| | | | |
|---|---|---|---|
| PETROBRAS | **TECHNICAL SPECIFICATION** | Nº | I-ET-3010.00-5520-861-P4X-001 |
| | CLIENT: | SHEET | 1 of 38 |
| | JOB: | | -- |
| | AREA: | | |
| SRGE | TITLE: **CONTROL AND SAFETY SYSTEM - CSS** | | INTERNAL |
| | | | ESUP |

**MICROSOFT WORD / V. 2016 / I-ET-3010.00-5520-861-P4X-001_M.DOCX**

## INDEX OF REVISIONS

| REV. | DESCRIPTION AND/OR REVISED SHEETS |
|---|---|
| 0 | ORIGINAL ISSUE |
| A | GENERAL REVISION |
| B | REVISED WHERE INDICATED |
| C | REVISED WHERE INDICATED ACCORDING TO CONSISTENCY ANALYSIS |
| D | ITEM 4.1.13 REVISED ACCORDING TO CLARIFICATION NOTICE DUE TO BIDDERS QUESTIONS |
| E | ITEM 4.1.11 REVISED ACCORDING TO CLARIFICATION NOTICE DUE TO BIDDERS QUESTIONS |
| F | ITEM 8.2.3 REVISED ACCORDING TO CLARIFICATION NOTICE DUE TO BIDDERS QUESTIONS |
| G | REVISED WHERE INDICATED |
| H | REVISED WHERE INDICATED |
| J | REVISED WHERE INDICATED |
| K | REVISED WHERE INDICATED |
| L | REVISED WHERE INDICATED |
| M | REVISED WHERE INDICATED, INCLUDING CONSISTENCY ANALYSIS |

| | REV. 0 | REV. E | REV. F | REV. G | REV. H | REV. J | REV. K | REV. L | REV. M |
|---|---|---|---|---|---|---|---|---|---|
| DATE | FEB/28/19 | OCT/19/20 | NOV/12/20 | JAN/12/21 | APR/01/21 | AUG/18/21 | AUG/05/22 | SEP/30/22 | DEC/02/22 |
| DESIGN | ESUP | ESUP | ESUP | ESUP | ESUP | ESUP | ESUP | ESUP | ESUP |
| EXECUTION | CAMILA | CAMILA | CAMILA | U5D6 | Q082 | U5D6 | U44D | C27N | C27N |
| CHECK | ANDRÉ LUIS | ANDRÉ LUIS | ANDRÉ LUIS | CLWK | U49R | U49R | U5D6 | U5D6 | U5D6 |
| APPROVAL | ANDREAZC | ANDREAZC | ANDREAZC | U49R | U4JB | U4JB | CDC1 | CDC1 | CDC1 |

# SUMMARY

# 1 INTRODUCTION

## 1.1 Object

1.1.1 This Typical Technical Specification establishes the minimum requirements for the design and supply of the UNIT's Control and Safety System (CSS).

1.1.1.1 The CSS is the main automation system of the UNIT. It is responsible for the main automatic process control loops shown in complementary documents. Besides process control logic, CSS also acts as the system responsible for the main automatic shutdown and Fire and Gas logics of the UNIT.

1.1.2 This specification describes:

1.1.2.1 The main functional and technical requirements of CSS. As CSS is essentially composed by programmable logic controllers, the requirements of I-ET-3010.00-5520-862-P4X-001 – PROGRAMMABLE LOGIC CONTROLLERS – PLC shall be followed.

1.1.2.2 The main requirements of CSS interfaces with other systems of the UNIT, including Supervision and Operation System (SOS), Electrical System, PA/GA (Public Address/General Alarm) and Automation Systems of PACKAGE UNITS.

1.1.2.3 Emergency Panels, that are responsible for manual actuation of emergency shutdown pushbuttons and blow-down valves;

1.1.2.4 Other dedicated electro-mechanical panels.

1.1.2.5 This document shall be read in conjunction with Project´s document entitled AUTOMATION AND CONTROL ARCHITECTURE (item 2.2.2.2).

## 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:

| | |
|---|---|
| AFDS | Addressable Fire Detection System |
| $CO_2$ | Carbon Dioxide |
| CSS | Control and Safety System |
| EMI | Electromagnetic Interference |
| ESD | Emergency Shutdown |
| FAT | Factory Acceptance Test |
| FGS | Fire and Gas System |
| FPSO | Floating, Production, Storage and Offloading |
| HART | Highway Addressable Remote Transmitter |
| HCS | Hull Control System |

| | |
|---|---|
| HDS | Historical Data Server |
| HFGS | Hull Fire and Gas System |
| HMI | Human Machine Interface |
| HSD | Hull Shutdown System |
| HSDN | High Speed Deterministic Network |
| I/O | Input/Output |
| LAN | Local Area Network |
| MTBF | Mean Time Between Failures |
| MTE | Brazilian Ministry of Labor (Portuguese: *Ministério do Trabalho e Emprego*) |
| MTTR | Mean Time to Recovery |
| SNTP | Simple Network Time Protocol |
| OM | Maintenance Inhibition command (previously called as Maintenance Override) |
| OO | Operational Inhibition command (previously called as Operational Override) |
| OPC | Open Platform Communications (former OLE for Process Control), regulated by OPC Foundation |
| OPC UA | OPC Unified Architecture, regulated by OPC Foundation |
| PA/GA | Public Address/General Alarm |
| PCS | Process Control System |
| PID | Proportional–Integral–Derivative Controller |
| PLC | Programmable Logic Controller |
| PSD | Process Shutdown System |
| RFI | Radio-frequency Interference |
| SAT | Site Acceptance Test |
| SIT | Site Integration Test |
| SPCS | Subsea Production Control System |
| SOS | Supervision and Operation System |
| VAC | Ventilating and Air Conditioning |
| VCI | Volatile Corrosion Inhibitor |

# 2 REFERENCE DOCUMENTS, CODES AND STANDARDS

## 2.1 External references

### 2.1.1 International Codes, Recommended Practices and Standards

**IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION**

| | | |
|---|---|---|
| IEC | 60079-2 | EXPLOSIVE ATMOSPHERES – PART 2: EQUIPMENT PROTECTION BY PRESSURIZED ENCLOSURE “p” |
| IEC | 60529 | DEGREES OF PROTECTION PROVIDED BY ENCLOSURES (IP CODE) |
| IEC | 60533 | ELECTRICAL AND ELECTRONIC INSTALLATIONS IN SHIPS - ELECTROMAGNETIC COMPATIBILITY (EMC) – SHIPS WITH A METALLIC HULL |
| IEC | 61000 | ELECTROMAGNETIC COMPATIBILITY (EMC) - ALL PARTS |

| | | |
|---|---|---|
| IEC | 61131 | PROGRAMMABLE CONTROLLERS – ALL PARTS |
| IEC | 62381 | AUTOMATION SYSTEMS IN THE PROCESS INDUSTRY - FACTORY ACCEPTANCE TEST (FAT), SITE ACCEPTANCE TEST (SAT) AND SITE INTEGRATION TEST (SIT) |
| IEC | 61892 | MOBILE AND FIXED OFFSHORE UNITS – ELECTRICAL INSTALLATIONS – ALL PARTS |

**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 115 (21/MARÇO/2022) | REQUISITOS DE AVALIAÇÃO DA CONFORMIDADE PARA EQUIPAMENTOS ELÉTRICOS PARA ATMOSFERAS EXPLOSIVAS - CONSOLIDADO. |

2.1.2.1 All Regulatory Standards issued from National Labour Inspection Secretary (NRs, from *Secretaria de Inspeção do Trabalho*) shall be followed.

2.1.3 **Classification Society**

2.1.3.1 Project's Detail Engineering Design Phase documents shall be submitted to Classification Society's approval. 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's requirements, along with the specific requirements identified in this document, also including 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. They shall be used as the main specification for the Project.

2.2.1.2 Typical Document List

| | |
|---|---|
| I-ET-3010.00-1200-940-P4X-002 | GENERAL TECHNICAL TERMS |
| I-ET-3010.00-5520-862-P4X-001 | PROGRAMMABLE LOGIC CONTROLLERS - PLC |
| I-ET-3010.00-1200-800-P4X-002 | AUTOMATION, CONTROL AND INSTRUMENTATION ON PACKAGE UNITS |
| I-ET-3010.00-5520-888-P4X-001 | AUTOMATION PANELS |
| I-ET-3010.00-5520-861-P4X-002 | SUPERVISION AND OPERATION SYSTEM - SOS |
| I-ET-3010.00-1200-850-P4X-002 | ASSET MANAGEMENT SYSTEM (AMS) |
| I-ET-3010.00-5140-700-P4X-003 | ELECTRICAL REQUIREMENTS FOR PACKAGES FOR OFFSHORE UNITS |
| I-ET-3010.00-5522-855-P4X-001 | ADDRESSABLE FIRE DETECTION SYSTEM |
| I-ET-3010.00-5500-854-P4X-001 | MACHINERY MONITORING SYSTEM (MMS) |
| I-ET-3010.00-1200-859-P4X-001 | AUTOMATION REQUIREMENTS FOR CORROSION MONITORING SYSTEM (CMS) |
| I-MD-3010.00-5510-760-PPT-001 | GENERAL CRITERIA FOR TELECOMMUNICATIONS DESIGN |
| I-ET-3010.00-5140-797-P4X-001 | ELECTRICAL SYSTEM AUTOMATION ARCHITECTURE |
| I-DE-3010.00-5140-797-P4X-001 | ELECTRICAL SYSTEM AUTOMATION ARCHITECTURE DIAGRAM |
| I-DE-3010.00-1210-888-P4X-001 | PRODUCTION WELL CONTROL RACK – LAYOUT |
| I-DE-3010.00-1210-888-P4X-002 | PRODUCTION WELL CONTROL RACK - FUNCTIONAL DIAGRAM |
| I-DE-3010.00-5139-390-P4X-001 | HYDRAULIC POWER UNIT (HPU) FOR TOPSIDES VALVES - HYDRAULIC DIAGRAM |
| I-ET-3000.00-5139-800-PEK-004 | HYDRAULIC POWER UNIT FOR SUBSEA EQUIPMENT WITH MULTIPLEXED ELECTROHYDRAULIC AND DIRECT HYDRAULIC CONTROL SYSTEM (OWN FLOATING PRODUCTION UNIT) |
| I-ET-3010.00-1210-888-P4X-001 | PRODUCTION WELL CONTROL RACK |

| | |
|---|---|
| I-ET-3010.00-1210-888-P4X-003 | SESDVS CONTROL RACK |
| I-ET-3010.00-5139-390-P4X-001 | HYDRAULIC POWER UNIT (HPU) FOR TOPSIDES VALVES |
| I-ET-3010.00-5520-800-P4X-002 | IMPLEMENTATION OF INTERLOCKING AND CONTROL LOGIC |
| I-ET-3010.00-5425-260-P4X-001 | CO2 FLOODING FIRE FIRE FIGHTING SYSTEM |
| I-DE-3010.00-5140-797-P4X-002 | ELECTRICAL SYSTEM AUTOMATION TYPICAL ACTUATION DIAGRAMS |
| I-LI-3010.00-5140-797-P4X-001 | ELECTRICAL SYSTEM AUTOMATION INTERFACE SIGNALS LIST. |

