PETROBRAS	**TECHNICAL SPECIFICATION**	Nº: I-ET-3010.00-5520-862-P4X-001	
	CLIENT:	SHEET 1 of 25	
	JOB:	--	
	AREA:		
DP&T-SUP	TITLE: **PROGRAMMABLE LOGIC CONTROLLERS - PLC**	NP-1	
		ESUP	

MICROSOFT WORD / V. 2013 / I-ET-3010.00-5520-862-P4X-001_0.DOCX

INDEX OF REVISIONS

REV.	DESCRIPTION AND/OR REVISED SHEETS
0	ORIGINAL ISSUE

	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G	REV. H
DATE	SEPT/19/18								
DESIGN	ESUP								
EXECUTION	CAMILA								
CHECK	GNIEDU								
APPROVAL	PEDRO								

SUMMARY

1 INTRODUCTION

1.1 Object

1.1.1 This Technical Specification describes the minimum requirements and basic characteristics for the Programmable Logic Controllers (PLCs), part of the Control and Safety System (CSS) of the Floating Production Unit (FPU).

1.1.2 This specification deals mainly with CSS PLCs and Remote I/Os.

1.2 Definitions

UNIT	FPSO (Floating, Production, Storage and Offloading), FSO (Floating, Storage and Offloading), SS (Semi-Submersible) or Fixed Offshore Unit.
PACKAGED UNIT	An assembly of equipment supplied interconnected, tested and operating, requiring only the available utilities from the UNIT for the operation of the PACKAGED UNIT.
PURCHASER	The Company designated as such in the Contract or the Purchase Order.
MANUFACTURER	The responsible for fabrication of equipment
VENDOR	System or equipment supplier.

1.3 Abbreviations

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	OLE for Process Control Unified Architecture
PID	Proportional–Integral–Derivative Controller
PLC	Programmable Logic Controller
RTDS	Real Time Data Server
VCI	Volatile Corrosion Inhibitors

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	60079	ELECTRICAL APPARATUS FOR EXPLOSIVE GAS ATMOSPHERES – ALL PARTS
IEC	60092-504	ELECTRICAL INSTALLATIONS IN SHIPS - PART 504: SPECIAL FEATURES - CONTROL AND INSTRUMENTATION
IEC	60529	DEGREES OF PROTECTION PROVIDED BY ENCLOSURES (IP CODE)
IEC	60533	ELECTRICAL AND ELECTRONIC INSTALLATIONS IN SHIPS - ELECTROMAGNETIC COMPATIBILITY
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 LOGIC 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	STANDARD FOR INFORMATION TECHNOLOGY, TELECOMMUNICATION AND INFORMATION EXCHANGE BETWEEN SYSTEMS
ANSI/IEEE	C 37.90.1	SURGE WITHSTAND CAPABILITY (SWC) TESTS FOR PROTECTIVE RELAYS AND RELAY SYSTEM

NFPA - NATIONAL FIRE PROTECTION ASSOCIATION

NFPA	496	STANDARD FOR PURGED AND PRESSURIZED ENCLOSURES FOR ELECTRICAL EQUIPMENT

2.1.2 Brazilian Codes and Standards

INMETRO - INSTITUTO NACIONAL DE METROLOGIA, NORMALIZAÇÃO E QUALIDADE INDUSTRIAL

PORTARIA Nº 179 (18/MAIO/2010)	REGULAMENTO DE AVALIAÇÃO DA CONFORMIDADE DE EQUIPAMENTOS ELÉTRICOS PARA ATMOSFERAS POTENCIALMENTE EXPLOSIVAS, NAS CONDIÇÕES DE GASES E VAPORES INFLAMÁVEIS E POEIRAS COMBUSTÍVEIS
PORTARIA Nº 89 (23/FEVEREIRO/2012)	ALTERAÇÃO DA PORTARIA INMETRO Nº 179, DE 18/MAIO/2010.

MTE – MINISTÉRIO DE TRABALHO E EMPREGO

NR	10	SEGURANÇA EM INSTALAÇÕES E SERVIÇOS EM ELETRICIDADE
NR	17	ERGONOMIA
NR	26	SINALIZAÇÃO DE SEGURANÇA
NR	30	ANEXO II – PLATAFORMAS E INSTALAÇÕES DE APOIO

2.1.3 Classification Society

2.1.3.1 The DETAIL DESIGN PHASE shall be submitted to approval by Classification Society. The design and installation shall take into account their requirements and comments.

