENTS

10.1 On completion of FAT, all equipment shall be prepared for shipment and storage.

10.2 Equipment supplied loose shall be packed and crated for transportation. In addition, if some rack equipment is susceptible to transportation damage, it shall be removed from the system rack for separate packing and crating.

10.3 In order to prevent corrosion, VCI shall be used adequately, where applicable, as part of preparation for shipment and storage instead of desiccants such as silica gel. The latter shall be used only in cases where VCI is not applicable. Both VCI and desiccants shall not be used together for protecting the same compartment.