### 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)**

TOPSIDES AND HULL AUTOMATION INTERFACE

AUTOMATION INTERFACE OF PACKAGE UNITS

FLOW METERING SYSTEM (FMS)

INSTRUMENTATION ADDITIONAL TECHNICAL REQUIREMENTS

FIELD INSTRUMENTATION

SPECIAL MONITORING SYSTEMS

**DRAWINGS (I-DE)**

FLOW METERING SYSTEM (FMS) ARCHITECTURE

NETWORK INTERCONNECTION DIAGRAM

AUTOMATION AND CONTROL ARCHITECTURE

EMERGENCY SHUTDOWN DIAGRAM

GENERAL NOTES

**LISTS (I-LI)**

EQUIPMENT LIST

I/O LIST

INSTRUMENT LIST

**DESCRIPTIVE MEMORANDUM (I-MD)**

AUTOMATION AND CONTROL SYSTEM FUNCTIONS

**DATA SHEETS (I-FD)**

SAFETY DATA SHEET

2.2.3 **PETROBRAS Reference Documents**

DR-ENGP-M-I-1.3 SAFETY ENGINEERING GUIDELINE

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

# 3 ENVIRONMENTAL AND OPERATIONAL CONDITIONS

3.1 For environmental and operating conditions and/or any requirements, refer to project's technical specification entitled "INSTRUMENTATION ADDITIONAL TECHNICAL REQUIREMENTS".

3.2 The available power supplied by the UNIT to CSS is defined in I-ET-3010.00-5140-700-P4X-003 – ELECTRICAL REQUIREMENTS FOR PACKAGES FOR OFFSHORE UNITS.

3.3 Internally to each panel, the external power will be converted to 24 VDC, using redundant modules. There will be at least one pair of redundant 24 VDC power supplies for each subsystem, to feed all internal CSS components (see I-ET-3010.00-5520-888-P4X-001 - AUTOMATION PANELS). Figure 1 applies for CSS REMOTE I/O PANELS and for CSS PROCESSORS PANELS. Subsystems shall not share their 24 VDC power supplies.

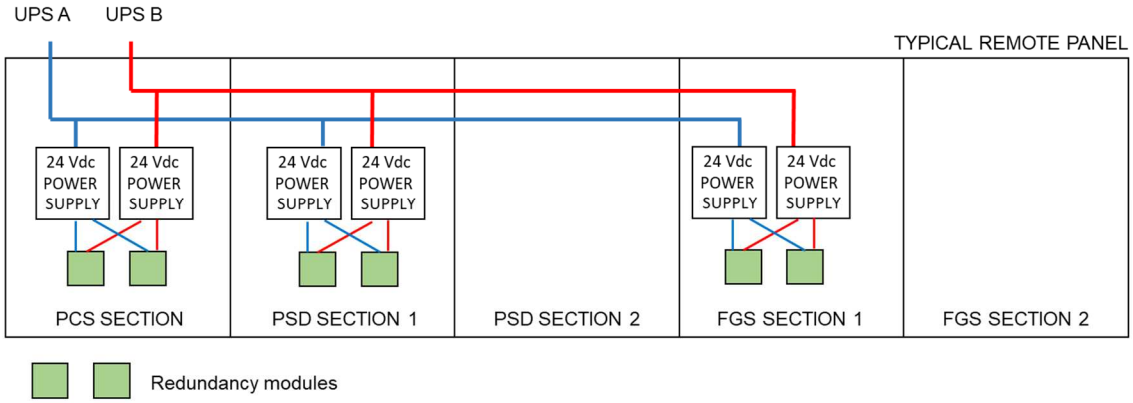


Figure 1- Example of Topsides REMOTE I/O PANEL with one pair of redundant power supplies per subsystem. PSD SECTION 2 is powered by the redundancy modules of PSD SECTION 1, and FGS SECTION 2 is powered by the redundancy modules of FGS SECTION 1. Figure also applies to CSS PROCESSORS PANELS.

3.4 For information about CSS panels, see I-ET-3010.00-5520-888-P4X-001 – AUTOMATION PANELS and item 7.

# 4 TECHNICAL REQUIREMENTS

## 4.1 General Description

4.1.1 Control and Safety System (CSS) is the implementation of the main automation system that performs process control, process safety and mitigation of the UNIT. It is the most important part of the Automation and Control Architecture.

4.1.2 CSS is the Control and Safety layer concerning the Industrial Automation pyramid, and acts as the interface between the Operation and Supervision and Field layers.

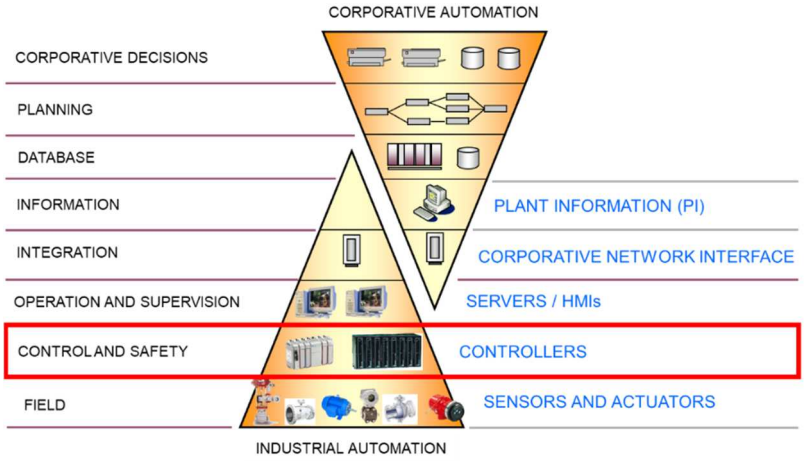


Figure 2 – Industrial and Corporative Automation Pyramids

4.1.3 In order to perform its functions, CSS shall be implemented using sets of redundant processors, named subsystems (see item 4.1.4), communicating with a Supervisory System (SOS). The subsystems shall be as follows:

- **Topsides CSS**: Process Control System (PCS), Process Shutdown System (PSD) and Fire and Gas System (FGS);
- **Hull CSS:** Hull Control System (HCS), Hull Shutdown System (HSD), and Hull Fire and Gas System (HFGS).
- For UNITS with Turret, dedicated processors for Turret Control (TCS) and for Turret Shutdown (TSD) shall also be supplied.

4.1.4 Each CSS subsystem has its own functions and one shall not perform the functions of the other: PCS and HCS shall execute process control/monitoring; PSD and HSD define the prevention systems (process safety); FGS and HFGS define the risk mitigation system. The functions of each subsystem are defined in more detail as follows:

- **PCS – Process Control System:** responsible to perform the analogue control and monitoring functions of the process variables related to the Production and Facilities systems (Topsides) and to communicate with the Topsides Electrical System controllers for electrical devices actuation in normal operation;
- **HCS – Hull Control System:** responsible to perform the analogue control and monitoring functions of the process variables related to the Production and Facilities systems (Hull) and to communicate with the Hull Electrical System controllers for electrical devices actuation in normal operation;
- **PSD – Process Shutdown:** responsible to perform the emergency shutdown logics of the process variables related to the Production and Facilities systems (Topsides), the data acquisition of the ESD hardwired signals of PACKAGE UNITS and to perform hardwired electrical devices actuation in abnormal situation (Topsides ESD-2). PSD generates Topsides ESD-2 level signals and initiators.
- **HSD – Hull Shutdown:** responsible to perform the emergency shutdown logics of the process variables related to the Hull Production and Facilities systems, the data acquisition of the ESD hardwired signals of Hull PACKAGE UNITS and to perform hardwired electrical devices actuation in abnormal situation (Hull ESD-2). HSD generates Hull ESD-2 level signals and initiators.
- **FGS – Fire and Gas System:** responsible to perform the Fire & Gas detection, firefighting (water, foam, $CO_2$) and safety-related ventilation and air conditioners´ logics of Topsides Systems. FGS also generates detected/confirmed fire and gas signals and alarms, as well as ESD-3P/T signals.
- **HFGS – Hull Fire and Gas System:** responsible to perform the Fire & Gas detection, firefighting (water, foam, and $CO_2$) and safety-related ventilation and air conditioners´ logics of Hull Systems. HFGS also generates detected/confirmed fire and gas signals and alarms, as well as ESD-3P/T signals.
- **Note:** Depending on the Acquisitions philosophy proposed for the Design, FGS and HFGS shall be unified for the whole UNIT.

4.1.5 All the CSS redundant processors shall be connected to a single Supervisory Software, in order to comply with fully integrated automation architecture. For more information about the Supervision and Operation System (SOS), see I-ET-3010.00-5520-861-P4X-002 - SUPERVISION AND OPERATION SYSTEM - SOS.

4.1.6 The CSS processors shall be based on Programmable Logic Controllers (PLCs). Distributed control systems technology (DCS) shall not be accepted, in order to optimize maintenance and spare parts offshore and onshore. PLC emulators running in computers are not accepted either.

4.1.6.1 PLC requirements are described in I-ET-3010.00-5520-862-P4X-001 – PROGRAMMABLE LOGIC CONTROLLERS – PLC.

4.1.7 The processors of each CSS subsystem shall be redundant, with simplex I/O cards.

4.1.8 The processors of each CSS subsystem shall be identical, in order to allow interchangeability.

4.1.9 CSS programming general requirements shall be according to I-ET-3010.00-5520-800-P4X-002 - IMPLEMENTATION OF INTERLOCKING AND CONTROL LOGIC.

4.1.10 CSS is composed by hardware, software and services related to its complete functioning. The following equipment are part of CSS scope:

- Sets of redundant power supplies, redundant processors, network cards and I/O cards, each set corresponding to a subsystem (see item 4.1.3), all arranged inside panels, according to item 7;
- REMOTE I/O PANELS for each subsystem, each one containing redundant power supplies, redundant network cards and I/O cards, all arranged inside panels;
- Redundant network between CSS processors and their REMOTE I/O PANELS;
- Redundant network between CSS processors;
- Complete notebook with all necessary software, properly licensed to PETROBRAS, for CSS configuration and programming;
- Emergency Panels and other dedicated electro-mechanical panels;
- Network switches for interface with the Electrical System;
- Panels, racks, cables inside panels, connectors, media, etc.

4.1.11 In the UNIT's Arrangement, CSS components shall be installed taking into account the following philosophy:

- All processors subsystems shall be installed inside dedicated panels in enclosed non-classified rooms;
- All Fire and Gas remote I/Os shall be installed inside REMOTE I/O PANELS in enclosed non-classified rooms;

- Topsides Control and Shutdown I/Os shall be installed inside REMOTE I/O PANELS located near the process areas (internal or external areas, depending on the Design).
- Hull Control and Shutdown I/Os shall be installed inside REMOTE I/O PANELS located near Hull area (internal or external, depending on the Design).