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

2.2 Internal References

2.2.1 Project Documents

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	CSS/SOS PANELS
I-ET-3010.00-1200-800-P4X-002	AUTOMATION, CONTROL AND INSTRUMENTATION ON PACKAGED UNITS
I-ET-3010.00-5522-855-P4X-001	ADDRESSABLE FIRE DETECTION SYSTEM – AFDS

2.2.2 PETROBRAS Reference Documents

DR-ENGP-M-I-1.3	ENGENHARIA DE SEGURANÇA
DR-ENGP-M-I-1.5	CRITERIOS GERAIS PARA PROJETO DE INSTRUMENTAÇÃO

2.3 Any discrepancy observed by VENDOR between specification documents shall be informed to PURCHASER. VENDOR shall not proceed with any such aspect of the work until receiving an answer from the PURCHASER on how to proceed.

2.4 PURCHASER is responsible for ensuring that the product was received according to documentation supplied by VENDOR and specified by PETROBRAS. VENDOR is responsible for correcting any documentation according to supplied product in case of discrepancies.

2.5 Brazilian regulation (MTE section) and INMETRO regulation superpose all codes and regulations listed in item 2.2, since they are enforced by Brazilian law.

3 ENVIRONMENTAL AND OPERATIONAL CONDITIONS

3.1 For operational and environmental conditions additional to this section see specific project documentation.

3.2 Equipment shall be suitable to withstand the dynamic loads imposed by the vessel motions during tow and on location.

3.3 The available power supply is 220 VAC (HOLD) as defined in I-ET-3010.00-5140-700-P4X-003 – ELECTRICAL REQUIREMENTS FOR PACKAGES FOR OFFSHORE UNITS. VENDOR shall convert and distribute the different power supplies inside the panel, including where necessary power supply unit for the cabinet

internal distribution of 24 VDC. For further details, see I-ET-3010.00-5520-888-P4X-001 – CSS/SOS PANELS.

3.4 All panels, materials and equipment proper to be used in hazardous areas, shall have conformity certificates complying with "*PORTARIA INMETRO Nº 179, de 18/maio/2010*", and its annexes, changed by "*PORTARIA INMETRO Nº 89, de 23/fevereiro/2012*" and its annexes, and shall be approved by Classification Society.

3.5 All electrical and electronic devices, beyond mechanical parts of the equipment, shall be designed and constructed in a tropicalized version. Tropicalization process comprises application of reinforced protective resin Class 2 according to IEC 61086 and fungus proof according to ASTM G21 in all printed circuit boards, use of anti-rust materials and accessories and other implementations according to MANUFACTURERS' experiences and related rules, aiming to provide a robust and reliable construction.

4 COMPONENT DESCRIPTION OVERVIEW

4.1 General Description

4.1.1 The following items present the major 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.

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 PACKAGED 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 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 must meet the local content requirements.

4.1.4 All CSS Programmable Logic Controllers shall be of the same MANUFACTURER, brand and model, run the same firmware version and be supplied by the same VENDOR.

4.2 Hardware

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

.

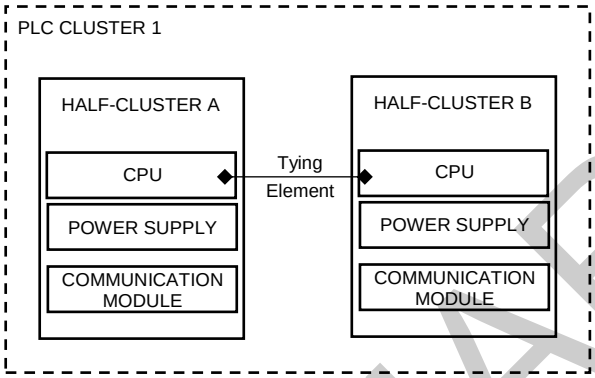

Figure 1 – PLC cluster and its half-clusters in hot standby.

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 7.2.2. For a detailed description of the HSDN, see I-ET-3010.00-5520-861-P4X-001 - CONTROL AND SAFETY SYSTEM – CSS and the automation architecture drawing specific to the project.

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

4.2.4 Gigabit Ethernet TCP/IP Interfaces: four (04) for each PLC cluster. These interfaces shall be used for communications between Real Time Data Server (RTDS) and all PLCs. Each two Gigabit Ethernet -TCP/IP Interfaces shall be mounted in different racks, one in the main PLC rack and the other one in the hot standby PLC rack in order to comply with the redundant topology.