4.1.12 The design life of CSS shall be 25 (twenty-five) years as a minimum, with the following requirements:

- CSS shall operate 24 hours/day, 7 days/ week;
- System maintenance and support shall be available along this life cycle, including the availability of compatible replacements;
- The entire system, including all sub-components, shall allow future upgrade or migration;
- Obsolescence plan shall be supplied with the proposal.

4.1.13 Canceled.

4.1.14 No obsolete CSS component shall be accepted. Only products which manufacturing will not be discontinued for the next 10 years shall be accepted.

4.1.15 CSS Architecture is graphically represented in project's drawing entitled AUTOMATION AND CONTROL ARCHITECTURE. This document shows all the equipment and systems of the UNIT with their corresponding interconnections to each of the CSS subsystems.

4.1.16 All CSS components (processors and cards) shall be of the same MANUFACTURER, brand and model and run the same firmware version.

## 4.2 Safety Requirements

4.2.1 PCS and HCS systems shall not be used for safety and mitigation functions.

4.2.2 CSS shall provide test capability for inputs, outputs and logic control during fault repair.

4.2.3 CSS shall provide diagnostics for: all power supplies, all processors cards, all redundancy cards/channels, all network communication cards, all I/O cards, all I/O points and serial and network interfaces with the programmer. These diagnostics shall be used for calculation of system availability and reliability, as well as for logic and alarm annunciation in the Supervisory System.

## 4.3 Availability and Redundancy Requirements

4.3.1 Each subsystem shall be composed of redundant processors in hot standby configuration.

4.3.1.1 Hot-standby redundancy configuration means that both of the redundant processors shall remain active reading all inputs. Only the main processor

executes logic and writes in the outputs. In the event of a failure in the main processor, the other one shall assume the logic execution and output writing, without affecting the logics executed by the other processors.

4.3.1.2 Failure of one redundant component shall not interfere with the availability of other components (e.g. failure of one network communication card shall not make the entire processor unavailable).

4.3.1.3 Redundancy shall be designed so that any common failure does not cause a loss of process control and operational availability.

4.3.2 It shall be possible a hot replacement of a failed standby processor without affecting the running (duty) processor. When both processors fail, or when single processors (non-redundant processors) are installed (e.g. In PACKAGE UNITS), failed processors shall be exchanged without affecting logics executed by other processors.

4.3.3 Required CSS availability, not including the field instrumentation, shall be, at least:

- PCS and HCS: >= 99.0 %;
- PSD, HSD, FGS and HFGS: >= 99.5 %.

4.3.4 CSS availability calculation shall be based on the use of Mean Time to Repair (MTTR) data. Mean Time Between Failures (MTBF) data for all CSS components shall be informed by MANUFACTURER, including data for processors, including redundancy, communication cards, power supplies and I/O cards.

4.3.5 Availability figures are for each subsystem (PCS, HCS, HSD, PSD, FGS and HFGS), not only per processor. The following parameters shall be used in the calculations:

- Mean Time to Repair (MTTR): 2 h;
- Process startup time: 6 h;
- Periodic inspection interval: 1 (one) year for safety functions, 2 (two) years for control functions.

4.3.6 On power loss of any processor, the involved processor shall retain its application software and data (for example, redundant battery backups), for at least 120 days.

4.3.7 Software updates shall be possible with one CPU running, without requiring process shutdown.

4.3.8 Failure of the main CSS components (power supplies, processors, network cards, I/O cards and I/O channels) shall be sent to registers accessible by the processors, to be used in the automatic logic, in alarm generation and in the Supervisory System, for displaying, alarm annunciation and registering.

## 4.4 I/O Requirements

4.4.1 Each CSS architecture (TOPSIDES CSS and HULL CSS) shall allow at least 20 (twenty) remote I/O panels and at least the number of estimated physical remote I/O points plus spare (according to item 4.5), distributed among these panels.

4.4.2 In order to increase safety functions reliability and plant availability, any voted I/O and I/O associated with redundant equipment shall be installed at different I/O cards.

4.4.3 The following rules shall be applied for I/O allocation:

- Multiple analogue inputs or outputs used for redundancy (i.e. triplicate transmitters used for voting in safety functions) shall be located in different input cards;
- Flame, gas or smoke detectors for the same zone shall be located in segregated cards. Exception is made when digital addressable systems are used for sensors communication. All fire and gas detectors shall be located to FGS/HFGS subsystems, by means of analog input cards. For diagnostic, HART protocol shall be used.
- All I/O associated with redundant process equipment (i.e. duty-standby motors, pumps) shall be located in separate cards;
- Whenever possible, I/O shall be allocated in cards in a way to minimize the number of devices that would be affected by a card failure;
- Split range and cascade control loops outputs shall be located in the same output card;
- Cascade PID process variables shall be located in the same input card;
- Limit switches of the same valve shall be connected to the same input card, for each subsystem, and the solenoid shall be located in the same section;
- Where redundant cards or channels are applied (e.g., voting), these shall be installed in different racks/rails of their redundant partners, with different power supplies.
- ESD initiators and the corresponding output signals shall be connected to the same subsystem (PSD, HSD, FGS, HFGS), in hardwired connection.
- All I/O signals shall be connected to the processor which executes the respective logics. Inputs and outputs of the same control or safety loop shall be connected to the same processor.
- The decision of racks and/or sections segregation shall be made during Detail Engineering Design Phase taking into account the available physical space for expansion of the Remote I/O Panel.
- The distribution of discrete output signals related to BDVs' opening commands shall be done in such a way that one (01) single failure of a non-redundant CSS component does not cause a flow rate greater than 100% of the maximum flare capacity. Redundant CSS components do not need to be taken into account in the analysis.

4.4.4 For Failure and override (maintenance inhibition) logics for voted inputs used in Fire and Gas logic (mainly fire and gas detectors), DR-ENGP-M-I-1.3 - SAFETY ENGINEERING GUIDELINE shall be consulted for the programming.

4.4.5 In case there is a failure in an I/O card/channel associated to a redundant equipment, this shall only affect the logic associated with the related equipment.

4.4.6 Racks used for redundant I/O cards architecture shall not share common features such as buses, etc.

4.4.7 Fire Fighting CO2 field instruments data (solenoids and pushbuttons), if available, shall be acquired by FGS/HFGS and shall have line monitoring (DIM/DOM).

4.4.8 All analogue field instruments with HART communication protocol shall be connected to analog I/O cards with HART communication capabilities (AIH).

4.4.9 The total power consumption of the cards, racks and sections shall be taken into account when sizing processors power supplies and fuses.

4.4.10 I/O cards connected to solenoid valves shall have fuses installed inside them, in the terminal strips that supply power to those solenoids. Each I/O channel connected to a solenoid valve shall have an individual fuse.

4.4.11 Analog input card channels for 2-wire instruments, digital input card channels and digital output card channels shall be protected with fuse terminal block on positive and knife terminal block on negative.

4.4.12 Analog input card channels for 3-wire instruments shall be protected with fuse terminal block on positive +24 VDC, fuse terminal block on I+ and knife terminal block on 0VDC.

4.4.13 Analog input card channels for 4-wire instruments shall be protected with fuse terminal block on positive +24 VDC, fuse terminal block on I+, knife terminal block on 0VDC and knife terminal block on I-.

4.4.14 Analog Output card channels shall be protected with fuse terminal block on positive +24 VDC and knife terminal block on negative.

4.4.15 In order to protect CO2 actuation logic against undesirable and unsafe operations, the following actions of prevention shall be adopted:

- use of specific memory area for the logic programming;
- use of dedicated I/O cards, in FGS/HFGS;
- use of password to access the application program for maintenance.

4.4.16 For further $CO_2$ flood fire-fighting system I/O allocation requirements see I-ET-3010.00-5425-260-P4X-001 – CO2 FLOODING FIRE FIRE FIGHTING SYSTEM.

## 4.5 Future expansion capability

4.5.1 The total amount of I/O points shall be counted. Then, 20% of this quantity shall be added and physically connected, by panel, section and I/O type. Additionally, for each panel subsystem section, it shall be foreseen empty slots related to 10% of the section I/O count, for future use.

4.5.2 During Detail Engineering Design Phase, the total I/O quantity shall be reassessed based on Basic Engineering Design documentation, Safety Studies and other Detail Engineering Design documentation.

4.5.3 Remote I/O racks shall be expandable.

4.5.4 All channels, including spare or additional channels, shall be wired to terminals, ready for field interconnection.

4.5.5 All empty I/O slots shall be provided with blank plates.

4.5.6 Application program shall take into account at least the maximum number of I/Os, including installed and uninstalled spare.

4.5.7 For each CSS subsystem, a spare area for data exchange of, at least, 5 MBytes in addressable memory of PLC application shall be configured in order to attend future expansions, without the need to stop the PLC for download new items.

## 4.6 Failed component replacement

4.6.1 The system hardware shall have hot swap capability.

4.6.2 For redundant processors in hot-standby configuration, it shall be possible to replace the failed component without affecting the system's operation. For example, if the running processor fails, its redundant pair shall take over the control and shall continue to execute the logic and to write in the outputs while the failed module is replaced. The replaced module will then operate as the standby and can take over control if the running module fails.

4.6.3 For non-redundant system components, the replacement of one module shall not affect other modules in the system. For example, if a simplex I/O card or network card fails, it shall be possible to replace it without the need to reset any other card.

4.6.4 Individual modules of the CSS shall be designed to restart automatically when replaced or powered up following a power loss.

## 4.7 Response Time Requirements

4.7.1 CSS response time is defined as the maximum time from the occurrence of an event at the input terminations to the response at output terminals. This covers I/O card response times, processor scan rates and any communication delays (I/O bus, data communication networks). CSS response time shall be such that it does not compromise safety and operation of the UNIT. The maximum response times are:

- Closed control loops: 1 second;
- Safety interlocking and Emergency shutdown loops: 0.5 second.

4.7.2 Fixed scan rate in all CSS processors programming is allowed.

4.7.3 Scheduling tasks (different processors scan rates) is allowed, with the suggested maximum scan time:

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

## 4.8 Synchronization Requirements

4.8.1 To maintain an appropriate chronology of events, all CSS processors (for each subsystem), as well P2, P2C, P2S and P2SC PACKAGE UNITS processors, shall be synchronized by a Time Server. The Time Server is part of the scope of the Electrical System. This Time Server shall read date/time information from the UNIT's GPS and send this information to all the processors using SNTP (Simple Network Time Protocol). This shall be done through the CSS Data Acquisition LAN.

4.8.2 The synchronization accuracy shall be better than 500 milliseconds and poll interval shall be 24h or less.

4.8.3 CSS shall be synchronized with SOS.

4.8.4 See NETWORK INTERCONNECTION DIAGRAM Drawing.

### 4.9 Processor Loading

4.9.1 Processor application software size shall be such that there is enough memory to allow the program to run, without affecting I/O scanning, communications or diagnostics, even when all I/O (installed, spare and 10% future installation capacity) and associated application software is added, occupying a maximum of 70% of the memory during execution.

4.9.2 If the manufacturer recommends greater spare memory requirements, these shall apply.

4.9.3 Processor cycle times shall be set to ensure that when higher priority activities such as scanning I/O and executing application software are complete, there is sufficient free time for the processor to execute system diagnostics, communications (to other processors and HMI) and other activities such as intercommunications from the running duty processor to the standby processor.

4.9.4 A single failure in one processor or remote communication card shall not interrupt the whole I/O communication continuity, i.e. a bumpless switchover shall be guaranteed.

### 4.10 Management of Change Requirements

4.10.1 CSS application program shall be capable of storing logs in order to keep record of all software modifications of each subsystem.

4.10.2 Modification logs shall include date/time, modified information and user identification.

## 5 PROCESSOR TO PROCESSOR COMMUNICATION

5.1 Processors of different subsystems communication shall take place via a dedicated, redundant and deterministic high-speed network (HSDN). Data to be transmitted using HSDN shall be restricted to the minimum, and subject to PETROBRAS approval.

5.2 The use of Ethernet in a deterministic configuration for HSDN is accepted. In this case, low utilization of the whole channel capacity shall be ensured in order to avoid congestion and minimum total latency.

5.3 HSDN bit transmission rate shall be at least 2 Mbps.

5.4 When transferring data between processors, such as communication configuration, logic must be set up in a separately identifiable program area in the processor.

5.5 All communicated data, communication diagnostics data, and communication configuration shall be stored in the same program area.

## 5.6 Fail-Safe, Line Monitoring and Fail-Reliable Configurations

5.6.1 Most inputs and outputs shall in general use the principle of fail-safe (do not require energy to go to the safe state). The following inputs and outputs shall require energy to go to safe sate (energize to trip) and shall be monitored:

- ADV (deluge valves) solenoids (discrete output monitored - DOM)
- Firefighting $CO_2$ solenoids (discrete output monitored - DOM)
- Firefighting $CO_2$ start pushbuttons (discrete input monitored – DIM)

5.6.2 In case of communication between processors and between processor and remote I/O card, errors may occur, preventing a transmitted signal to be reached to the receiver. When communication fails, a value shall be assigned by the receiver to this signal. The value, which will be assigned, depends on whether the data transmission is configured as *fail-safe* or *fail-reliable* or if there is a pre-defined value by Design.

5.6.3 Fail-safe communication configuration shall imply that on Loss of Communication Status, a fail-safe value shall be assigned (substituted) to the signal being communicated. Loss of Communication Status shall be generated upon the loss of communication or at a data read error for a predetermined time period (maximum 10 seconds) between two processors. This time period shall be determined by evaluating the risk of communicating data as Fail-Reliable for that time period. An alarm shall also be generated to indicate Loss of Communication Status.

5.6.4 Fail-reliable communication configuration shall imply that on Loss of Communication Status, the signal shall hold its last good value and an alarm shall be generated to indicate Loss of Communication. A Loss of Communication Status shall be generated upon the loss of communication, or at a data read error for a predetermined time period (typically 5 seconds), between two processors.

5.6.5 Table 1 indicates the requirements when there is failure in power supply, communication or I/O card:

Table 1 – Data status in failure conditions

| DATA | STATUS | NOTES |
|---|---|---|
| Sequence Logic | Pre-defined status to be defined by Design | |
| Control Loop status (manual/automatic) | Manual | To be confirmed during Commissioning Phase |
| Control Loop parameters (P, I, D) | Last value | Manual tuning is required |
| Block and Safety Valves (SDV, BDV) | Fail Safe (SDV closed; BDV open) | Manual reset action is required |
| Pumps and other electrical equipment | Fail Safe (stop) | Manual restart action is required |

| | | |
|---|---|---|
| On-off and control valves (XV, PV, LV, FV, TV) | Pre-defined status to be defined by Design | |

# 6 SYSTEM DIAGNOSTICS

6.1 CSS shall incorporate system diagnostics so that faults are identified and reported to maintenance/operation staff. Whenever a fault is detected, an alarm of mal-functioning shall be activated at Supervisory System. The priority and Group shall be defined in Design.

6.2 System diagnostic shall cover the following status, at minimum:

- Processor(s) failure;
- I/O modules and channels;
- I/O communication channels;
- System and field power supplies;
- Processor software check, comprising application and system software and memory integrity;
- Process hardware check;
- Network communication cards;

6.3 CSS actions taken as the result of diagnostic errors are as a minimum:

- Any undefined condition detected through diagnostic check shall result in fail-safe action, ex: undefined logic-result (e.g.: divided by zero, negative square root, etc.);
- Loss of an I/O module, loss of both processors, loss of all power supplies shall result to fail-safe actions and alarm annunciation.

6.4 Remote I/O total communications failure shall carry the outputs to safe state. Accordingly, the Remote I/O cards shall have 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. Special cases will be informed by Design.

6.5 Upon communications return, the application program shall be notified and a message shall be displayed at Supervision and Operation System.

6.6 The PLCs shall have built-in capacity to send failure information to external bits accessible by the Supervisory System.

# 7 PANELS

7.1 CSS shall be supplied installed in panels, with the following subdivisions: (for more information see I-ET-3010.00-5520-888-P4X-001 – AUTOMATION PANELS):

- TOPSIDES CSS PROCESSORS PANEL, with independent sections for each topsides CSS subsystem (PCS, PSD and FGS processors);
- HULL CSS PROCESSORS PANEL, with independent sections for each Hull CSS subsystem (HCS, HSD and HFGS processors);

- TOPSIDES CSS REMOTE I/O PANELS – remote panels that house power supplies, I/O network cards and I/O cards for each Topsides CSS subsystem (dedicated sections for each subsystem - PCS, PSD and FGS);
- HULL CSS REMOTE I/O PANELS – remote panels that house power supplies, I/O network cards and I/O cards for each Hull CSS subsystem (dedicated sections for each subsystem – HCS, HSD and HFGS).

7.2 Electromechanical characteristic of the panels, including pressurization guidelines, are in I-ET-3010.00-5520-888-P4X-001 – AUTOMATION PANELS.

7.3 Connection between the CSS PROCESSORS PANELS with their corresponding CSS REMOTE I/O PANELS shall be implemented through a dedicated I/O redundant high-speed deterministic network (I/O Deterministic Communication Network), both permanently active. Connection shall be done by means of optical fiber (for external areas) or electric cables (internal areas). In case electric cables are used, cable length shall not be greater than 100m. Each redundant I/O network shall be directly connected to each redundant CPU and both I/O redundant networks shall be accessible by each redundant CPU, independently of the status of the other redundant CPU.

7.4 Redundant networks shall run through different paths in the UEP (including redundant I/O networks).

7.5 All FGS / HFGS I/Os shall be installed in the indoor CSS REMOTE I/O PANEL nearest to the related instrument.

7.6 Design will inform how many panel sections are allowed to be towed, installed and moved together.

## 7.7 CSS Processors Panels

7.7.1 There shall be 1 (one) TOPSIDES CSS PROCESSORS PANEL and 1 (one) HULL CSS PROCESSORS PANEL, with 3 (three) sections each (one per each subsystem), installed indoors, at air conditioned areas.

7.7.2 Each CSS PROCESSORS PANEL section shall be composed by one subsystem (two half-clusters). Each half-cluster shall have at least the following characteristics:

- Power supplies;
- One processor (CPU);
- One redundancy card (for data updating and synchronization between active and standby CPU);
- Two redundant Ethernet/TCP-IP cards to perform communication with Supervisory System;
- Two redundant I/O network cards to perform communication of the PLCs with the CSS REMOTE I/O PANELS. (Note: I/O network shall be redundant and deterministic);

- Two redundant network cards to perform communication between processors of different CSS subsystems (HSDN) (Note: Processor to processor network shall be redundant and deterministic);
- Three Modbus TCP/IP communication cards to perform communication with other systems (e.g., Electrical System Controllers and/or Addressable Fire Detection System (AFDS));
- One chassis where the aforementioned components shall be mounted.

7.7.3 Dedicated diagnosis signals shall be made available in the Supervisory System in order to indicate failure of any half-cluster component and/or the occurrence of half-cluster switchover.

7.7.4 CSS PROCESSORS PANEL shall not house I/O cards. These shall be placed in CSS REMOTE I/O PANELS.

7.7.5 The dedicated sections of each CSS PROCESSORS PANEL shall be electrically isolated. Each panel will receive external redundant power supply from the UNIT UPS, according to I-ET-3010.00-5140-700-P4X-003 – ELECTRICAL REQUIREMENTS FOR PACKAGES FOR OFFSHORE UNITS.

7.7.6 CSS PROCESSORS PANELS and CSS REMOTE I/O PANELS are emergency loads.

## 7.8 CSS Remote I/O Panels

7.8.1 The quantity of CSS REMOTE I/O PANELS and panel sections may be different for each project. The specific information shall be consulted in the Project's EQUIPMENT LIST.

7.8.2 Each TOPSIDES CSS REMOTE I/O PANEL shall have dedicated sections segregated for each subsystem: Topsides Control System (PCS), Topsides Shutdown System (PSD) and Fire and Gas System (FGS) or according to Project's EQUIPMENT LIST.

7.8.3 Each HULL CSS REMOTE I/O PANEL shall have dedicated sections segregated by each subsystem: Hull Control System (HCS), Hull Shutdown System (HSD) and Hull Fire and Gas System (HFGS) or according to Project's EQUIPMENT LIST.

7.8.4 The dedicated sections of each CSS REMOTE I/O PANEL shall be electrically isolated. Each panel will receive external redundant power supply from the UNIT UPS, according to I-ET-3010.00-5140-700-P4X-003 – ELECTRICAL REQUIREMENTS FOR PACKAGES FOR OFFSHORE UNITS.

7.8.5 Only 24 VDC nominal voltage instruments shall be fed by the CSS REMOTE I/O PANEL components. For any instrument requiring a nominal voltage other than 24 VDC, the project's technical specification entitled FIELD INSTRUMENTATION shall be consulted.

7.8.6 The 24 VDC electrical power source used to feed the analogue input cards and 3 (three) wire instruments shall be the same.

7.8.7 24 VDC electrical power sources, CSS REMOTE I/O PANEL circuit breakers and cabling shall be sized for PCS/PSD/FGS and HCS/HSD/HFGS considering full power / full current consumption (actuated, heat resistors enabled etc.) of all instruments fed by CSS REMOTE I/O PANEL simultaneously. No power factor / utilization factor shall be applied.

7.8.8 The power, voltage, and current demanded by each CSS REMOTE I/O PANEL from each UPS shall be indicated in the SOS.

## 7.9 MANUAL ESD STATIONS and EMERGENCY PANELS

7.9.1 If required by Classification Society, MANUAL ESD STATIONS shall be provided in open areas, and their quantities and locations shall be defined during the Project's Detail Engineering Design Phase.