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

4.2.6 Modbus TCP interfaces, two for each half-cluster for redundant communication with the Electrical System Gateway and two more per half-cluster for communication with the AFDS (for more information see I-ET-3010.00-5522-855-P4X-001 - ADDRESSABLE FIRE DETECTION SYSTEM - AFDS).

4.2.7 The following components shall have diagnostics capability: all I/O cards, communication modules, CPUs and power supplies.

4.3 Software

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

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 of I/O racks. Whatever the number of CPU racks (one or two); the cluster connects to a single I/O subsystem. The clusters comprising 2 (two) CPU Racks are kept synchronized through a tying element (see Figure 1). Failure of any of these components or the communication 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, namely the CPU, the power supply and the communications subsystem.

5.2.2 The term "CPU" is reserved, in this Specification, for the PLC element responsible for running the Application Program. The power supply group is also regarded as being constituted by a single element.

5.2.3 The communications subsystem is constituted by the Standby Update Channel (tying element), the High Speed Deterministic Network (HSDN), the Gigabit Ethernet-TCP/IP Interface, the USB-C interface (if used) and the I/O Deterministic Communication Network. Each of these elements, as well as the CPU and the power supply, are assigned in the half-cluster rack, on the Automation and Control Architecture.

5.2.4 Half-Cluster Operation

5.2.4.1 In the standby operation both half-clusters 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 be alarmed at Supervision and Operation System HMIs.

5.2.4.2 The half-cluster operating in hot standby must not have the data on its I/O addresses updated by reading the data from the I/O addresses of the other half-cluster (accessing through the standby update channel, for example). The data update between active and standby CPUs shall be done by a uniquely redundant network.

6 SOFTWARE STRUCTURE

6.1 Program Editor and Application Program

6.1.1 The PLC shall provide means to be configured and programmed. Software, referred to as the program editor, running on a PC or notebook, shall allow the user to both configure the PLC hardware and develop the application program. The program editor software shall run on latest Windows® operating system approved by PETROBRAS, 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 language used 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 Gigabit Ethernet-TCP/IP interface and/or via USB-C port (whichever port is available on the PLC for programming functions).

6.2 Firmware

6.2.1 The firmware shall be furnished on the latest version available on date of supply. If major updates are performed on firmware during warranty period, VENDOR 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 on the 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. Due to the large number of points gathered by the PLC systems, it is advisable to maximize the configuration in the unsolicited mode. 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 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 shall not be 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 run.

7.1.3 Active/Standby Switching

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. This switching shall be signed by a PLC status register and be alarmed at Supervision and Operation System HMIs.

7.1.4 Memory Sizing

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

7.1.4.2 100 % of the memory shall be of retentive type.

7.1.4.3 Control modules shall be capable (such as battery backup) to store 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 **Minimum** Hardware Capacity of each Half-Cluster

Memory (in Megabytes)	1.0
Maximum Scan time (in milliseconds)	**NOTE 1**
Real Time Clock	1
Standby Update	1
HSDN interface	2 (redundant)
Gigabit Ethernet-TCP/IP Interface for communication with the Supervision and Operation System	2
Gigabit Ethernet-TCP/IP and / or USB-C Interface for programming functions	2
I/O Deterministic Communication Network (local and remote) Interfaces	2 (redundant)
Modbus TCP Interface (AFDS and electrical system gateway)	4
Minimum Remote I/O Subsystems	25
Minimum Discrete inputs and outputs	4,096
Minimum Analog inputs	1,000
Minimum Analog outputs	400

NOTE 1: Scan time shall be as such 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

7.1.7 CPU Tests and Diagnostic

7.1.7.1 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.

7.1.7.2 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.

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

7.1.7.4 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.

7.1.7.5 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.

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

- System software 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.

7.1.8 Access Levels

7.1.8.1 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 Standby Update Channel

7.2.1.1 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.

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

7.2.1.3 The standby update channel must 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.

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

7.2.2 High Speed Deterministic Network (HSDN)

7.2.2.1 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.

7.2.2.2 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. The time interval to determine network failure shall be according to project's AUTOMATION NETWORK REQUIREMENTS documentation.

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

7.2.2.4 The communications 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.

7.2.2.5 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.

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

7.2.2.7 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 Gigabit Ethernet-TCP/IP Interface

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

7.2.3.2 The Gigabit Ethernet-TCP/IP Interface comprises its own processor for the whole protocol implementation, namely the lower layers of the IEEE 802.3. The Gigabit Ethernet-TCP/IP Interface is also redundant, each 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 cluster shall automatically assume the control.

7.2.3.3 The physical media for the Gigabit Ethernet-TCP/IP Interface is the unshielded twisted pair (IEEE 802.3z) in enclosed rooms and optical fiber in the field.