7.9.2 Additionally, two Emergency Panels shall be provided indoors:

- EMERGENCY PANEL A: shall be provided in order to house ESD pushbuttons (ESD-2, ESD-3P, ESD-3T, ESD-4), "PREPARE FOR ABANDON", BDVs depressurization pushbuttons (one for each BDV) and "EMERGENCY GENERATOR DIESEL ENGINE SHUTDOWN".

- EMERGENCY PANEL B: shall be provided in order to house ESD pushbuttons (ESD-2, ESD-3P, ESD-3T and ESD-4), "PREPARE FOR ABANDON" pushbutton and "EMERGENCY GENERATOR DIESEL ENGINE SHUTDOWN".

7.9.3 All pushbuttons shall be protected against involuntary activation, "Lift and Push the button" type. Addressable type is not acceptable. See also Table 2.

7.9.4 ESD-2 pushbuttons shall be connected directly to both PSD and HSD.

7.9.5 ESD-3P, ESD-3T, ESD-4 and "PREPARE FOR ABANDON" pushbuttons shall be connected directly to both FGS and HFGS.

7.9.6 BDVs pushbuttons connection to CSS subsystems shall be verified in Project's documentation.

7.9.7 "EMERGENCY GENERATOR DIESEL ENGINE SHUTDOWN" pushbutton shall be connected to HFGS.

7.9.8 The manual ESD signals from these pushbuttons shall be interlocked with the automatic ESD logic in order to result in a single shutdown command to each final element.

7.9.9 ESD-2 signals generated by HSD logic shall be sent to PSD and vice-versa.

7.9.10 ESD-3P/3T signals generated by FGS logic shall be sent to HFGS and vice-versa.

7.9.11 ESD-3P/3T signals generated by FGS logic shall be sent to PSD and ESD-3P/3T signals generated by HFGS logic shall be sent to HSD.

7.9.12 ESD-4 signals from pushbutton received by FGS logic shall be sent to HFGS and vice-versa. This will work as redundancy, since the ESD-4 signal shall not be fail-safe.

7.9.13 "PREPARE FOR ABANDON" pushbuttons in EMERGENCY PANELS A and B shall have 3 contacts, 1 (one) to be directly connected to PA/GA panel A, 1 (one) to be directly connected to PA/GA panel B and 1 (one) to be connected to CSS-(H)FGS remote I/O panel. At CSS-(H)FGS side, the contact shall be normally open (NO) with line monitoring (DIM). The contacts at PA/GA side shall be according to PA/GA technical specification.

7.9.14 Each CSS discrete output (DO) responsible for sending the ESD-2/3P/3T signals shall have an associated interposing relay. In all of these cases, the panel sending the discrete output shall hold the interposing relay (see Figure 3). Discrete Output Relay (DOR) is not accepted.

7.9.15 Each CSS discrete input (DI) responsible for receiving the ESD-2/3P/3T signals shall be fail-safe (DI).

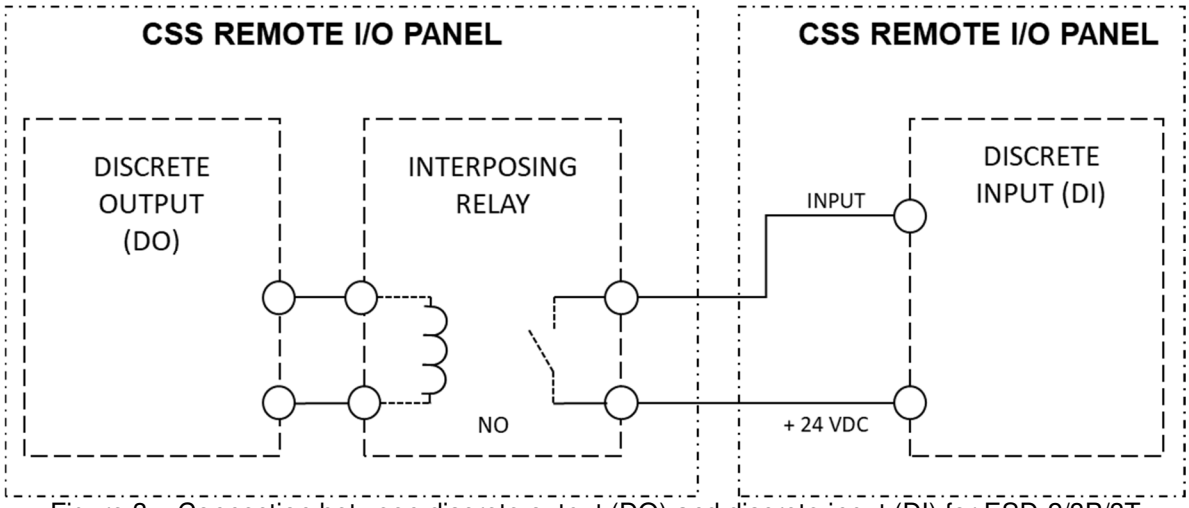


Figure 3 – Connection between discrete output (DO) and discrete input (DI) for ESD-2/3P/3T transmission between CSS REMOTE I/O PANELS.

7.9.16 The CSS discrete output responsible for sending the ESD-4 signal shall be monitored (DOM) and have an interposing relay associated. The panel sending the discrete output shall hold the interposing relay. Discrete Output Relay (DOR) is not be accepted. A resistor shall be placed after the interposing relay, in the CSS REMOTE I/O PANEL responsible for sending the ESD-4 (see Figure 4). This resistor shall be sized during Project's Detail Engineering Design Phase.

7.9.17 The CSS discrete input responsible for receiving the ESD-4 signal shall be monitored (DIM).

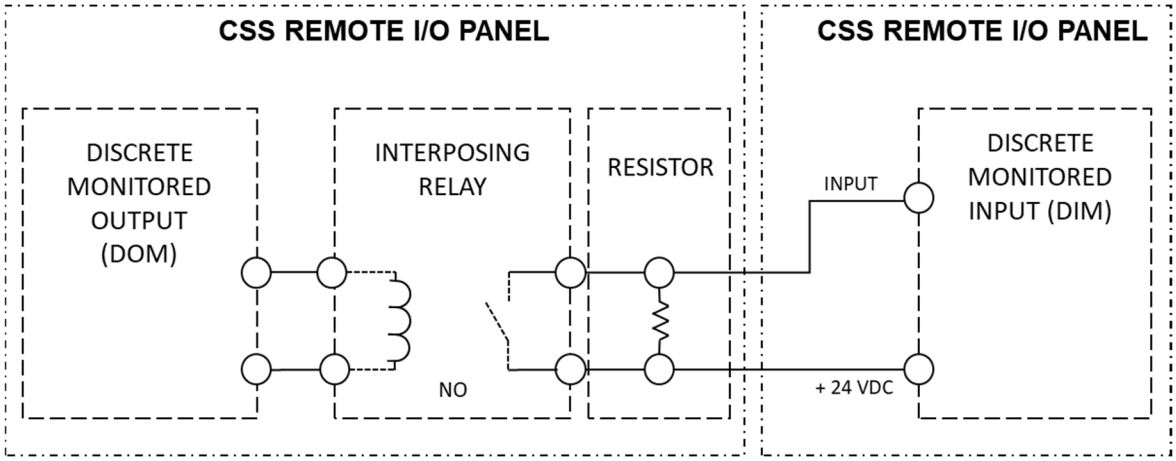


Figure 4- Connection between monitored discrete output (DOM) and monitored discrete input (DIM) for ESD-4 transmission between CSS REMOTE I/O PANELS.

7.9.18 Table 2 describes the ESD signals that shall be exchanged between CSS REMOTE I/O PANELS, MANUAL ESD STATIONS and EMERGENCY PANELS pushbuttons.

Table 2 - ESD signals exchanged between CSS REMOTE I/O PANELS, MANUAL ESD STATIONS and EMERGENCY PANELS pushbuttons

| FROM | I/O TYPE | TO | CSS I/O TYPE | SIGNAL | FAIL STATE |
|---|---|---|---|---|---|
| MANUAL ESD-2 PUSHBUTTON | ELECTRICAL CONTACT PUSHBUTTON | PSD REMOTE I/O PANEL | DIM | ESD-2 | ENERGIZE TO TRIP |
| MANUAL ESD-2 PUSHBUTTON | ELECTRICAL CONTACT PUSHBUTTON | HSD REMOTE I/O PANEL | DIM | ESD-2 | ENERGIZE TO TRIP |
| PSD REMOTE I/O PANEL | DO | HSD REMOTE I/O PANEL | DI | ESD-2 | FAIL-SAFE |
| HSD REMOTE I/O PANEL | DO | PSD REMOTE I/O PANEL | DI | ESD-2 | FAIL-SAFE |
| MANUAL ESD-3T PUSHBUTTON | ELECTRICAL CONTACT PUSHBUTTON | FGS REMOTE I/O PANEL | DIM | ESD-3T | ENERGIZE TO TRIP |
| MANUAL ESD-3T PUSHBUTTON | ELECTRICAL CONTACT PUSHBUTTON | HFGS REMOTE I/O PANEL | DIM | ESD-3T | ENERGIZE TO TRIP |
| MANUAL ESD-3P PUSHBUTTON | ELECTRICAL CONTACT PUSHBUTTON | FGS REMOTE I/O PANEL | DIM | ESD-3P | ENERGIZE TO TRIP |
| MANUAL ESD-3P PUSHBUTTON | ELECTRICAL CONTACT PUSHBUTTON | HFGS REMOTE I/O PANEL | DIM | ESD-3P | ENERGIZE TO TRIP |
| MANUAL ESD-4 PUSHBUTTON | ELECTRICAL CONTACT PUSHBUTTON | FGS REMOTE I/O PANEL | DIM | ESD-4 | ENERGIZE TO TRIP |

| FROM | I/O TYPE | TO | CSS I/O TYPE | SIGNAL | FAIL STATE |
|---|---|---|---|---|---|
| MANUAL ESD-4 PUSHBUTTON | ELECTRICAL CONTACT PUSHBUTTON | HFGS REMOTE I/O PANEL | DIM | ESD-4 | ENERGIZE TO TRIP |
| PREPARE FOR ABANDON PUSHBUTTON | ELECTRICAL CONTACT PUSHBUTTON | HFGS REMOTE I/O PANEL | DIM | PREPARE FOR ABANDON | ENERGIZE TO TRIP |
| PREPARE FOR ABANDON PUSHBUTTON | ELECTRICAL CONTACT PUSHBUTTON | PA/GA A (see item 8.8) | N/A | PREPARE FOR ABANDON | -- |
| PREPARE FOR ABANDON PUSHBUTTON | ELECTRICAL CONTACT PUSHBUTTON | PA/GA B (see item 8.8) | N/A | PREPARE FOR ABANDON | -- |
| FGS REMOTE I/O PANEL | DO | HFGS REMOTE I/O PANEL | DI | ESD-3T | FAIL-SAFE |
| FGS REMOTE I/O PANEL | DO | HFGS REMOTE I/O PANEL | DI | ESD-3P | FAIL-SAFE |
| HFGS REMOTE I/O PANEL | DO | FGS REMOTE I/O PANEL | DI | ESD-3T | FAIL-SAFE |
| HFGS REMOTE I/O PANEL | DO | FGS REMOTE I/O PANEL | DI | ESD-3P | FAIL-SAFE |
| FGS REMOTE I/O PANEL | DOM | HFGS REMOTE I/O PANEL | DIM | ESD-4 | -- |
| HFGS REMOTE I/O PANEL | DOM | FGS REMOTE I/O PANEL | DIM | ESD-4 | -- |
| FGS REMOTE I/O PANEL | DO | PSD REMOTE I/O PANEL | DI | ESD-3T | FAIL-SAFE |
| FGS REMOTE I/O PANEL | DO | PSD REMOTE I/O PANEL | DI | ESD-3P | FAIL-SAFE |
| HFGS REMOTE I/O PANEL | DO | HSD REMOTE I/O PANEL | DI | ESD-3T | FAIL-SAFE |
| HFGS REMOTE I/O PANEL | DO | HSD REMOTE I/O PANEL | DI | ESD-3P | FAIL-SAFE |

7.9.19 EMERGENCY PANEL A shall be installed at CCR-Operation Ambiance and EMERGENCY PANEL B at Radio Room, both wall-mounted.

7.9.20 Construction, structure, plates, color and painting system for EMERGENCY PANELS shall follow the same standard of the CSS indoor panels.

7.9.21 Prevention and mitigation emergency shutdown actions shall be according to Project's documentation entitled EMERGENCY SHUTDOWN DIAGRAM.

7.9.22 MANUAL ESD STATIONS and EMERGENCY PANELS shall have a clear (transparent) protective lid in order to prevent accidental actuation, as required by NR 12 - *SEGURANÇA NO TRABALHO EM MÁQUINAS E EQUIPAMENTOS*. The protective lids shall remain unlocked.

7.9.23 Figure 5 shows suggested layout for EMERGENCY PANEL A (CCR).

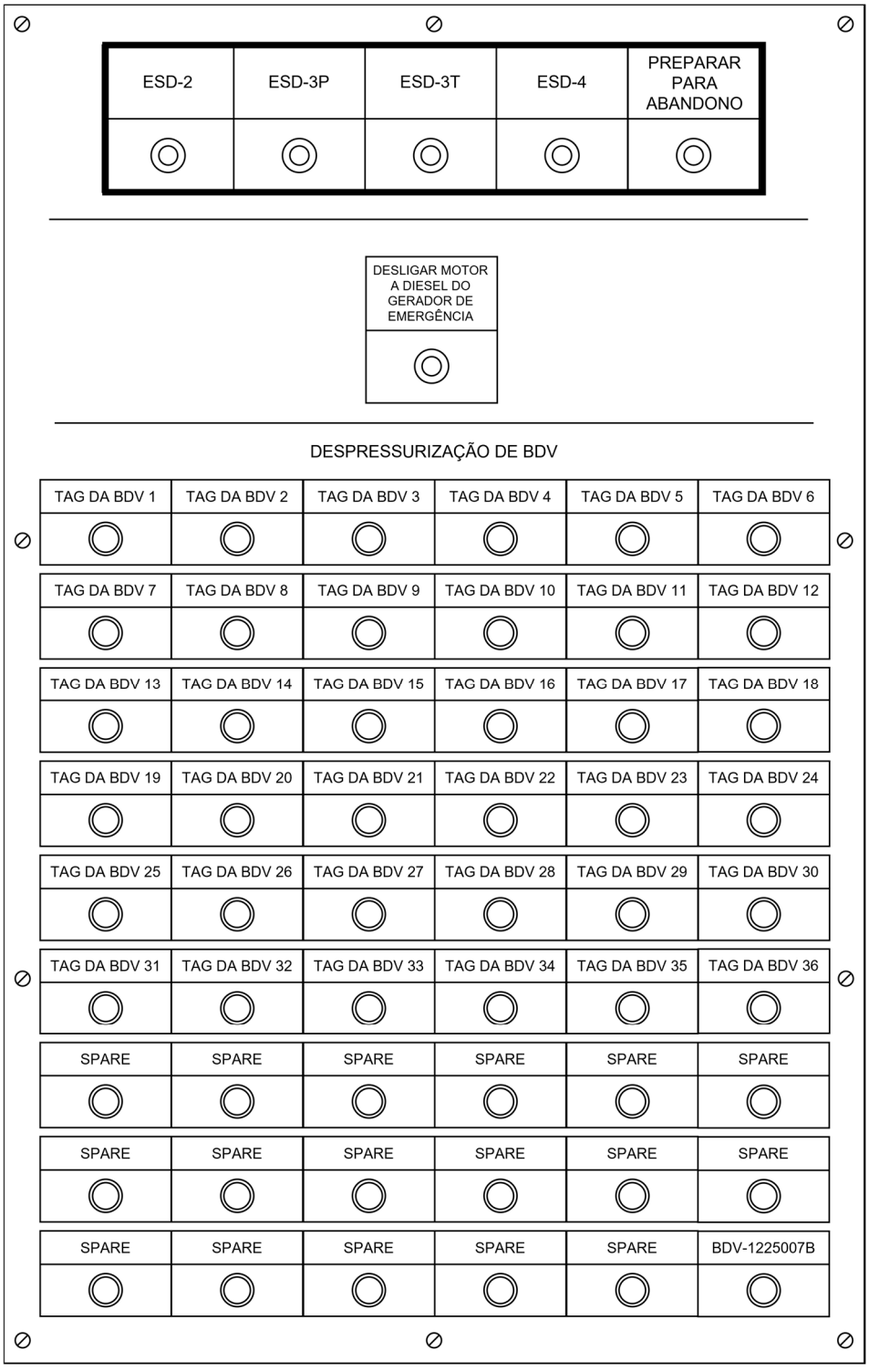


Figure 5 – Suggested layout for EMERGENCY PANEL A

## 7.10 ALARM PANELS

7.10.1 Two ALARM PANELS shall be placed at the operator's desk, next to the SOS HMIs, in order to indicate Hull and Topsides high priority Alarm resume.

7.10.2 TOPSIDES ALARM PANEL shall be composed of two indicators: one for TOPSIDES DETECTED FIRE / DETECTED GAS and one for TOPSIDES PROCESS PRIORITY ALARMS.

7.10.3 HULL ALARM PANEL shall be composed of two indicators: one for HULL DETECTED FIRE / DETECTED GAS and one for HULL PRIORITY ALARMS.

7.10.4 Each indicator shall be a 24 VDC audible alarm (buzzer) combined with LED signaling device.

7.10.5 Audible alarm intensity shall not be greater than 50 dB.

7.10.6 Indicator LED signal shall be intermittent. Red lamps shall be used to indicate DETECTED FIRE / DETECTED GAS and yellow lamp shall be used to indicate PRIORITY ALARM RECEIVED.

7.10.7 Alarm acknowledgement shall only be done through the Supervisory System. The ALARM PANELS do not need any acknowledgement device.

7.10.8 Topsides and Hull Priority Alarms shall be defined during Detail Engineering Design Phase.

7.10.9 Figure 6 shows a suggested layout for ALARM PANELS.

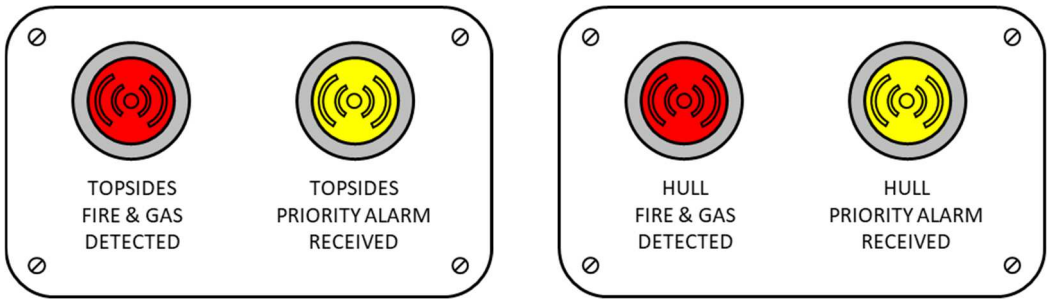


Figure 6 – Suggested layout for ALARM PANELS

## 7.11 Inhibition (Overrides)

7.11.1 Whenever input devices inhibition is required for plant operation, such as: temporary maintenance, plant or unit/equipment start-up, F&G detectors failures and input devices functionality test, two types of inhibition (overrides) shall be provided, as follows:

- OM (MAINTENANCE INHIBITION): instrument inhibition for maintenance purposes;

- OO (OPERATIONAL INHIBITION): individual logic signal inhibition for operation purposes, preventing system from shutting down in determined cases.

7.11.2 Instrument and signals subject to OO and to OM are defined in Detail Engineering Design Phase.

7.11.3 For further details, see Project's AUTOMATION AND CONTROL SYSTEM FUNCTIONS Descriptive Memorandum and SOS SCREENS Technical Specification.

# 8 CSS INTERFACES

## 8.1 General Information

8.1.1 The CSS shall have data exchanged with SOS, PACKAGE UNITS, Electrical System and other special systems.

8.1.2 For better understanding, refer to Technical Specifications listed in Item 2.2.

## 8.2 CSS – SOS

8.2.1 The interface between CSS and SOS shall be performed through two redundant network interfaces at each subsystem half-cluster (one subsystem contains two half-clusters).

8.2.2 This network is the Data Acquisition layer of the Automation Network, split into CSS Data Acquisition LAN and Package Unit LAN.

8.2.3 CSS supplier shall provide its corresponding OPC-UA software connector to communicate with SOS OPC-UA connector.

8.2.4 For more information, see Typical Document I-ET-3010.00-5520-861-P4X-002 – SUPERVISION AND OPERATION SYSTEM – SOS and Project´s drawings AUTOMATION AND CONTROL ARCHITECTURE and NETWORK INTERCONNECTION DIAGRAM.

## 8.3 CSS - Addressable Fire Detection System

8.3.1 The interface between FGS, HFGS and the AFDS Panel(s) shall be implemented through a network with communication protocol according to documentation specific to the project.

8.3.2 Resources shall be provided in order to guarantee the communication with the AFDS without losing supervision data, even at the failure of one of the dual FGS/HFGS racks.

8.3.3 Each FGS/HFGS system rack shall have a dedicated RS-485 or Modbus TCP/IP card to communicate with the AFDS.

8.3.4 All Fire detection and firefighting logics shall be implemented at FGS/HFGS, using both FGS/HFGS I/Os and the AFDS inputs. Despite being technically possible, AFDS shall not be used for logic, just as inputs.