7.2.3.4 Analogously to the HSDN, the Gigabit 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.

7.2.4 I/O Deterministic Communication Network

7.2.4.1 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.

7.2.4.2 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. 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. Once the communication is reestablished with at least one of the channels, all signals shall return to normal operating condition (overrides shall be removed).

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

7.2.4.4 The distances involved in the interconnection between the clusters and remote I/O panels range from 2 to 250 m.

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

7.2.4.6 Redundant cables shall be furnished and installed with proper connectors at both ends. The PLC documentation shall address explicitly this issue.

7.2.4.7 The I/O Deterministic Communication Network shall be tested continuously according to project's AUTOMATION NETWORK REQUIREMENTS documentation. The diagnosis of the tests shall be available on system status registers, discriminating the evaluated channel.

7.2.4.8 Remote I/O total communications failure shall carry the outputs to the safest state. Accordingly, the Remote I/O cards shall have some intelligent logic to energize / de-energize the required outputs in case of total communications failure. On the PLC side, the inputs updated through the faulty communications network shall evolve to the highest shutdown attained levels.

7.2.4.9 Upon communications return, the application program shall be notified, for displaying a message at Supervision and Operation System HMIs.

7.2.4.10 Each half-cluster shall access both I/O redundant deterministic communication networks independently of the status of the other redundant CPU.

7.2.4.11 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. PURCHASER shall state in the proposal the I/O Deterministic Communication Network scan time for each bus (worst case and normal operation).

7.2.5 Communication Network with Electrical System

7.2.5.1 Each half-cluster shall have redundant communication (Modbus TCP) with the Electrical System Gateway (i.e. one connection to gateway A and one connection to gateway B per half-cluster).

7.2.5.2 This communication may not be done through the ports dedicated to the PLC programming functions.

7.2.6 USB-C Interface

7.2.6.1 The USB-C port is 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 of the Gigabit Ethernet-TCP/IP Interface, for downloading the Application Program or for allowing the operator to intervene directly in the PLC operation. Analogously to the Gigabit Ethernet-TCP/IP Interface, there is a "driver" for protocol management.

7.2.7 Synchronization

7.2.7.1 The CSS CPUs clock shall be able to receive a SNTP communication protocol to guarantee 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 or 0 or last value;
- Discrete outputs: 1 or 0 or last value.

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

- 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 (AI3) with Hart protocol (AI3 Hart);
- Analog input 0 - 20 mA, field powered, 4-wires (24 VDC, power supply input separate from the current loop) (AI4) with Hart protocol (AI3 Hart);
- Analog output 4 - 20 mA, system powered with Hart protocol (AO Hart);
- Discrete input, DI 24 VDC;
- Discrete input with line monitoring (DIM);
- Discrete output 24 VDC, system powered, load consumption 5 W maximum (**NOTE 1**) (DO);
- Discrete output 24 VDC with line monitoring (DOM).

NOTE 1: These output terminals shall be equipped with fuses, located at their associated terminal strip.

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 beyond 4-20 mA range are defined as fault signals and this shall be detected and indicated by the CSS as bad quality measurement.

7.3.4 I/O cards for discrete signals shall have individual card protection for short-circuit.

7.3.5 Cards shall be of plug-in type and shall have welded male connectors on 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 hot-swap of the I/O cards (removal/insertion without requiring them to be previously deenergized and without carrying out any damage to the cards or to the PLC functioning) shall be possible. 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, on 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 I/O System shall be balanced, i.e. one bus shall not contain many analog cards while another bus contains only I/O cards for discrete signals in the same system.

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 It is required insulation by optical coupling between the field interface and the internal circuits for each input.

7.4.4 Inputs points 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 card shall have, at maximum, 16 (sixteen) inputs.

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

7.5 Analog Inputs

7.5.1 The analog input cards receive a 4 - 20 mA signal from the field transmitters. Some field transmitters are smart type, meaning that they are able to inform the status related to their operation and use the range 0 – 4 mA to inform diagnosis. The range of the analog input cards shall be configured to 0 - 20 mA or 4 - 20 mA.

7.5.2 Analog input cards shall always have HART capability.

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.

7.6 Discrete Outputs

7.6.1 The following types of loads shall be handled: discrete output 24 VDC, system powered, load 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 maximum current each.

7.6.3 Each output point 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, the outputs shall be compatible with their 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 must 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 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.

7.8 Racks for Circuit Cards

7.8.1 Every I/O rack shall be provided with 2 (two) power supplies (hot standby). Under nominal 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 VENDOR 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 unlimitedly the environment, 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 production unit 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 The VENDOR shall report the basic requirements for proper installation of the communications cables, in order to minimize EMI/RFI.

7.11.2 For EMI, in general, the 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 clusters (embracing the Update Channel), HSDN, Gigabit Ethernet-TCP/IP Interface (embracing the Communications Driver), USB-C Interface, when used, (embracing the Communications Driver), I/O Deterministic Communication Network HART Communication, Local/Remote I/O Systems, loop/line monitors, I/O test circuits, etc.

8 SOFTWARE REQUIREMENTS

8.1 Program Editor

8.1.1 The program editor shall be delivered in DVD or USB flash drive (preferably) media installed in the hard disk of the programming terminal.

8.1.2 The program editor shall accept Portuguese language accented characters, complied with the 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 DVD or USB flash drive (preferably) shall allow the installation of at least four licenses in the hard disk of different programming terminals.

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;
- Intensive use of the Windows® environment, in order to speed up the program development;
- Ladder-type or Function block representation for input and output variables, respectively contact and coil symbols. In the case of analog points, an alternative representation shall be provided;
- Ladder-type or Function block representation for discrete input variables assignments, namely a coil driven by a logical concatenation of contacts shall be represented by just drawing a line between the contacts group and the associated coil;
- Capability of generating encapsulated routines for repetitive tasks;
- Pre-configured PID control block, 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 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 realize 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 alteration while PLC is running;
- PLC emulator module for testing/development of the application program.

8.3 Functions and Data Types

8.3.1 The following minimum facilities for translating the functional requirements to a structured application program are required:

- Some flexible forms of addressing, in addition to the absolute address formulation, namely indirect, indexed and/or base addressing;
- Alternative means for designating an address, such as string association, etc.;
- Acceptance of various number formats, namely binary, octal, hex, 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 variables 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;
- USB-C ports accessing: instructions for outputting/inputting data through the USB-C ports;
- Gigabit Ethernet-TCP/IP accessing instructions for Supervision and Operation System communications.

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 with the indirect addressing scheme (variable name) provided by the tools for editing and linking the CSS 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. OPC-UA driver shall be installed on the Supervision and Operation System server.

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 the appropriate actions on the event of communications failure. This feature shall be provided on both sides of the link, so as to avoid the PLC waiting indefinitely for Supervision and Operation System or vice versa.

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

9 DOCUMENTATION

9.1 Complete documentation of the PLC, covering all devices and services, shall be supplied with the proposal, for approval, and for final acceptance.

9.2 There shall be supplied with the proposal, in the number of copies defined at PURCHASER documents, at least the following technical documents, where applicable:

- Technical specifications, comprising: system, equipment, accessories, cables, materials and software;
- Datasheets and brochures for each equipment;
- All equipment and installation data including: material list, equipment list, spare part list, power consumption, weight, software manual, panel layout, system layout, etc.;
- Complete description of services, training courses, tests, etc.

9.3 There shall be supplied for approval, in the number of copies defined at PURCHASER documents, at least the following technical documents, where applicable:

- Technical specifications, comprising: system, equipment, accessories, cables, materials and software;
- Datasheets and drawings for each equipment;
- Installation drawings including general arrangement, electrical diagrams, wiring diagrams, cable list, material list and equipment list;
- Test procedures, training course program and services schedule;
- Programming tools, system reports, system diagnosis, etc.;
- Source version for all application programs with comments.

9.4 Complete PLC documentation, including operation manual, installation manual and maintenance manual shall be provided, in the number of DVD or USB flash drive (preferably) copies requested at PURCHASER documents, including all programming and configurations software.

10 ACCEPTANCE TESTS

10.1 For Acceptance Tests, refer to I-ET-3010.00-5520-888-P4X-001 – CSS/SOS PANELS.

11 TRAINING

11.1 For PLCs Training, refer to contractual terms.

12 WARRANTY

12.1 VENDOR shall give warranty for all components, even for equipment or device furnished by others, up to 24 (twenty four) months from delivery or for 12 (twelve) month operation.

12.2 This warranty shall cover fabrication or installation problems, as well as any service included in the scope of supply.

12.3 VENDOR shall warranty the supply of spare parts, at least, for up to 10 (ten) years after the date of the acceptance tests, and technical assistance at installation site performed by qualified maintenance staff, when requested.

12.4 During warranty period, any defective part shall be changed for a new one, within one week after the problem report by PURCHASER.

13 PACKING REQUIREMENTS

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

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

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