8.3.5 For specific information about AFDS, refer to I-ET-3010.00-5522-855-P4X-001 - ADDRESSABLE FIRE DETECTION SYSTEM.

8.3.6 Information regarding number and types of sensors per zone is indicated in project's document entitled SAFETY DATA SHEET.

## 8.4 CSS - VAC

8.4.1 The interface with VAC equipment (dampers, air-conditioner, etc.), where applicable, shall be hardwired, through the FGS / HFGS system.

## 8.5 CSS – PACKAGE UNITS

8.5.1 CSS shall have hardwired signals exchanged with the PACKAGE UNITS Automation Systems (typically trip initiators, emergency shutdowns, confirmed fire and confirmed gas signals). Other signals may be applied, depending on the PACKAGE UNIT.

8.5.2 Hardwired interface between CSS and the PACKAGE UNITS shall be implemented through the I/O cards of the CSS Remote I/O Panels and the PACKAGE UNITS Automation Systems.

8.5.3 Normally, the interface between CSS and PACKAGE UNITS Automation Systems are discrete signals. However, it might be possible to exchange analog signals as well. The project documentation (P&ID's, Technical Specifications and I-ET-3010.00-1200-800-P4X-002 - AUTOMATION, CONTROL AND INSTRUMENTATION ON PACKAGE UNITS) shall also be consulted.

8.5.4 For analog signals interchanged between PACKAGE UCP and CSS, galvanic isolators shall be foreseen. The isolators shall be located in the adequate subsystem section of the CSS REMOTE I/O PANEL.

8.5.5 For further information, refer to I-ET-3010.00-1200-800-P4X-002 - AUTOMATION, CONTROL AND INSTRUMENTATION ON PACKAGE UNITS and project's documentation entitled AUTOMATION INTERFACE OF PACKAGE UNITS.

## 8.6 CSS - Electrical System

8.6.1 The redundant Electrical System controllers (see I-DE-3010.00-5140-797-P4X-001 - ELECTRICAL SYSTEM AUTOMATION ARCHITECTURE DIAGRAM) shall communicate with the CSS subsystems.

8.6.1.1 Topsides Electrical System controllers shall communicate with PCS, PSD and FGS. Hull Electrical System controllers shall communicate with HCS, HSD and HFGS.

8.6.2 Shutdown signals from PSD, HSD, FGS and HFGS of all electrical loads shall be hardwired from each CSS I/O to the correspondent electrical equipment drawer.

8.6.3 Local start pushbuttons of all electrical loads shall be hardwired to PCS/HCS REMOTE I/Os.

8.6.4 Local stop pushbuttons of normal loads shall be hardwired to PSD/HSD or FGD/HFGS REMOTE I/Os.

8.6.5 Local stop pushbuttons of essential loads shall be hardwired to switchgear/MCC.

8.6.6 Interface between PSD, HSD, FGS and HFGS with the relays of electrical loads shall be established by sending a discrete hardwired signal from the subsystem's REMOTE I/O to the electrical drawer for emergency stop commands.

8.6.7 Interface between PCS, HCS, FGS and HFGS with Electrical System controllers shall be established by a Modbus TCP/IP network for automatic control (CSS) and remote commands (SOS). Other networks may be defined in Project. Figures 7 and 8 show the schematics for the interfaces between TOPSIDES CSS and Hull CSS with the Electrical System Network.

8.6.8 Each network switch shall be Layer 2 / 1u, according to Project's documentation entitled AUTOMATION NETWORK REQUIREMENTS and with the maximum number of available ports for a 1u switch.

8.6.9 For emergency shutdown commands sent from CSS or field pushbuttons of normal loads to electrical drawers, an interposing relay shall be included in Electrical system side (see Figure 9).

8.6.10 Temporary bypass of PSD/HSD for pump/motor start-up shall be done using the HSDN.

8.6.11 For more details of electrical loads actuation see I-DE-3010.00-5140-797-P4X-002 – ELECTRICAL SYSTEM AUTOMATION TYPICAL ACTUATION DIAGRAMS and I-LI-3010.00-5140-797-P4X-001 - ELECTRICAL SYSTEM AUTOMATION INTERFACE SIGNALS LIST.

8.6.12 The interface between the CSS and Electrical System shall also be implemented as described in I-DE-3010.00-5140-797-P4X-001 – ELECTRICAL SYSTEM AUTOMATION ARCHITECTURE DIAGRAM, I-ET-3010.00-5140-797-P4X-001 – ELECTRICAL SYSTEM AUTOMATION ARCHITECTURE, AUTOMATION AND CONTROL ARCHITECTURE Drawing and NETWORK INTERCONNECTION DIAGRAM Drawing.

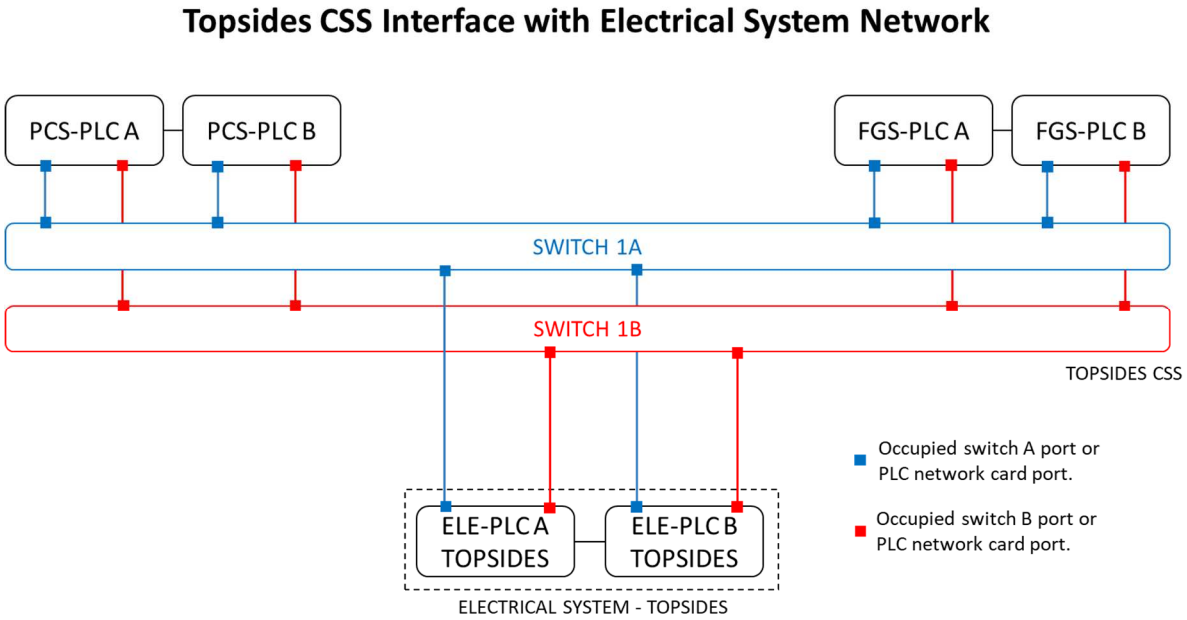


Figure 7 – Topsides CSS interface with Topsides Electrical System Processors.

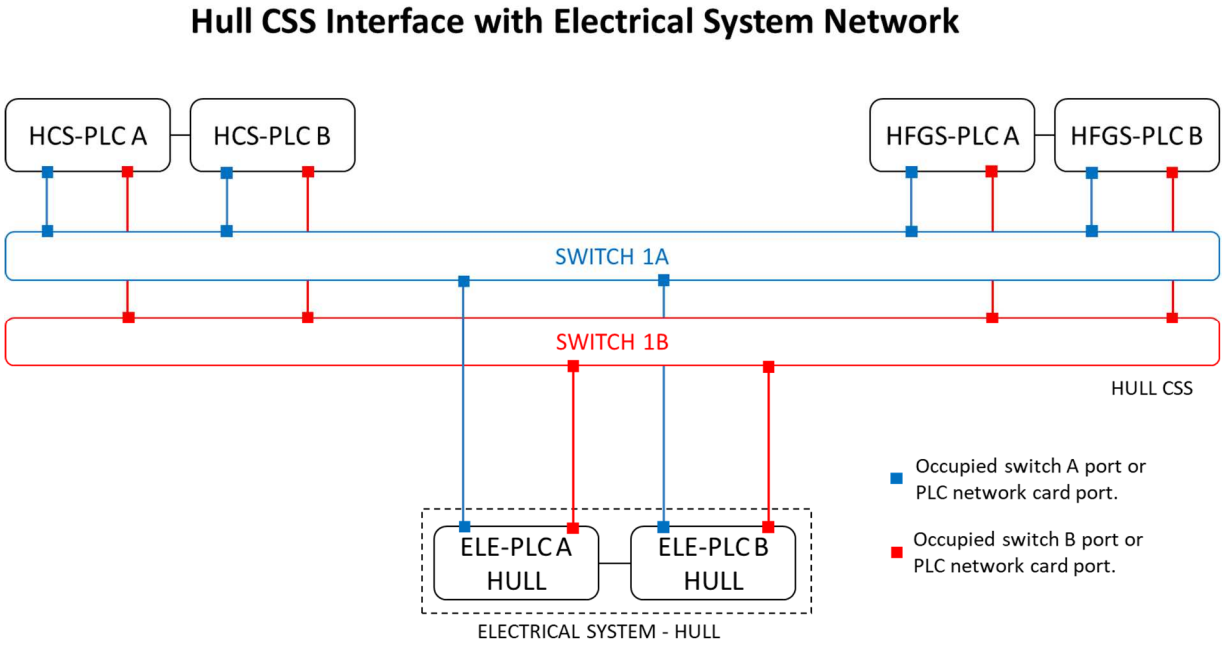


Figure 8– Hull CSS interface with Hull Electrical System Processors

## 8.7 CSS – SPCS

8.7.1 For interface description between CSS and SPCS, see the following Project´s documents:

- I-DE-3010.00-1210-888-P4X-002 - PRODUCTION WELL CONTROL RACK - FUNCTIONAL DIAGRAM;
- I-DE-3010.00-1210-888-P4X-001 - PRODUCTION WELL CONTROL RACK – LAYOUT;

- I-ET-3000.00-5139-800-PEK-004 - HYDRAULIC POWER UNIT FOR SUBSEA EQUIPMENT WITH MULTIPLEXED ELECTROHYDRAULIC AND DIRECT HYDRAULIC CONTROL SYSTEM (OWN FLOATING PRODUCTION UNIT);
- I-ET-3010.00-5139-390-P4X-001 – HYDRAULIC POWER UNIT (HPU) FOR TOPSIDES VALVES;
- I-DE-3010.00-5139-390-P4X-001 - HYDRAULIC POWER UNIT (HPU) FOR TOPSIDES VALVES - HYDRAULIC DIAGRAM;
- I-ET-3010.00-1210-888-P4X-001 - PRODUCTION WELL CONTROL RACK;
- I-ET-3010.00-1210-888-P4X-003 - SESDVS CONTROL RACK;
- AUTOMATION AND CONTROL SYSTEM FUNCTIONS descriptive memorandum;
- SPECIAL MONITORING SYSTEMS technical specification.

8.7.2 TPT/TPT-AR are hardwired signals (4-20 mA).

## 8.8 CSS - Telecom System

8.8.1 The interface with the PA/GA System shall be accomplished through FGS and HFGS.

8.8.2 Signals shall be exchanged between Telecom Systems and CSS through a CSS REMOTE I/O PANEL located in the same room as the CSS PROCESSORS PANEL.

8.8.3 Monitored Discrete Outputs (DOM) from FGS and HFGS shall send 24 VDC signals to PA/GA System located in Telecom Rooms for alarm activation.

8.8.4 Discrete 24 VDC malfunction alarm signals shall be sent from the Telecom Power System battery charger(s) (DO) to a CSS REMOTE I/O PANEL (DI). These signals shall be displayed at the Supervisory System.

8.8.5 Discrete 24 VDC I/O signals (DO) shall be sent from a CSS REMOTE I/O PANEL to the Telecom Power System battery charger(s) (DI) in order to shutdown charger(s) in case of hydrogen detection and ventilation failure in the batteries room.

8.8.6 For each discrete signal exchanged between CSS and Telecom System, an interposing relay shall be included. The interposing relay shall be installed in the Telecom Panel.

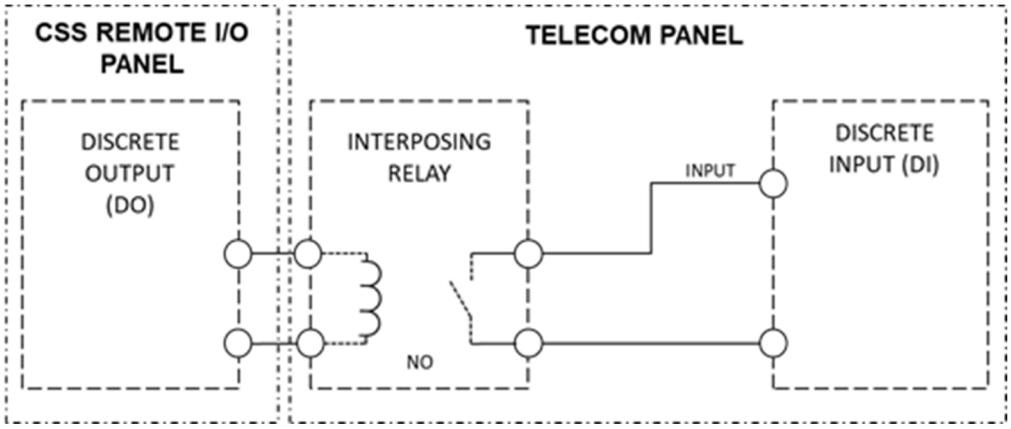


Figure 9 – Discrete signal exchanged between CSS and Telecom System or between CSS and Electrical loads´ drawers/IEDs.

8.8.7 For further details, see AUTOMATION AND CONTROL ARCHITECTURE drawing and I-MD-3010.00-5510-760-PPT-001 - GENERAL CRITERIA FOR TELECOMMUNICATIONS DESIGN.

## 8.9 CSS – Machinery Monitoring System (MMS)

8.9.1 CSS interface with MMS shall be according to I-ET-3010.00-5500-854-P4X-001 - MACHINERY MONITORING SYSTEM (MMS).

## 8.10 CSS – Flow Metering System (FMS)

8.10.1 CSS interface with FMS shall be according to project's drawing entitled FLOW METERING SYSTEM (FMS) ARCHITECTURE and technical specification entitled FLOW METERING SYSTEM (FMS).

## 8.11 CSS – Asset Monitoring System (AMS)

8.11.1 CSS shall be supplied with all equipment (HART I/O cards, HART modules, converters, switches etc.) needed, in order to read HART data from field instrumentation and to send data to the Asset Monitoring System (AMS).

8.11.2 In case switches are necessary, these shall be rack mounted (19" standard rack) and installed inside PCS/HCS section of CSS SERVERS PANEL.

8.11.3 HART data shall be made available to the AMS through the CSS Data Acquisition LAN.

8.11.4 See I-ET-3010.00-1200-850-P4X-002 - ASSET MANAGEMENT SYSTEM (AMS) for additional interface requirements.

## 8.12 Other Interfaces

8.12.1 For other CSS interfaces, see the following Project´s documents:

- I-ET-3010.00-1200-859-P4X-001 - AUTOMATION REQUIREMENTS FOR CORROSION MONITORING SYSTEM (CMS)
- TOPSIDES AND HULL AUTOMATION INTERFACE
- AUTOMATION INTERFACE OF PACKAGE UNITS
- SPECIAL MONITORING SYSTEMS

# 9 DOCUMENTATION

9.1 Complete documentation of the CSS, covering all devices (including installed software and firmware versions) 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 PETROBRAS documents, at least the following technical documents:

- Technical specifications, comprising: equipment, accessories, panel and materials;
- Data-sheets and brochures for each equipment;
- All equipment and installation data including: material list, equipment list, spare part list, power consumption, heat dissipation, weight, panel lay-out, etc;
- Complete description of services, tests, etc.
- Documentation requested by other project documents related to CSS system (see item 2.2.1).

9.3 There shall be supplied for evaluation, in the number of copies defined at PETROBRAS documents, in searchable PDF and editable files (when applicable), at least the following technical documents:

- Technical specifications, comprising all equipment, instrument, accessories, cables and materials;
- Drawings for all panel, racks and their components;
- Calculation reports of all panel components including dimensioning of circuit breakers, power sources and internal cables, considering the maximum consumption of internal components (e.g. all I/O cards including I/O cards of future expansion at maximum power and current consumption) in editable file format;
- Data sheets of panel and rack components (including PLCs);
- Installation drawings including general arrangement, electrical diagrams, wiring diagrams, cable, material list, and equipment list;
- Utilities consumption list with nominal power consumption, consumed power, typical dissipated power and maximum dissipated power, considering "as purchased" loads information.
- Calculation method shall be presented in a report with the power values for each CSS component discriminated. Any power factor and / or utilization factor considered for the calculations shall be informed. Item 7.8.7 shall be fully complied with.
- Weight control report with the weight of CSS assembled parts and discriminated weights of each individual component.
- I/O list and memory map;
- Test procedures;
- Certificate of materials;

- Explosive atmospheres and IP degree certificates;
- Availability calculations;
- All software properly licensed to PETROBRAS;
- Commented Application source program and Executive application program;
- All hardware, software and users´ manuals;
- Complete CSS certified documentation, as required at I-ET-3010.00-5520-862-P4X-001 - PROGRAMMABLE LOGIC CONTROLLERS - PLC and I-ET-3010.00-5520-888-P4X-001 – AUTOMATION PANELS, including Operation Manual and Maintenance Manual.

# 10 ACCEPTANCE TESTS

10.1 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 punch list control system defined in contract.

10.2 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).

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

10.4 Personnel, material, necessary equipment and instruments for all the tests shall be provided, independent of the place where they are carried out, until the final commissioning and acceptance of the UNIT by PETROBRAS.

## 10.5 Factory Acceptance Tests (FAT)

10.6 The following tests, besides the tests required at I-ET-3010.00-5520-862-P4X-001 - PROGRAMMABLE LOGIC CONTROLLERS - PLC and I-ET-3010.00-5520-888-P4X-001 – AUTOMATION PANELS, shall be performed, where applicable, prior to delivery:

- Mechanical Inspection;
- Hardware inventory check;
- Software licensing check;
- Wiring and Termination inspection;
- Start-up Test;
- Visualization/operation;
- General System functions including hardware redundancy and diagnostic check;
- Functional test;
- Subsystems interface test;
- Maximum response time test (see item 4.7).

10.6.1 FAT shall be witnessed, to be agreed between PETROBRAS and CSS SUPPLIER during Project. FAT report tests shall be signed and sent to PETROBRAS.

10.6.2 Prior to the witnessed FAT, SUPPLIER shall send the Tests proceedings to

PETROBRAS, according to Project's schedule, and shall execute previous tests and present the documentation to PETROBRAS, in order to reduce repairs and/or modifications during FAT.

10.6.3 The FAT shall be fully documented, including any equipment failure, repairs or replacements. The FAT procedure shall include handling over all records made during the construction period such as test results, list of changes, as-built drawings, calibration certificates and any other documentation.

10.6.4 All documentation (project and tests) shall be sent in digital media.

10.6.5 Testing methods and accuracy of measurements shall be subject to the Classification Society and PETROBRAS approval.

10.6.6 Any malfunctions of the equipment shall be rectified and tested again, at CSS SUPPLIER'S expenses, and be submitted to PETROBRAS approval. Evidence of the correction shall be presented.

10.6.7 In FAT location, all facilities such as redundant external power supplies shall be available. Ambiance temperature shall be controlled. The FAT facility shall include adequate air conditioning to ensure that the testing environment (where there are numerous screens and other equipment generating large amounts of heat) is maintained at a comfortable temperature (less than 25 °C).

10.6.8 Electrical and RFI & EMI Immunity tests shall be according to project's "INSTRUMENTATION ADDITIONAL TECHNICAL REQUIREMENTS" technical specification.

10.6.9 Functional Tests shall be as described below:

- Complete system functional test, with simulation of all input situations and observation of expected outputs; the overall reaction time shall be verified;
- Input / Output Tests;
- Devices shall be tested according to test and operation device manuals.

10.6.10 FAT report shall include a punch list with all non-impeditive deviations and anomalies that will be treated in field, including the date for treatment deadline.

10.6.11 During FAT, all Ex certificates of each component and of the assembly shall be verified and validated.

10.6.12 During FAT, inventory shall be kept of all CSS components and spare parts in order to guarantee traceability and availability.

### 10.7 Site Acceptance Test (SAT)

10.7.1 All tests performed at the factory (FAT) shall be repeated at the installation site (SAT). IEC 62381 requirements shall also be taken into account.

10.7.2 During SAT, any necessary design modifications after FAT shall be tested and FAT punch list items shall be treated.

10.8 After the CSS installation at the site, at least the following tests (SAT) shall be provided in order to assure that the equipment is correctly installed:

- Mechanical Inspection;
- Hardware and Software inventory check;
- Start-up/Diagnostic Check;
- Software downloads and functional tests;
- CSS synchronization with SOS;
- Integrated response time between CSS and SOS (equal to or less than 2 seconds).

### 10.9 Site Integration Test (SIT)

10.9.1 For Site Integration Tests (SIT) refer to IEC-62381 – AUTOMATION SYSTEMS IN THE PROCESS INDUSTRY – FACTORY ACCEPTANCE TEST (FAT), SITE ACCEPTANCE TEST (SAT) AND SITE INTEGRATION TEST (SIT).

10.9.2 The tests shall include all interconnection and communication tests between CSS, SOS and the Automation systems.

## 11 PACKING REQUIREMENTS

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

11.2 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.

11.3 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.